IJNS
International Journal of Network Security

ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 20, No. 6 (Nov. 2018)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at http://ijns.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

Volume: 20, No: 6 (November 1, 2018)

International Journal of Network Security

Uniform Resource Locator Based Steganography Methodology

Abdelrahman Desoky
(Corresponding author: Abdelrahman Desoky)
Department of Computer Science, Claflin University
400 Magnolia St, Orangeburg, SC 29115, USA
(Email: desoky@desoky.com)
(Received Dec. 30, 2017; revised and accepted Apr. 22, 2018)

Abstract

The Internet is widely popular and has become a culture of most, if not all, mankind worldwide. The use of the Internet is solely through accessing web-addresses like social-media, online-news, emails, *etc.* Obviously, this generates enormous traffic allowing communicating parties to establish a covert channel without a suspicious pattern. This renders the Uniform Resource Locator (URL) a highly attractive steganographic carrier to securely conceal and transmit messages. As a result, a novel URL-Based Steganography Methodology (URL-Stega) is presented in this paper. URL-Stega generates a steganographic cover in a form of a web-link. Simply, URL-Stega encodes a message then assigns it to steganographic carriers such as words, alphabet, numeric, alphanumeric, or other legible URL characters in order to camouflage data in the generated URL (Web Address). In addition, generated text-cover (URL-Cover) can be embedded among other legitimate non-coded text to make it harder for adversary to suspect and/or analyze such text. Unlike contemporary text-steganographic techniques, URL-Stega doesn't hide messages in the actual text body. Instead, URL-Stega conceals both the message and its transmission in innocent web-links rather than webpage contents. Yet, shortening the generated URL-Cover as any non-steganographic URL makes it more impressive to conceal data. URL-Stega neither hides data in a noise (errors) nor produces noise while a message is concealed in a legitimate URL. The presented implementation, validation, and steganalysis of URL-Stega demonstrate: robustness of achieving the steganographic goal, adequate room for concealing data, and superior bitrate than any other contemporary text steganography approaches from roughly about 39.47% up to 75.0%.

Keywords: Indicators; Social-media; Steganography; URL-Stega

1 Introduction

Steganography is the scientific art of concealing the presence of covert communications. The steganographic goal is to prevent an adversary from suspecting the existence of covert communications [7, 8]. Unlike cryptography, the aim of steganography is not to impede an attacker from deciphering a hidden message like ciphertext. To emphasize, if suspicion is raised when using any steganographic technique, the goal of steganography is defeated regardless of whether or not a plaintext is revealed [7]. Contemporary approaches in the literature are often classified based on the steganographic cover type like image, audio, graph [21], and text. When text is employed for hiding data and generating the steganographic cover, an approach is usually categorized as textual steganography to distinguish it from non-textual techniques like image or audio. Textual steganography has become more favorable in recent years because the size of non-textual cover is relatively large and burdens the traffic of covert communications [28].

Contemporary steganography, other than Nostega-based techniques, hides a message as noise in a cover that is assumed to be unnoticeable. For instance, an encoded message can be embedded into an image by altering it without noticeable degradation to human eyes [28]. Similarly, a message can be hidden in a text by modifying the format and style of an existing text [7, 8]. The alteration of authenticated covers may raise suspicion, and the message may be detectable regardless of whether or not a plaintext is revealed. The same applies for hiding data in unused or reserved space for systems software including designated storage area of an operating system, the file headers on a hardrive [30], or in the packet headers of communication protocols such as TCP/IP packets [26]. These techniques are vulnerable to distortion attacks [7].

On the other hand, a similar argument is made in the literature about textual steganography approaches such as: null cipher [7], mimic functions [36], NICETEXT and SCRAMBLE [5], translation-based [25], confusing ap-

proach [33], and abbreviation-based [31]. The vulnerability and concerns of these textual approaches are explained minutely in [7] and can be summarized as follows. First, the textual-cover either introduce detectable flaws (noise) such as: incorrect syntax, lexicon, rhetoric, or grammar when generating a text-cover. Such flaws can raise suspicion about the presence of covert communications. Second, the content of the cover may be meaningless and semantically incoherent, and therefore draw suspicion. Third, the bitrate is very small. Since there is a limit on how many flaws a document can typically have, a very large document is needed to hide few bytes of data. In fact, this applies to non-textual approaches as well. Fourth, the bulk of the efforts have been focused on how to conceal a message and not on how to conceal its transmittal. In other words, the establishment of a covert communication channel has not been an integral part of most approaches found in the literature. Fifth, while these approaches may fool a computer examination, they often fail to pass human inspections. A successful textual steganographic system (stegasystem) must be capable of passing both computer and human examinations. These concerns have motivated the development of the

URL-Based Steganography Methodology (URL-Stega), as introduced in this paper. URL-Stega overcomes the issues mentioned above by manipulating only the textual part of a web-link (Web Address/URL) to camouflage both a message and its transmittal. Fundamentally, URL-Stega exploits textual elements of URL such as words, alphabet, numeric, alphanumeric, and other legible URL characters in order to camouflage data in the generated Web Address. In addition, the generated text-cover (URL-Cover) can be embedded among other legitimate non-coded text to make it harder for an adversary to suspect and/or analyze such text. Unlike contemporary text-steganographic techniques, URL-Stega doesn't hide messages in the actual text body. To emphasize, URL-Stega does not conceal data in the actual content of a webpage. Instead, URL-Stega conceal both the message and it its transmission in innocent web-links. Shortening the generated URL-Cover as any non-steganographic URL makes it more impressive to conceal data. Such elements can be fabricated in a legitimate way in order to embed data without generating any type of suspicious pattern. Basically, URL-Stega encodes a message and then assigns it to legitimate elements (*e.g.* words, alphabet, numeric, alphanumeric, other legible URL's characters, *etc.*) in order to generate a text-cover in a form of a web address.

The main advantages of URL-Stega are as follows. First, the high demand for using Internet by a wide variety of people worldwide creates a high volume of traffic which averts suspicion in the presence of covert communication channels. Second, URL-Stega does not imply a particular pattern (noise) that an adversary may look for. Third, the concealment process of URL-Stega has no effect on the linguistics of the generated cover (URL-cover) because no linguistic structures are required in URL to be obeyed. Therefore, a URL-cover is linguistically legible, and as such is capable of passing both computer and human examinations. Fourth, URL-Stega can be applied to all languages. Fifth, the textual of URL-Cover has plenty of room for concealing data, as demonstrated later in the paper. The observed average bitrate of the current implementation experiments is superior to all contemporary textual steganography approaches found in the literature to be roughly around 3.38% up to 7.67%. Sixth, URL-Stega is resilient to all known attacks, and the hidden message is anti-distortion. It is worth noting that the presented methodology in this paper follows this new Nostega paradigm [7, 9, 10] by exploiting URL to camouflage data without generating any suspicious pattern. Examples of other Nostega-based system are Sumstega [11, 12], Listega [13], Notestega [14], Matlist [15], NORMALS [16], Edustega [17], Headstega [18], Jokestega [19], and Chestega [22]. The implementation and steganalysis validation demonstrate that URL-Stega methodology is capable of achieving the steganographical goal.

The remainder of this paper is organized as follows. Section 2 explains the URL-Stega methodology and its implementation in detail. Section 3 presents the steganalysis validation and its bitrate versus others. Finally, Section 4 concludes the paper.

2 URL-Stega Methodology

To illustrate URL-Stega, consider the following scenario. Bob and Alice are on a spy mission. Like any ordinary people, Bob and Alice access, send, and receive URLs from each other via chat, email, or by any other electronic means. Before they go on their mission, which requires them to reside in two different countries, they strategically plan and set the rules for communicating covertly using their friendship as a steganographic umbrella to justify sending and receiving messages. They agree on concealing messages only in URLs in such a way that does not look suspicious while the content of a webpage is legitimate and nothing is concealed in it. To make this work, Bob and Alice can legitimately send, receive, and forward emails, chats, posts, and texts to each other or to other individuals without suspicion. Covert messages transmitted in this manner will not look suspicious because the content of the webpage contains no hidden message except its web-link. Furthermore, Alice is not always the sole user or recipient of Bob's URL and vice versa. In other words, other non-spy people may also receive messages from Bob or Alice. As a result, suspicion is further warded off, thereby fooling an adversary. However, only Bob and Alice will be able to unravel the hidden message because they know the rules of the game.

2.1 An Overview of URL-Stega Architecture

The core idea of URL-Stega methodology is basically camouflaging data in the natural and legitimate URL.

Therefore, URL-Cover will look like any ordinary web address.

As shown in Figure 1, a legitimate URL shows the use of Google search engine when searching the word "test". Note that a web link looks like an illegible text. However, due to the use of URL, an adversary will be fooled in URL-Cover because URL will legitimize the text-cover. URL is an excellent means for camouflaging data due to the common use of illegible format of text that can contain a combination of alphabet, numbers, or special characters, without obeying any linguistic syntax. In addition, URL looks as if it is in a random format which makes it easy to embed encoded messages for covert communications.

Linguistically and logically, the URL format like the combination of characters used in Figure 1, qualifies URL as a legitimate steganographic cover. Additionally, URL-Stega methodology takes advantage of the heavy traffic of the Internet via accessing web-addresses, social-media, online-news, emails, and more to conceal both a message and its transmittal in a web link format.

URL-Stega Architecture:
The following is an overview of the URL-Stega architecture, which consists of three modules, as shown in Figure 1:

1) Determining the Set of Characters (Module 1) to be used for encoding messages.

2) Building URL-Stega Encoder (Module 2) that is capable of encoding and camouflaging messages using the determined characters format from Module 1.

3) Establishing a Covert Channel (Module 3) to embed an encoded message in order to camouflage the message and its transmittal in a sub domain name such as a web link.

The following subsections explain these modules in detail.

2.2 Determining the Set of Characters (Module 1)

Determining the set of characters to be used by the encoder (Module 2) for encoding messages, as discussed in Subsection 3.3. Simply, the maximum number of characters in the character set may be equal to all allowed characters in Uniform Resource Identifier (URI) and should not exceed its maximum unless there is a legitimate reason to generate an illegitimate web-link. Generating illicit web-link is not recommended without legitimacy because it can easily be detected. Therefore, this paper will only use a legitimate character set that is allowed in URI/URL while other characters are forbidden. Table 1 shows the allowed characters in URI [1–3]. URL-Stega may use the entire set of characters in Table 1 or a subset.

Table 1: Allowable characters by URI

RFC 3986 section 2.2 Reserved Characters (January 2005)		RFC 3986 section 2.3 Unreserved Characters (January 2005)				Other characters in a URI must be percent encoded.
	!		A	a	0	
	*		B	b	1	
	'		C	c	2	
	(		D	d	3	
	)		E	e	4	
	;		F	f	5	
	:		G	g	6	
	@		H	h	7	
	&		I	i	8	
	=		J	j	9	
	+		K	k	-	
	$		L	l	_	
	,		M	m	.	
	/		N	n	~	
	?		O	o		
	#		P	p		
	[		Q	q		
	]		R	r		
			S	s		
			T	t		
			U	u		
			V	v		
			W	w		
			X	x		
			Y	y		
			Z	z		

2.3 Building URL-Stega Encoder (Module 2)

Coding is a very well researched technical field, and there are numerous published techniques that can be employed to generate steganographic code [7,20]. Therefore, this subsection only focuses on key issues that affect the implementation of URL-Stega Encoder and building a URL-Stega Encoder that is capable of encoding messages using the determined character type and the format from Module 1. Table 1 shows a list of most of the characters that can be used in URI/URL. However, when building such encoder, a subset of Table 1 may suffice to achieve the steganographic encoder goal. Note that the character set must cover the entire length of binary code. In other words, if the length of a binary code equal n digits then the steganographic parameters must be capable to cover n digits from all of 0's and up to all of 1's (e.g. 00000-11111, length of 5 digits). To emphasize, 2 digits 00-11, 3 digits 000-111, 4 digits 0000-1111, 5 digits 00000-11111, 6 digits 000000-111111, and so on. This is to cover all possible binary values. Therefore, if 2 digits are selected, then 4 different symbols/characters are needed in order to cover 4 different binary values, and if 3 digits are chosen, then 8 different characters are needed in order to cover 8 different binary values. Thus, a message may be encoded by slicing its binary string into a particular length of bits such as four bits, seven bits, or any required bit length.

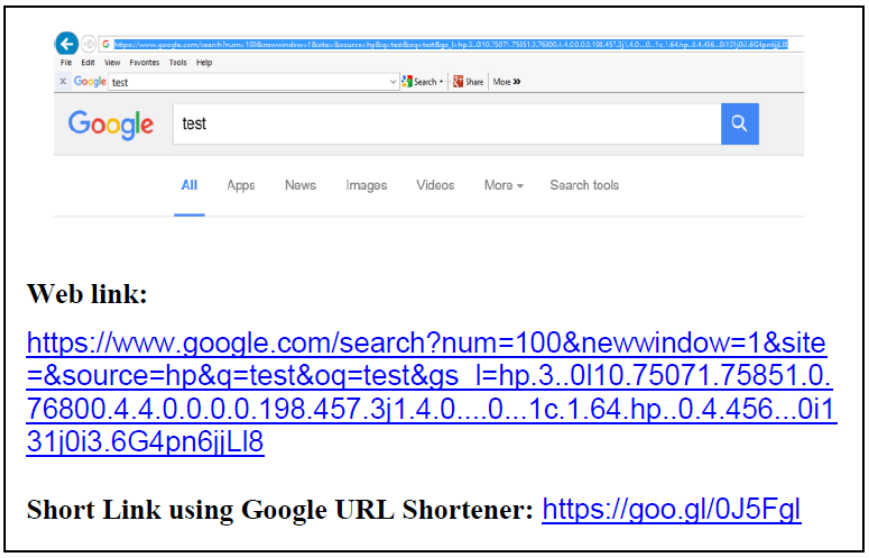


Figure 1: Shows a common web search result for the word "test" using the Google Search Engine. The search result is presented via web-link. Obviously, this web-link does not contain a hidden message and it is just an innocent and common practice of web search engine. The second web-link appears after shortening the first web-link using Google URL Shortener.

Example:

- A message in plaintext: "our meeting 8pm";
- The concatenated binary string of the ASCII representation of the above message is:

  01101111011101010111001000100000011101101
  01100101011001010111010001101001011011110
  01100111001000000011100001110000001101101

- Slicing this string (from the previous step) into 6 bits each will result in:

  011011 110111 010101 110010 001000 000110
  110101 100101 011001 010111 010001 101001
  011011 100110 011100 100000 001110 000111
  000001 101101

- URL-Cover of the binary code above, generated using Table 2 and Table 3, shows the mapping process for each character based on Table 2. The following is a pre-final URL-Cover before embedding it in domain name: "b3VyIg1lZXRpbmcgOHBt";
- Final URL-Cover, as shown in Figure 3, after embedding it in domain name (e.g. www.desoky.com) and it is ready to be delivered by accessing or sending it: "http://desoky.com/b3VyIg1lZXRpbmcgOHBt". Obviously, other existing domain names or generating new domain names can be used. In addition, URL-Cover can be shortened using any URL shortening tools, as shown in Table 4.

Table 2: 6 bit-based steganographic code table

URL-Stega Code	Binary Code	URL-Stega Code	Binary Code	URL-Stega Code	Binary Code
A	000000	a	011010	0	110100
B	000001	b	011011	1	110101
C	000010	c	011100	2	110110
D	000011	d	011101	3	110111
E	000100	e	011110	4	111000
F	000101	f	011111	5	111001
G	000110	g	100000	6	111010
H	000111	h	100001	7	111011
I	001000	i	100010	8	111100
J	001001	j	100011	9	111101
K	001010	k	100100	-	111110
L	001011	l	100101	_	111111
M	001100	m	100110		
N	001101	n	100111		
O	001110	o	101000		
P	001111	p	101001		
Q	010000	q	101010		
R	010001	r	101011		
S	010010	s	101100		
T	010011	t	101101		
U	010100	u	101110		
V	010101	v	101111		
W	010110	w	110000		
X	010111	x	110001		
Y	011000	y	110010		
Z	011001	z	110011		

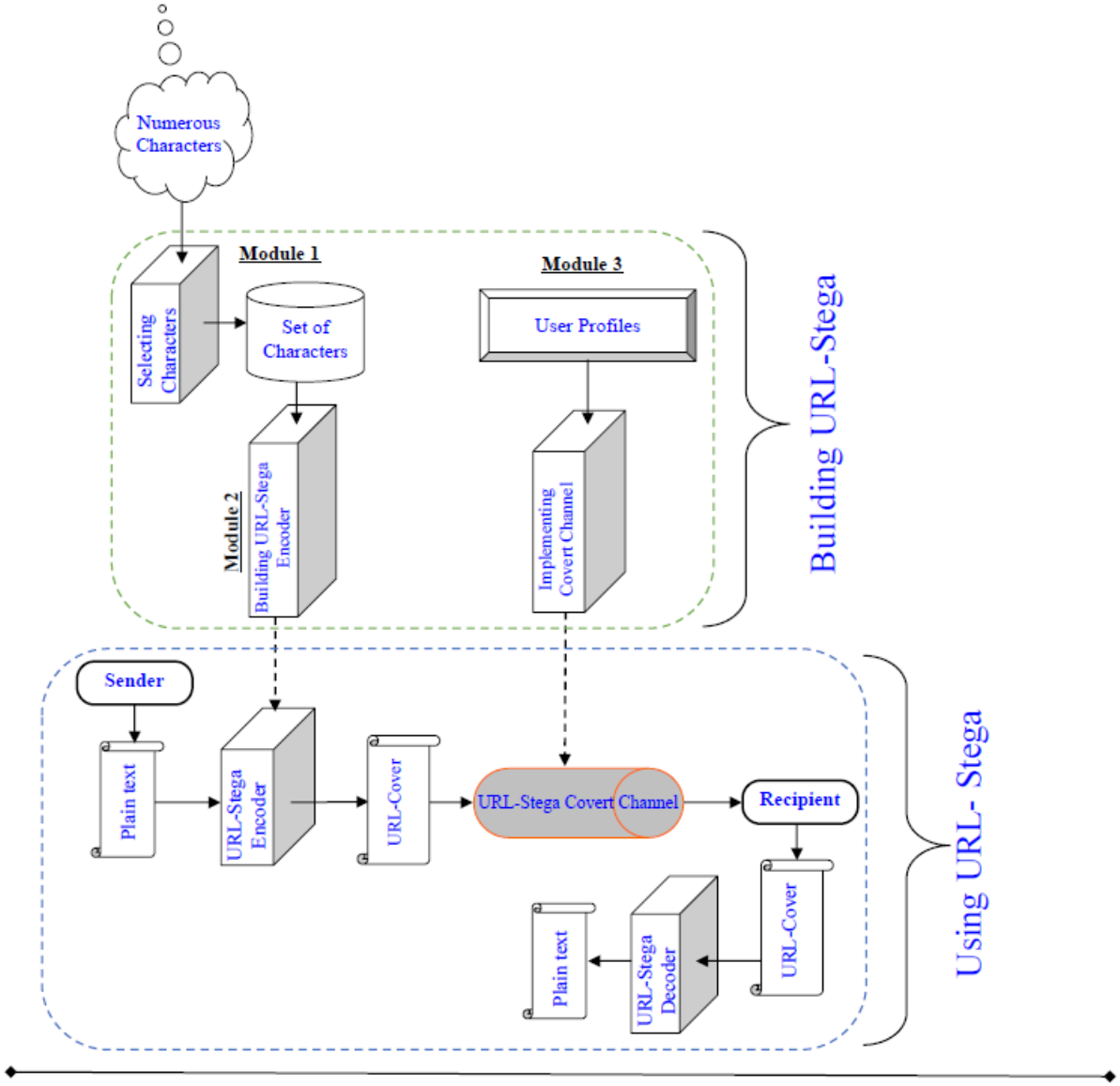


Figure 2: Illustrates the architecture and the use of URL-Stega. It shows the interaction of various modules to build URL Stega. Then, it shows the use of URL-Stega scheme by the communicating parties.

Table 3: Encoded message by encoding each 6 bits from Table 2

Index	Binary Message	URL-Cover
1.	011011	b
2.	110111	3
3.	010101	V
4.	110010	y
5.	001000	I
6.	000110	g
7.	110101	1
8.	100101	l
9.	011001	Z
10.	010111	X
11.	010001	R
12.	101001	p
13.	011011	b
14.	100110	m
15.	011100	c
16.	100000	g
17.	001110	O
18.	000111	H
19.	000001	B
20.	101101	t

- URL Checker can be used to avoid false link. There are some online tools that verify short URL in order to show the full URL, e.g. unfurlr.com [27], getlinkinfo.com [23], checkshorturl.com [6], unshorten.it [34], and urlxray.com [35].

In this paper, the steganographic code example is configured by determining the number of bits (m bits) used for binary values e.g. 4, 5, 7, *etc.* This is based on the available number of characters in the defined steganographic character set which is 64 characters according to Table 2. It is worth noting that Table 2 is derived from Table 1 as discussed earlier. The 64 characters in a steganographic character set are suitable to slice a binary message based on a length of 6 bits. The grouping in lengths of 6 digits will result in a value of 0 up to 63 in decimal and changing the value from 000000 up to 111111 in binary. Each character in URL-Cover conceals a particular m bits according to the steganographic code defined in Table 2. The current steganographic code is just a simple example to ease the understanding of the presented approach. The steganographic code may differ from one implementation to another and many alternatives with more sophisticated encoding techniques can be employed.

2.4 Establishing a Covert Channel (Module 3)

The frequent use of URL is widely popular and generates a high volume of traffic that allows communicating parties to establish a covert channel without a suspicious pattern. This makes web-link an attractive steganographic carrier for transmitting hidden messages. In this paper, Module 3 is responsible for embedding an encoded message in a domain name like a sub-link in order to generate a URL-Cover for concealing data. Unlike other steganographic approaches (e.g. image, audio, text, *etc.*) where a message is hidden in URL-Cover, it also addresses how a message is delivered. Specifically, a message is concealed in an image or audio file and then the file is delivered. Conversely, when concealing a message in URL, the message is delivered via accessing or sending the same URL. Thus, the steganographic cover is the same steganographic transmittal method, which is the covert communication channel. A sender will hide a message in a web-link, then a recipient will access or receive it via email, posting, chat, or by any other way. A sender and recipient may pre-agree on a particular URL domain name to use in order to hide and retrieve messages. Other ordinary people who are not part of the steganographic game can also access, send, and/or receive the same URL from each other for non steganographic purposes. Therefore, suspicion is warded off. Using URL makes it more legitimate and very difficult, if not impossible, to investigate. It is essential that legitimate users plot a convincing strategic plan and set the rules for communicating covertly using justifiable reasons as a steganographic umbrella to avert suspicious from covert communications. Basically, legitimate users have the right to use URL via accessing, sending, receiving, forwarding emails, chatting, posting, or texting each other. Covert messages transmitted in this manner will not look suspicious because such URL is sent via email, chat, posting, or texting while its content does not contain any hidden message except in the web-link. Therefore, such communication will be fully legitimate and justifies the discernable communications. The example presented in this paper conceals up to 120 bits in the URL-Cover. It is worth noting that the use of words and numerical values can be employed to conceal data. Due to the size constrain of this paper, the presented URL is just an example, and URL-Stega can conceal longer messages. After concealing data in URLs, web-links can also be combined with other web addresses (non-coded) that are not used to camouflage data for further protection and legitimacy. In this case, a predetermined-based protocol can be employed among communicating parties such as read every other URL, every fifth URL, or any other way in order to ease the process of unraveling a hidden message while making it harder on an adversary.

3 Steganalysis Validation

The aim of this section is to show the resilience of URL-Stega to possible attacks. The success of a steganographic approach is its ability of preventing an adversary from suspecting the presence of a hidden message. It is assumed that an adversary will perform all possible investigations,

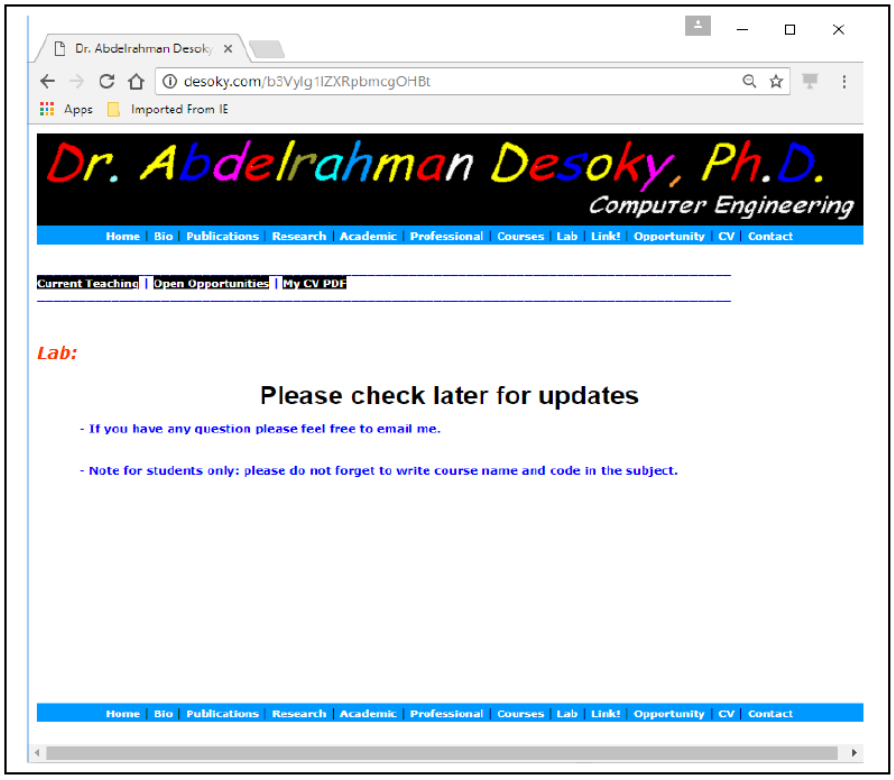


Figure 3: An actual example of URL-Cover. The message is not concealed in the web page content, but it is embedded in the URL.

and he is aware of URL-Stega as a public methodology. However, he does not know the actual URL-Stega configuration that the sender and recipient employed for their covert communication.

3.1 Traffic Attack

One possible attack an adversary may pursue is to inspect the communication traffic of images, graphs, audio files, and text files in order to detect the existence of covert communications. For example, the intelligence community has a number of tools at their disposal for analyzing traffic on the Internet, tracking access to web sites, monitoring checked out literature from public libraries, and so on. The main goal of a traffic attack is to detect unusual or questionable association between a sender and recipient. Traffic analysis intuitively can identify who communicates with whom. The relationship between the communicating parties and their profiles (*e.g.* occupation, interest, hobbies, *etc.*) will play an essential role in either legitimizing or suspecting the presence of covert communications. Traffic attacks can be a threat for most contemporary steganographic techniques regardless of the steganographic cover types used. In regards to URL-Stega, the profile of users and webpage contents of particular URL are checked instead of its validity and its consistency to the URL's text body. In other words, the URL is most likely overlooked because no one will read or pay too much attention to it since it contains no meaningful information. For this reason, it is a common behavior that all Internet users accessing a web-address pay attention to the contents of the webpage rather than its web-address. On the other hand, if someone unrelated to the medical field such as a taxi driver, baker, or carpenter accesses, sends, and receives web-address for medical research without a justifiable reason, suspicion can be raised and further investigation may be prompted. Additional investigations may involve a thorough analysis of a steganographic cover as detailed in the next subsections.

Traffic analysis is deemed ineffective with URL-Stega. URL-Stega camouflages the transmittal of a hidden message (URL-Cover) making it appear legitimate, averting suspicion. URL-Stega is based on Nostega paradigm [9, 10]. URL-Stega by default ensures that the involved parties establish a covert channel. This is achieved by securing that the users have a legitimate relationship with each other and the used URL is justifiable. As such, the traffic of communication is innocent and appears like normal communication. Analyzing the traffic between them will not reveal any questionable association and will not trigger any further investigation. In addition, URL-Stega requires the communicating parties to use innocent URL domains like news, blog, or others that are commonly used by a wide variety of people. The common use of such domains generate a high volume of traffic which makes it impractical for an adversary to investigate all traffics.

Table 4: List of different short link of the same URL-Cover

Tool Name for Shortening the URL	Short URL-Cover
Google URL Shortener [24]	https:/goo.gl/3AcmRm
Bitly [4]	http://bit.ly/2rwqLic
Ow.ly via Hootsuite [29]	http://ow.ly/XZjk30cIKC4
TinyURL by Gilby [32]	https://tinyurl.com/y9zvza9w

The voluminous traffic plays a core role that allows the communicating parties to establish a covert channel in order to transmit a URL-Cover without drawing attention. As a result, URL-Stega is an attractive steganographic methodology. Finally, note that if further investigations on a URL-Cover are triggered by traffic analysis, they would not be successful as will be explained later. To sum, differentiating between a URL-Cover containing a hidden message with that of other URL peers without a hidden message is infeasible.

3.2 Contrast and Comparison Attacks

In text steganography, there are two ways of contrast attack [7]. First, contradictions between a profile of users and a URL/webpage subject which an adversary may look for. Such, contradictions reveal the fact of an unmatched subject of URL and its user profiles as discussed in traffic attack. This can be a sign of using steganographic tools. URL-Stega scheme is resilient against such attack by establishing a covert channel that guarantees to match the user profiles to a webpage subject. Second, another type of contradictions may exist in the text, and an adversary may try to look for them only inside a text-cover. This is unlike the first type of contradictions where the text is compared to its user profiles. When a piece of text contains this type of contradictions, most likely the text is incoherent. Whether or not a URL-Cover contains contradictions in its textual URL, suspicion will not be triggered because a URL is not intended to be read. In other words, a URL is not a text that obeys linguistics rules such as syntax and grammar as such it is not intended to be read or contain information. This is a strong natural immunity for URL-Cover against contrast attack.

Unlike contrast attack, comparison-attack attempts to detect alterations in an authenticated text. To emphasize, an adversary's goal is to employ comparison-attack to find any modifications between the original text and the target-text that may reveal the manipulation of content to embed a message. For example, if an adversary compares an article to its original and detects alteration, it implies a steganographic tool was used. However, comparison attack cannot be used against the presented approach because URL-Cover is not a textual document like a news article that can be subject to alteration. Therefore, URL-Cover is naturally resistant against comparison attack too.

3.3 Linguistics Attacks

Linguistic examination distinguishes the text that is under attack from normal human language which can be done via inspecting the meaning, syntax, lexicon, rhetoric, semantic, coherence, and any other features that can help in detecting or suspecting the existence of a hidden message. These examinations are used to determine whether or not the text under investigation is normal. Obviously, the URL is a type of text that link users to a webpage, and it is not an informative text to be read. No one pays attention to such text (URL). Conversely, everyone will pay attention to the contents of a webpage rather than its URL. This is a common behavior of all Internet users due to the fact that there is nothing to be read in a web-address itself. A web-address (URL) may contain weird text, as shown in Figure 1, which will ease the generating process of URL-Cover and help legitimize it. This is very noticeable in looking to a number of web-links. For example, when searching the web, the URL of the search result will contain abnormal text. In this paper, a text abnormality means that a text neither obeys linguistic syntax nor correct spelling of any legitimate languages. Generally, in text steganography when detecting noise (text abnormality) the goal of steganography is defeated regardless of whether or not a plaintext is revealed. However, this is not the case in the URL-Stega because it is very common and legitimate that the URL contains such abnormality which makes web-link an attractive steganographic carrier for concealing data.

The text used in URL is a different type of text that follows only the rules of URI rather than following the rules of normal language like syntax, grammar, and so on. Investigating the textual URL-Cover should be based on the rules of URI such as the permissible characters, as shown in Table 1. URL-Stega methodology requires the implementation process to obey all the rules of URI. One may say a wrong web-link that violates the rules of URI can also be used because there are so many users that send, receive, and attempt to access incorrect web-addresses. However, this may trigger suspicion because it is not a common practice to frequently use a wrong web-link. Additionally, when using incorrect web-link, the detection of violating URI's rules can easily be achieved. URL-Cover does not use sophisticated text, and it is easy for such scheme to retain the textual normality according to URI rules. Yet, there is no linguistic structure to be obeyed in URL and thus it does not generate any noise

(linguistic flaws). As a result, the generated cover is normal text, as demonstrated in the implementation section. Therefore, URL-Stega is capable of passing any linguistic attack by both human and machine examinations.

However, a statistical attack tracks a profile of the text used. A statistical signature (profile) of a text may refer to the frequency of words and characters used. An adversary may use the statistical profile of a particular topic for documents that contains no hidden message and compares it to a statistical profile of the suspected URL-Cover to detect any differences. An alteration in the statistical signature of a particular document may be a possible way of detecting a noise that an adversary would watch for. Unlike image steganography, tracking statistical signatures is an ineffective means for attacking textual steganography [7, 10, 25]. Nonetheless, URL-Stega is resistant to statistical attacks because it uses legitimate textual URL that is generated based on URI rules. In addition, the generated textual cover (URL-Cover) retains the same profile of its peers' text that contains no hidden message. Basically, most alterations introduced by URL-Stega are nonlinguistic and do not produce any flaws (noise), as demonstrated in the implementation section. As a result, statistical attacks on URL-Cover is ineffective.

3.4 Bitrates

The aim of this section is to evaluate the presented URL-Stega bitrate to contemporary textual steganography approaches. The bitrate is defined as the size of the hidden message relative to the size of the cover. The average bitrate of the presented URL-Stega system used in this paper is roughly between 39.47% and 75.0%. It is worth noting that the bitrate may differ from one element to another and from one implementation to another, as observed. To put this bitrate figure in perspective, the bitrate of contemporary textual steganography approaches has been investigated and for more information refer to [7]. Tables 5 and 6 summarize the findings of the bitrate and categorize them based on the pursued approaches.

Table 5: The bitrate of URL-Cover with and without shortening it

Tool Name for Shorting the URL	Bitrate
Without shorting the URL	39.47%
Google URL Shortener [24]	75.0%
Bitly [4]	71.42%
Ow.ly via Hootsuite [29]	62.5%
TinyURL by Gilby [32]	53.57%

Table 6: The bitrate of contemporary textual steganography approaches other than Nostega-based approach as discussed in [7]

Approach	Bitrate
Mimic functions	0.90%
NICETEXT	0.29%
Winstein	0.5%
Murphy et al.	0.30%
Nakagawa et al.	0.034%
Translation-based	0.33%
Confusing	0.35%

4 Conclusion

The high demand of using the Internet by a wide variety of people makes it feasible for communicating parties to establish a covert channel for transmitting hidden messages (URL-Cover). Thus, URL is an attractive steganographic carrier. Such features motivated the development of the URL-Based Steganography Methodology (URL-Stega). URL-Stega conceals data only in legitimate textual URL/web-address. URL-Stega neither hides data in a noise (errors) nor produces noise. Instead, it camouflages data by exploiting elements that are allowed by URI rules, such as alphabet, numeric, alphanumeric, abbreviation, words, and other legible URL characters in order to construct a URL-Cover that looks innocent. The bitrate of the presented implementation in this paper is roughly about 39.47% and up to 75.0%. This bitrate is superior to all other contemporary text steganography approaches found in the literature and it confirms the effectiveness of URL-Stega. The steganalysis validation shows that URL-Stega methodology is capable of achieving the steganographic goal.

References

[1] T. Berners-Lee, L. Masinter, M. McCahill, *Uniform Resource Locators (URL)*, RFC 1738, Dec. 1994. (`https://tools.ietf.org/html/rfc1738`)

[2] T. Berners-Lee, R. Fielding, L. Masinter, *Uniform Resource Identifiers (URI): Generic Syntax*, RFC 2396, Aug. 1998. (`https://tools.ietf.org/html/rfc2396`)

[3] T. Berners-Lee, R. Fielding, L. Masinter, *Uniform Resource Identifier (URI): Generic Syntax*, RFC 3986, Jan. 2005. (`https://tools.ietf.org/html/rfc3986`)

[4] Bitly, *Harness Every Click, Tap And Swipe*, June 23, 2018. (`https://bitly.com`)

[5] M. Chapman, G. I. Davida, "Plausible deniability using automated linguistic steganography," in *International Conference on Infrastructure Security (In-*

fraSec'02), Lecture Notes in Computer Science, vol. 2437, pp. 276-287, 2002.

[6] CheckShortURL, *URL Checker*, June 23, 2018. (`http://www.checkshorturl.com`)

[7] A. Desoky, *Noiseless Steganography: The Key to Covert Communications*, Information Security Publisher/CRC Press/Taylor & Francis Group, 2016.

[8] A. Desoky, "Comprehensive linguistic steganography survey," *International Journal of Information and Computer Security*, vol. 4, no. 2, pp. 164-197, 2010.

[9] A. Desoky, "Nostega: A novel noiseless steganography paradigm," *Journal of Digital Forensic Practice*, vol. 2, no. 3, pp. 132-139, Mar. 2008.

[10] A. Desoky, *Nostega: A Novel Noiseless Steganography Paradigm*, Ph.D. Dissertation, University of Maryland, Baltimore County, May 2009.

[11] A. Desoky, "Sumstega: Summarization-based steganography methodology," *International Journal of Information and Computer Security*, vol. 4, no. 3, pp. 234-263, 2011.

[12] A. Desoky, *et al.*, "Auto-summarization-based steganography," in *Proceedings of the 5th IEEE International Conference on Innovations in Information Technology*, Dec. 2008.

[13] A. Desoky, "Listega: List-based steganography methodology," *International Journal of Information Security*, vol. 8, no. 4, pp. 247–261, 2009.

[14] A. Desoky, " Notestega: Notes-based steganography methodology," *Information Security Journal: A Global Perspective*, vol. 18, no. 4, pp. 178-193, Jan. 2009.

[15] A. Desoky, "Matlist: Mature linguistic steganography methodology," *Journal of Security and Communication Networks*, vol. 4, no. 6, pp. 697-718, 2011.

[16] A. Desoky, "NORMALS: Normal linguistic steganography methodology," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 3, pp. 145-171, 2010.

[17] A. Desoky, "Edustega: An education-centric steganography methodology," *International Journal of Security and Networks*, vol. 6, no. 2/3, pp. 153-173, 2011.

[18] A. Desoky, "Headstega: E-mail-headers-based steganography methodology," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 4, pp. 289-310, 2010.

[19] A. Desoky, "Jokestega: Automatic joke generation based steganography," *International Journal of Security and Networks*, vol. 7, no. 3/4, pp. 148-160, 2012.

[20] A. Desoky, "Innocipher: A novel innocent-cipher-based cryptography paradigm - High level of security for fooling the enemy," *Information Security Journal*, vol. 22 , no. 2, 2013.

[21] A. Desoky, M. Younis, "Graphstega: Graph steganography methodology," *Journal of Digital Forensic Practice*, vol. 2, no. 1, pp. 27-36, Jan. 2008.

[22] A. Desoky and M. Younis, "Chestega: Chess steganography methodology," *Journal of Security and Communication Networks*, vol. 2, no. 6, pp. 555-566, Mar. 2009.

[23] GetLinkinfo, *URL Checker*, June 23, 2018. (`http://getlinkinfo.com`)

[24] Google, *Google URL Shortener*, June 23, 2018. (`https://goo.gl`)

[25] C. Grothoff, *et al.*, "Translation-based steganography," in *Proceedings of Information Hiding Workshop (IH'05)*, pp. 213-233, June 2005.

[26] T. G. Handel, M. T. Sandford, "Data hiding in the OSI network model," in *First International Workshop, Proceedings on Information Hiding*, Lecture Notes in Computer Science, vol. 1174, Springer, pp. 23-38, 1996.

[27] MailChimp, *What's behind that short link?*, June 23, 2018. (`http://unfurlr.com`)

[28] A. Martin, G. Sapiro, G. Seroussi, "Is image steganography natural?" *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2040-2050, Dec. 2005.

[29] Ow.ly via Hootsuite, *Ow.ly: Now Inside the Hootsuite Dashboard*, June 23, 2018. (`http://ow.ly`)

[30] SecuriTeam, *ScramDisk - Disk Encryption Tool*, Jan. 4, 2000. (`http://www.securiteam.com/tools/5VP011F0BY.html`)

[31] M. Shirali-Shahreza, *et al.*, "Text Steganography in SMS," in *International Conference on Convergence Information Technology*, pp. 2260-2265, Nov. 2007.

[32] TinyURL by Gilby, June 23, 2018. (`http://tinyurl.com` and `http://www.gilby.com`)

[33] M. Topkara, U. Topkara, and M. J. Atallah, "Information hiding through errors: A confusing approach," in *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*, Jan. 2007.

[34] Unshorten.It, *URL Checker*, June 23, 2018. (`https://unshorten.it`)

[35] URL X-ray, *URL Checker*, June 23, 2018. (`http://urlxray.com`)

[36] P. Wayner, "Mimic functions," *Cryptologia*, vol. 16, no. 3, pp. 193-214, 1992.

Biography

Dr. Abdelrahman Desoky is an associate professor at Claflin University. He is an experienced scientist researcher and educator at both the graduate and undergraduate level with over twenty years of IT experience in the academic and industrial sectors. Dr. Desoky received a Doctoral Degree (Ph.D.) from the University of Maryland, Baltimore County, and a Master of Science (M.Sc.) from the George Washington University; both degrees are in Computer Engineering. His Doctoral Dissertation is entitled Nostega: A Novel Noiseless Steganography Paradigm. The paradigm explores the topic of Noiseless Steganography, which refers to the science and

art of covert communications. Nostega provides a way to secure information in static stage and during data transmission to a legitimate recipient. His M.Sc. degree concentrated on Computer Architecture and Networks, with research focusing on Security Architecture for Computers and Networks. He is the author of security book entitled "Noiseless Steganography: The key of Covert Communications".

Application of Artificial Intelligence Technology in Computer Network Security

Jialiang Zhang
(Corresponding author: Jialiang Zhang)
Criminal Investigation Police University of China, Shenyang, Liaoning, 110854, China
No. 83-21-212, Tawan Street, Huanggu district, Shenyang, Liaoning, 110854, China
(Email: zhangjl_vip@sina.com)
(Received; revised and accepted)

Abstract

Since the 21st century, the degree of informatization has been greatly accelerated, which has brought great convenience to people's life. Moreover the problem of computer network security has become a crucial point in the development of information technology. How to protect network security and safeguard their own rights and interests are the problems faced by network security. Artificial intelligence technology is also developing with the progress of information technology. This study proposed the application of artificial intelligence in computer safety protection by combining artificial intelligence with computer network security. Artificial intelligence based Trojan horse detection model was established and tested. The experimental results demonstrated that the proposed artificial intelligence model could accurately and rapidly detect out Trojan horse program, with a low false alarm rate and missing alarm rate, suggesting favorable performance. This work provides a reference for the application of artificial intelligence technology in computer network security.

Keywords: Artificial intelligence; Computer network security; Trojan horse detection

1 Introduction

Artificial intelligence, a branch of computer science, is a new technical science which focuses on developing theories, methods, technologies and application systems for simulating, extending and expanding human intelligence [3, 27]. The technology can operate computer by simulating the intelligence of multiple people to make it solve and analyze problems like human. Artificial intelligence technology has been widely used in various fields, and scholars in various countries have conducted considerable research on it. Liao *et al.* [13] applied artificial intelligence technology in the medical field to help nurses solve problems and guide nursing. It was found through investigation that the heterogeneity of artificial intelligence technology in nursing diagnosis was 87%, suggesting a high applicability in the medical field. Wang [28] explored the application of artificial intelligence technology in intelligent video surveillance system, established artificial intelligence technology based image surveillance system, and explained the feasibility and advancement of the system through verification. Network is extremely developed currently; however there are many threats such as virus on the Internet. How to prevent those threats has been the primary problem.

Morel [16] considered that network security needed to be based on artificial intelligent technology. He also advocated focusing on Web application security in practice and controlling the possibilities of false positive and false negative using knowledge based system, probabilistic reasoning and Bayesian updating. Demertzis and Iliadis [7] proposed a network based online system for network security protection. The system analyzed the basic characteristics of network traffic with the minimum computing power to find the existence and types of potential network abnormalities and identified Packed Executable with the minimum computing power and resource to find the existence of malicious software. Ling *et al.* [14] proposed a model built on AdjointVM. The model is a virtual computer with the ability of double circular chain intrusion detection which can block the invasion of attacker. In this study, artificial intelligence was analyzed and applied in network safety protection; the way how to combine artificial intelligence and computer network security was proposed. This work provides a reference for the application of artificial intelligence in network security.

2 Artificial Intelligence Technology

Artificial intelligence technology mainly aims at studying and developing simulation of human brain, i.e. developing artificial intelligence systems which can operate artifi-

cial intelligence behaviors through computer according to human body intelligent activity rules [5]. Artificial intelligence technology involving many subjects and theories including linguistics, computer science and neurology is a subject with high comprehensive level [12]. Application of artificial intelligence technology in practice should coordinate with other subjects to achieve the combination of theory and technology and generate intelligence technologies that imitate human brain.

Artificial intelligence technology has four major characteristics. The first characteristic is favorable fuzzy information processing capacity. Compared to other computer technologies, it was better in processing fuzzy information [4]. The second characteristic is strong collaboration ability. Artificial intelligence divides network security management into three levels, and managers at the higher level should monitor managers at the lower level. Such a complete monitoring system greatly enhances the collaboration ability of network security defense. Next is good learning and nonlinear processing ability. It can learn during information mining. The current network is complex and changes constantly. Many unexpected matters may happen during network security management, which makes computer network a nonlinear control object [20]. The last characteristic is low computational cost. Calculation tasks can be fulfilled by one time based on optimal solution obtained through control algorithm, which reduces resource consumption and achieves energy conservation [23].

3 Application of Artificial Intelligence Technology in Computer Network Security

3.1 Firewall

Firewall technology is the most extensively applied technology in network security management. It can protect computer network through identifying all activities which may damage the completeness and confidentiality of information [6, 8, 10]. Firewall can guarantee information security. Setting firewall can isolate hostile attacks from Hacker to computer in the internal and external network.

3.2 Anti-virus Technology

Online anti-virus technology based on artificial intelligence can timely discover the invasion of network virus and alarm users to respond timely according to warning messages [17, 21, 22].

3.3 Establishment of Rule Generation Type Expert System

Expert technology is one of the extensively applied artificial intelligence technologies in network security management [2, 15]. Expert system is an invasion detection system designed based on all professional knowledge of experts. Application of expert system can reduce the workload of invasion detection.

3.4 Application of Artificial Neural Network System

Artificial neural network is good at identifying invasion mode which carries noise or is hidden [24]. The system is designed based on the long-term simulation of human brain; hence it has favorable learning ability and strong adaptive capacity and can efficiently identify invasion behaviors.

3.5 Application of Artificial Immunological Technique

Artificial immunological technique, one of artificial intelligence technologies, can simulate a series of defense manifestations produced after human immunity [29]. In computer network management, it can improve the learning ability of natural defense mechanisms, prevent information from invasion by network virus, and effectively protect the integrity and confidentiality of information.

4 The Framework of Trojan Horse Detection Model

Trojan horse virus refers to a kind of virus which controls a computer through specific programs. Generally, Trojan horse virus is divided into two programs, i.e. control site and controlled site. Trojan horse virus is prevalent currently. Unlike other viruses, it will neither multiply nor infect other files on purpose. But it induces users to download through disguise and then provide the channel of the invaded computer for the invader; as a result, the invader can damage or steal users' documents and even control host remotely. General viruses have strong infection ability because of self replication. It multiplies through self replication and spread by taking advantage of the weakness of computer.

Artificial intelligence based Trojan horse detection model classified programs using Bayesian classifier according to program behaviors and Trojan horse behavior features library. The model was mainly composed of program behavior extraction, behavior features library, program behavior analyzer, Trojan horse processor and user negotiation and judgment.

The main function of program behavior extraction was to monitor and record suspicious behaviors in system and send the recorded data to program behavior analyzer. There were suspicious behaviors such as automatic operation of documents, hiding documents and closing

security system when Trojan horse operated. Trojan horse behavior features library included information such as Trojan horse behaviors and its action objects of the

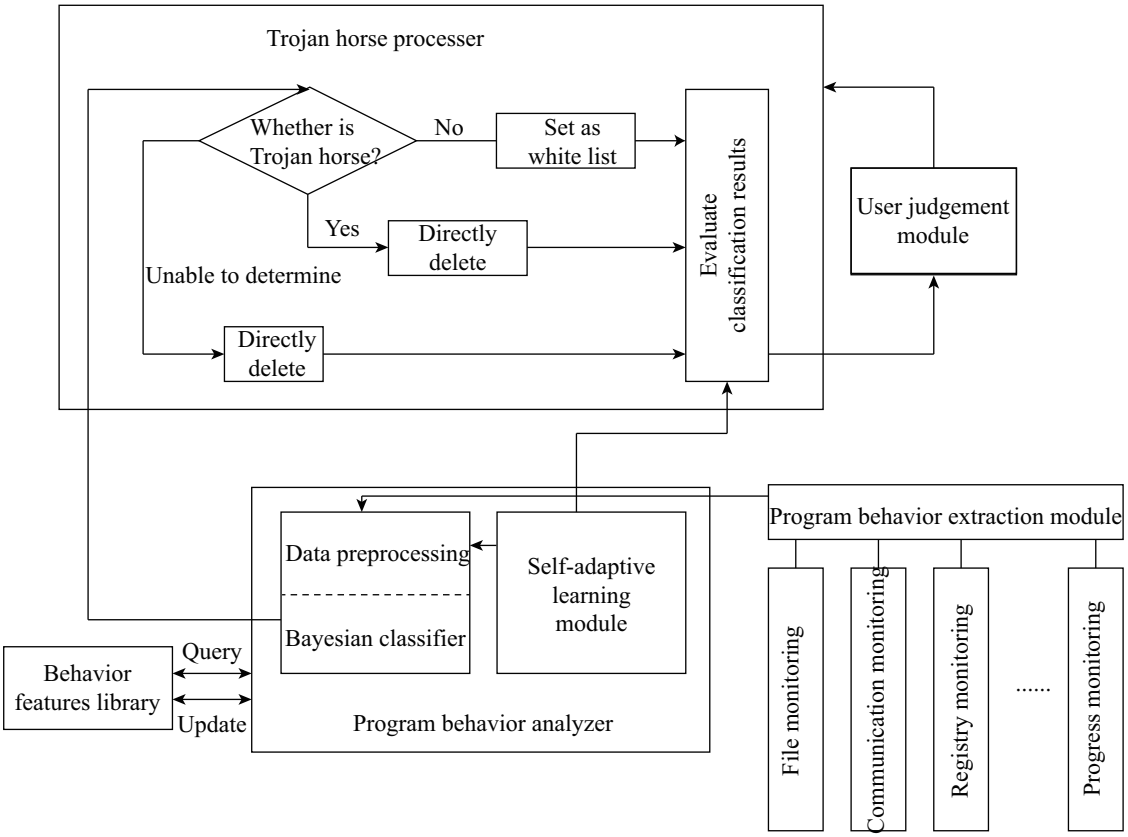


Figure 1: Artificial intelligence based Trojan horse detection model

Table 1: Brief description of behavior analysis module

		Input	**Output**	**Process**
Data preprocessing	Redundancy elimination	Processing feature vector independence	Non-redundant feature set	(1) Calculate feature CRR (2) Eliminate features with low correlation degree
	Feature vector independence processing	Non-redundant feature set	Mutually independent non-redundant feature set	Merge behavior attributes and reduce using SNCB model
	Weight calculation	Mutually independent non-redundant feature set	Feature weight	(1) Assign influence factors (2) Obtain influence degree (3) Calculate weight
Classification calculation		(1) Sample features set (2) Classification algorithm (3) Unknown examples (4) System parameter table	Classification results	(1) Statistical calculation of sample features (2) Extraction of features of examples (3) Classification
Classifier learning		Classification performance table performance table	(1) Feature set table (2) System parameter table	(1) Incremental learning (2) Relearning (2) Relearning

behaviors and a large amount of basic probability information. Program behavior analyzer, an important component of the system, could determine the category of programs using Bayesian classifier and constantly study according to the data provided by the behavior library to enhance its classification ability. In user judgment module, user set a value, and the size of the value determined the category width of the classifier. When the classifier was unable to make correct judgment, then it was processed by users; users processed results using processor after judgment. The main framework is shown in Figure 1.

4.1 Program Behavior Extraction Module

The monitoring and capture of program behaviors should be done inside operating system to achieve the monitoring of file system, registry and system process. In this study, APIHOOK technology was used to intercept the call of system program.

4.2 Behavior Features Database

Behavior characteristics database which included behavior characteristics of Trojan horse and normal program could provide basic evidences for computer classification. It could be divided into characteristic set database and feedback adaptive database. The characteristic set database mainly included characteristic set table, testing features table, parameter table and feature datum table. Feedback adaptive database mainly included classification performance table and system parameter table.

4.3 Behavior Analysis Module

Behavior analysis module had function of data preprocessing, classification calculation and classifier learning (Table 1).

Table 2: Duration of 10 times of detection

No.	Artificial intelligence technology(S)	Traditional technology (S)
1	1.4172	10.2547
2	0.9388	11.1024
3	1.2511	9.0325
4	0.8219	9.6935
5	1.2101	10.5241
6	1.5114	9.9857
7	0.9918	10.2155
8	1.1192	11.0123
9	0.9712	10.3954
10	1.0116	9.9069

4.4 System Response Module

After classification of programs which needs detection, system processing was needed. For example, Trojan horse program needs to be eliminated once abnormal behaviors of Trojan horse were detected out; monitoring stopped if normal program was detected out. When the model was unable to identify a program, then the program was isolated, determined by users, and processed after determination [1, 9, 26].

5 Experimental Results and Analysis

Artificial intelligence technology and the traditional computer network security management technology were tested to compare the network protective efficacy of the two technologies.

Firstly the detection speed of the two technologies was compared; 990 legal programs and 10 Trojan horse viruses. The Trojan horse programs used in this study was from China Hacker Union, and the legal programs were from common software and system files. The detection results are shown in Table 2.

As shown in Table 2, artificial intelligence technology cost no more than 1.5 s for scanning 1000 files, while the traditional technology cost more than 9 s. It indicated that artificial intelligence technology could more effectively and rapidly scan network source files and identify Trojan horse virus, suggesting a great role in the protection of computer network security.

To further test the detectability of artificial intelligent technology, parameter $\delta(\delta > 1)$ was introduced to measure the classification width of the classifier. The larger the value of δ, the smaller the determination scope, the more accurate the result, but the more undecidable situations; the smaller the value of δ, the larger the determination scope, the less undecidable situations, but the less accurate the result. The two technologies were tested by for three times according to different detection width δ. t stands for the number of Trojan horse programs, and n stands for the number of legal programs. The experimental results are shown in Table 3.

It could be seen from Table 3 that the detection effect of the artificial intelligent technology was superior to that of the traditional technology, and moreover the artificial intelligent technology had a low missing alarm rate and false alarm rate, suggesting a favorable performance in detecting Trojan horse viruses. But it should be noticed that the number of unclassified programs increased though the detection rate improved with the increase of δ. Hence the value of δ should not be too large.

With the development of information technology, the crime pattern has also changed, and internet gradually becomes a novel criminal means [25]. The development of network technologies results in the increase of network crimes and the severity of network invasion and attack;

Table 3: Comparison of the two technologies under different detection width

Evaluation index	δ=2, t=100,n=200		δ=8, t=100, n=200		δ=20, t=160, n=180	
	Artificial intelligent technology	The traditional technology	Artificial intelligent technology	The traditional technology	Artificial intelligent technology	The traditional technology
Number of Trojan horse viruses identified	96	82	98	83	158	129
Number of Trojan horse viruses identified as legal programs	4	8	1	9	3	9
Number of legal programs identified as Trojan horse virus	2	6	2	5	1	5
Number of unclassified	2	-	6	-	8	-
Detection rate	96%	82%	98%	83%	98.75%	80.6%
Missing alarm rate	4%	8%	1%	9%	3%	9%
False alarm rate	2%	4.67%	1%	4.67%	1.18%	4.11%
Unclassification rate	0.67%	-	2%	-	2.35%	-

hence stronger network defense systems are needed [19]. Artificial intelligence technology, one kind of computer science, is a technology simulating the thinking process and behaviors of human through computer. It mainly includes the principles of intelligence implementation and the manufacturing of computers which can simulate computer. Nakayamada *et al.* [18] applied artificial intelligence into electron beam lithography modeling and improved the production efficiency and location preciseness through adjusting point spread function. Kang *et al.* [11] introduced the tendency of artificial intelligence technology and applied it in health care, aiming to provide optimal treatment scheme for patients in clinical tests. This study applied artificial intelligence technology into network security management and found that the technology could precisely and rapidly detect virus files in other files.

6 Conclusions

In conclusion, artificial intelligence has strong fuzzy information processing ability, collaboration ability, learning ability, nonlinear processing ability and cost few resources in calculation. Based on artificial intelligence, this study proposed a Trojan horse detection model. The model could rapidly and accurately detect Trojan horse virus. The experiment suggested that the model could precisely find out Trojan horse viruses in a short time while defending computer network security, with a low missing alarm rate and false alarm rate. This work provides a reference for the application of artificial intelligence technology in computer network security management.

References

[1] A. A. Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116–123, 2017.

[2] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud security using Markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96-106, 2018.

[3] M. Anderson, R. Bartk, J. S. Brownstein, *et al.*, "Reports of the workshops of the thirty-first AAAI conference on artificial intelligence," *AI Magazine*, vol. 38, no. 3, pp. 72-82, 2017.

[4] C. Bhargava, V. K. Banga, and Y. Singh, "Reliability Comp arison of a fabricated humidity sensor using various artificial intelligence techniques," *International Journal of Performability Engineering*, vol. 13, no. 5, pp. 577-586, 2017.

[5] A. Bundy, *Preparing for the Future of Artificial Intelligence*, Penny Hill Press, 2016.

[6] D. Dai, "Human intelligence needs artificial intelligence," *Sensors*, vol. 5855, no. 3, pp. 95-99, 2018.

[7] K. Demertzis and L. Iliadis, *Hybrid Artificial Intelligence System for Cyber Security*, Apr. 2014. (`file:///C:/Users/user/Downloads/bioHAIFCS.pdf`)

[8] C. Huang and C. Wang, "Network security situation awareness based on the optimized dynamic wavelet neural network," *International Journal of Network Security*, vol. 20, no. 3, pp. 593-600, 2018.

[9] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[10] M. S. Hwang, C. T. Li, J. J. Shen, Y. P. Chu, "Challenges in e-government and security of information", *Information & Security: An International Journal*, vol. 15, no. 1, pp. 9–20, 2004.
[11] K. Y. Lee and J. Kim, "Artificial intelligence technology trends and IBM watson references in the medical field," *Korean Medical Education Review*, vol. 18, no. 2, pp. 51-57, 2016.
[12] S. Li, "Handwritten character recognition technology combined with artificial intelligence," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 20, no. 1, pp. 67-178, 2017.
[13] P. H. Liao, P. T. Hsu, W. Chu, and W. C. Chu, "Applying artificial intelligence technology to support decision-making in nursing: A case study in Taiwan," *Health Informatics Journal*, vol. 21, no. 2, pp. 137-148, 2015.
[14] C. H. Ling, W. F. Hsien, and M. S. Hwang, "A double circular chain intrusion detection for cloud computing based on adjointVM approach," *International Journal of Network Security*, vol. 18, no. 2, pp. 397-400, 2016.
[15] Y. Miao, "Fuzzy cognitive map for domain experts with no artificial intelligence expertise," in *International Conference on Control Automation Robotics & Vision*, Singapore, Dec. 2014.
[16] B. Morel, "Artificial intelligence and the future of cybersecurity," in *Proceedings of the 4th ACM workshop on Security and Artificial Intelligence*, pp. 93-98, 2011.
[17] K. Murugan and P. Suresh, "Efficient anomaly intrusion detection using hybrid probabilistic techniques in wireless ad hoc network," *International Journal of Network Security*, vol. 20, no. 4, pp. 730-737, 2018.
[18] N. Nakayamada, R. Nishimura, S. Miura, H. Nomura, and T. Kamikubo, "Electron beam lithographic modeling assisted by artificial intelligence technology," in *Proceedings of Symposium on Photomask and Next-Generation Lithography Mask Technology*, SPIE 10454, 2017.
[19] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.
[20] J. Orozco, Y. Bello, D. Patino, J. Colorado, F. Ruiz, and L. Solaque, "Non linear control of a robotic arm for pipeline reparation," *IEEE Latin American Transaction*, vol. 14, no. 12, pp. 4681-4687, 2017.
[21] A. A. Orunsolu, A. S. Sodiya, A. T. Akinwale, B. I. Olajuwon, M. A. Alaran, O. O. Bamgboye, and O. A. Afolabi, "An empirical evaluation of security tips in phishing prevention: A case study of nigerian banks," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 25-39, 2017.
[22] A. A. Orunsolu, A. S. Sodiya, A. T. Akinwale, B. I. Olajuwon, "An anti-phishing kit scheme for secure web transactions," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 72–86, 2017.
[23] C. Ramirez-Atencia, V. Rodrguez-Fernndez, A. Gonzalez-Pardo, and D. Camacho, "New artificial intelligence approaches for future UAV ground control stations," in *IEEE Congress on Evolutionary Computation*, San Sebastian, Spain, June 2017,
[24] R. Silipo and C. Marchesi, "Artificial neural networks for automatic ECG analysis," *Neural Network*, vol. 96, no. 5, pp. 80-90, 2017.
[25] J. R. Sun, M. L. Shih, and M. S. Hwang, "Cases study and analysis of the court judgement of cybercrimes in Taiwan," *International Journal of Law Crime & Justice*, vol. 43, no. 4, pp. 412-423, 2015.
[26] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.
[27] B. M. Wagman, "Artificial Intelligence and Human Cognition," *Quarterly Review of Biology*, vol. 68, no. 1, pp. 126-131, 2008.
[28] J. J. Wang, "Research on image monitoring system based on artificial intelligence technology," *Agro Food Industry Hi Tech*, vol. 28, no. 1, pp. 1816-1819, 2017.
[29] M. Wang, S. Feng, C. He, Z. Li, and Y. Xue, "An artificial immune system algorithm with social learning and its application in industrial PID controller design," *Mathematical Problems in Engineering*, vol. 2017, no. 3, pp. 1-13, 2017.

Biography

Jialiang Zhang, born in Harbin in the 3rd, January, 1981, has gained the master degree in the field of computer software engineering from Northwestern Polytechnical University, Shaanxi, China. Now he works as a lecturer in National Police University of China, Liaoning, China. His interests of research include computer software, database and network. He has published several papers in different journals of public security colleges. Moreover he won the second prize in the Innovation Competition for College Students in the Ministry of Public Security held in 2017 as an instructor, the second prize in the Education Software Competition held by the Ministry of Education of Liaoning Province held in 2015 and the second prize in the Courseware Competition of Liaoning Province held in 2015.

Detection and Isolation of Wormholes in Mobile Ad-hoc Networks Using Localization Information

Govand Salih Kadir[1] and Ihsan Alshahib Lami[2]
(Corresponding author: Govand Salih Kadir)
Department of Computer Science and Engineering, University of Kurdistan-Hewler[1]
30M Avenue, Erbil, Iraq
Department of Applied Computing, University of Buckingham[2]
Yeomanry House, Hunter St, Buckingham MK18 1EG, United Kingdom
(Email: g.kadir@ukh.edu.krd)
(Received Aug. 25, 2017; revised and accepted Nov. 28, 2017)

Abstract

Mobile Ad-hoc Networks rely on participating nodes to conduct routing duties and forwarding data packets between nodes, mainly due to their limited transmission capabilities. Routing protocols intend to minimize the exchange of information to reduce overhead, which in result leads to lack of knowledge about others beyond the transmission range of a selected path. This creates a perfect environment for wormholes (WHs) to direct the route discovery through themselves and harm the network. This paper proposes an enhancement to the SIMAN (Smart Identification of MANET Nodes) algorithm that facilitates location sharing of nodes within the discovered path and allows source nodes to reject the path if the distance between any two nodes exceeds the transmission capability of the wireless device. Nodes are authenticated through the original identity sharing mechanisms of the SIMAN algorithm applied during the RREP process of the AODV routing protocol.

Keywords: Aodv; Manet; Siman; Wormhole

1 Introduction

MANET emerged as a promising technology offers infrastructure-less networks that do not require central management entities. Current wireless devices, like Smart-phones, can use MANET to create/join a network, exchange data, and quickly disconnect without prior notification or permission. Nodes in MANET take the central role of finding the possible paths between any two or more nodes separated from each other via some distance within the network. These nodes are wireless devices with limited transmission and power capabilities that can sense the neighbors inside their transmission range only [6, 7]. Therefore, to find a path to a specific destination, each node relies on each other to forward packets. Moreover, routing protocols are designed to avoid overhead caused by additional processes that provide further information about the vicinity to preserve the limited resources of nodes inside the network. As a result, it creates a suitable environment for malicious nodes to expose and launch attacks. Wormholes (WH) are one of the dangerous attacks that is hard to detect and prevent due to limited knowledge about the physical location of nodes inside the network. Two or more malicious nodes can cooperate and use a high-speed link between them to win the route discovery and subsequently harm the network [15].

This paper proposes an enhancement to a previously designed algorithm called SIMAN [5].Which is designed to share knowledge about nodes identity inside the discovered path using AODV routing protocol RREP message. This is achieved by calculating two values from Friend nodes IP address (nodes who are known to each other during the initial network set-up and have an IP address with a prime number host part) and then using these two values by any node inside the transmission path to get a list of addresses for previous nodes inside the route to destination. Furthermore, the enhancement replaces nodes reliance on routing tables to retrieve the previous and next nodes address using a mathematical formula to forward packets during data transmission. This concept provides an abstract authentication of nodes inside the transmission path. Additionally, it is used to prevent newly joined unknown nodes called (Bridging nodes) from altering any information passed through the RREP message because they will not be aware of the algorithms existence.

The current enhancement uses location information, obtained from GPS-enabled devices like Smart-phones, to measure the distance between nodes and detect any abnormal distances. Every Friend node attach its coordinates to RREP message and passed it all the way back to the source node. The source node then accepts the discovered route if the distance between nodes is less than the threshold defined according to maximum transmission

characteristics of the wireless environment. Additionally, three Friend nodes cooperate to determine Bridging node coordinates and attach it to the RREP message on their behalf. If the distance between any two nodes inside the discovered path is greater than a pre-determined threshold, the source then rejects the path and start a new route discovery.

The rest of this paper organized as follows: Section 2 explores the recent work done that involves the usage of localization information to improve routing protocol performance and ways of WH attacks prevention. Section 3 explains the proposed algorithm design and Section 4 details the implementation of the algorithm using Riverbed Simulation software. Section 5 examines the simulation results of various scenarios in comparison to AODV routing protocol. Finally, we conclude the achievements obtained through this enhancement and identify the future use of this method in security protocols in Section 6.

2 Literature Review

MANET is restricted by the limited information shared among nodes about the physical location of others inside the network. Sharing such information improves the performance and provides better protection against malicious nodes. Researchers used various approaches toward this goal, in this section, we explore some of these methods used for this purpose.

The Geographical AODV (GeoAODV) is an improvement of the LAR protocol, which uses directed flooding technique with AODV routing protocols. The physical location of nodes is used to reduce the amount of broadcasted route requests messages aimed at a destination node by defining the request zone as an isosceles triangle. Nodes inside the request zone process RREQ messages and share location information, while others outside the zone discard the messages [1].

The same concept of requested and expected zones is used in another research to limit the search area during route discovery. A list added to the route request message, which contains a fourth Nominated Neighbor to rebroadcast. The algorithm partitions the radio transmission range into four zones and restricts the path discovery area to the expected zone. Then chooses one node per zone to forward the RREQ messages [3]. The proposed solutions reduce the route discovery traffic toward saving resources. However, it does not consider applying the zone restriction might lead to overhead and deny essential nodes that provide better alternative paths for data transmission.

In another research work, an On-demand Routing with Coordinates Awareness (ORCA) protocol uses the distance measurement for broadcasting route request messages. The node broadcast the packets to selected neighbors (called relays) using the shortest Euclidean distance to four points in its transmission range. Based on this calculation, the algorithm selects the neighbors closest to these polar points to flood the route requests [17]. The algorithm relies on Hello message to exchange the coordinates and identifiers of a node and its neighbors, which results in creating extra processing that causes overhead, especially in large networks.

Another recent approach, the distance measurement between nodes was used to improve the route stability affected by node mobility. Nodes typically use the RSSI method to quantify the mobility of its neighbors and formulate a method to find the coordinates of nodes when GPS devices do not exist. The method is used as a mobility metric to obtain routes that stay longer, which improves the performance [12]. This concept works better if the distance list was attached to the RREP message, rather than the RREQ, to avoid additional loads on nodes that are not a part of the established path.

The distance measurement between nodes used in another research to confirms the location of neighboring nodes securely in wireless sensor networks [14]. The neighbor verification protocol identifies nodes as true neighbors if the link between four nodes with known distances forms a convex quadrilateral. These nodes exchange location information through what is called a neighbor table, and they use encryption to prevent alteration. The disadvantage of this protocol is the number of operations conducted to exchange data and confirm each other, which creates overhead in addition to the inconsistencies that occur due to 4-clique tests.

Additionally, location information is used to detect and prevent attacks from malicious nodes like WHs. The nodes inside the discovered route measure the distance to the neighbors and share it with others inside the path [2]. The concept of this algorithm can provide knowledge beyond the neighbors of a node, and it requires a mechanism to hide the implementation from WHs because they can defeat the algorithm by merely sharing the wrong distance between them.

Likewise, another technique, called AODV With Wormhole Detection and Prevention (AODVWWDP), is used for WH elimination. This method uses location, hop count and neighboring nodes in a route selection process suggested by AODV. Every node makes sure that the path from neighbor to the node next to neighbor is WH free, by examining different paths and determining if the hop count is greater than a maximum hop count that was calculated earlier [13]. It is not clear in the research how the location helps toward eliminating open attacks from WH nodes, as they act like normal nodes and that can be hard to detect. Furthermore, several hop count calculations cause much overhead that consumes resources. Moreover, it is not clear how the node identifies the node next to neighbors without exchanging further information.

Similarly, the location information was used in another research to detect and prevent WHs by allowing nodes to share their distances from the next node and the next one beyond. This process map nodes inside the path so that the network provide knowledge about the distance

between all nodes [16]. In theory, the algorithm can provide knowledge about all node locations, even those beyond the neighbors, but there is no guarantee that the WHs will not alter this information, which can be a big problem because of a lack of authentication authority.

Another protocol called the distance bounding protocol checks the proximity of two-hop neighbors to verify the physical presence of the node beyond its known neighbors. The round-trip-time for multi-cryptographic challenge-response pairs are used to obtain the upper bound of physical location between two nodes [9]. As discussed earlier, sharing knowledge of nodes beyond its neighbors is crucial to improving the performance of the network, but key-based security solutions used to exchange information adds extra processing that causes overhead and consumes node resources.

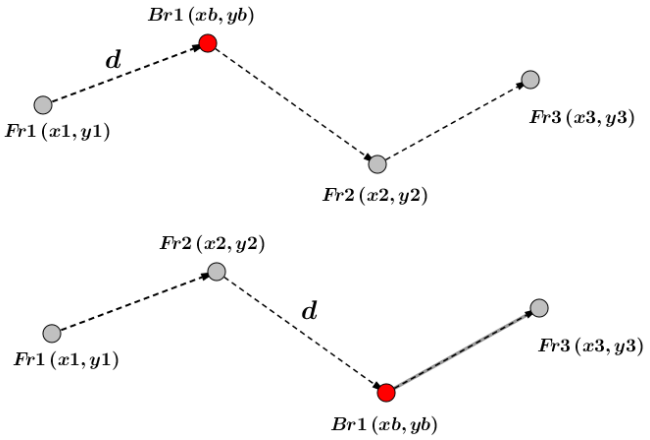


Figure 1: The sequence of friend and bridging nodes in the RREP process

3 Proposed Algorithm

The proposed algorithm is an enhancement of the original SIMAN algorithm, which uses two values generated from the IP addresses of the nodes inside the discovered path that is forwarded using RREP messages. These two values help to share knowledge about nodes identity inside the transmission path. The enhancement adds an extra field to the RREP message that holds a list, which contains the coordinates of the node in 2D obtained from a GPS device.

Each Friend node attaches its coordinates to the extra field added to RREP message, whereas Bridging nodes (earlier assigned prime ID by previous Friend nodes) are not involved in this process. Instead, Friend nodes cooperate to find the coordinates of the bridging node. Once the source node receives the RREP message, it uses the list of coordinates to measure the distance between nodes inside the discovered path and rejects the route if the distance exceeds the wireless transmission threshold. The algorithm is used to detect and isolate WH attacks initiated by malicious nodes hiding their location to take over the transmission path and harm the network. The measurement procedure, which is categorized according to the Friend and Bridging node topology layout, will be explained next.

3.1 Coordinate Measurement

1) If the procedure is between two Friend nodes (Fr), then the calculation will be a simple distance measurement between two points using the coordinate of the Friend attached to RREP.

2) If one of the nodes is a Bridge (Br), then the process requires the cooperation of three neighboring Friend nodes to calculate the coordinates of the Bridging node. The location of the Bridging node creates two different sequences: $\mathrm{Fr1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr3}$ and $\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3}$ as shown in Figure 1. Two different calculation tracks are used for different node

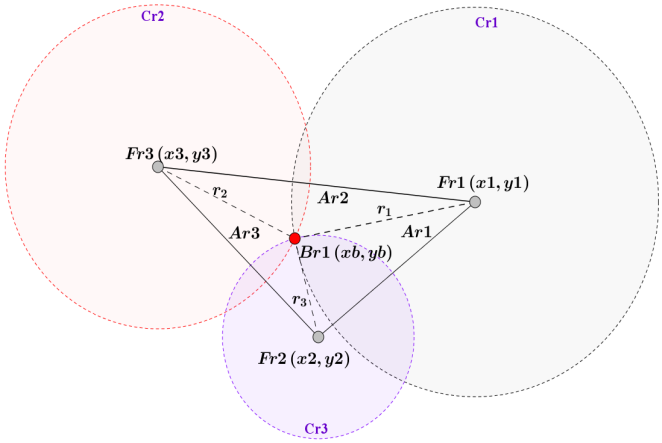


Figure 2: Three-circle intersection used to calculate bridging node location

sequences based on the location of the bridge node Br1 that can be inside or outside the triangle (Fr1, Fr2 and Fr3) as illustrated in Figure 2.

First track: If the Bridging node is located inside the triangle (Fr1, Fr2 and Fr3), then the intersection of the three circles theory will be used to calculate the coordinates (radical centre) [10]. Afterword, the resulting coordinates will be used to calculate the area of the three triangles (Ar1, Ar2 and Ar3). The sum of these areas should be equal to the area of the triangle (Fr1, Fr2 and Fr3) using the Pythagorean Theorem. The coordinates of the bridging node calculated using Equations (1) and (2) for the intersection of the three circles (Trilateration Estimation) [11]. Lets assume that:

$$A = ({y_3}^2 - {y_2}^2), B = ({x_3}^2 - {x_2}^2), C = ({r_2}^2 - {r_3}^2)$$

$$D = ({y_2}^2 - {y_1}^2), E = ({x_2}^2 - {x_1}^2), F = ({r_1}^2 - {r_2}^2)$$

Then

$$x_b = \frac{y_m[A+B+C] - y_n[D+E+F]}{2[x_m * y_n - x_n * y_m]} \quad (1)$$

and

$$A' = ({x_3}^2 - {x_2}^2), B' = ({y_3}^2 - {y_2}^2)$$

$$D' = ({x_2}^2 - {x_1}^2), E' = ({y_2}^2 - {y_1}^2)$$

Then

$$y_b = \frac{x_m[A'+B'+C] - x_n[D'+E'+F']}{2[y_m * x_n - y_n * x_m]} \quad (2)$$

The coordinate values then used to find the area of the three inner triangles (Fr1, Br1 and Fr2), (Fr1, Br1 and Fr3) and (Fr2, Br1 and Fr3) which is calculated using the determinant of three points (shoelace formula) as in Equation (3).

$$Tr_{area} = \frac{|x_1y_2 + x_2y_3 - x_3y_1 - x_2y_1 - x_3y_2 - x_2y_3|}{2} \quad (3)$$

The sum of these areas should equal the area of the main triangle (Fr1, Fr2 and Fr3) that contains them as in Equation (4).

$$Area_{main} = Ar_1 + Ar_2 + Ar_3 \quad (4)$$

Second track: Considering the two node sequences explained earlier as Fr1 → Fr2 → Br1 → Fr3 and Fr1 → Br1 → Fr2 → Fr3. The distance between the two outer Friend nodes (Fr1 and Fr3) represents the radius of two circles that intersect at two points. One of these two points represents the correct coordinates of the Bridging node as seen in Figure 3.

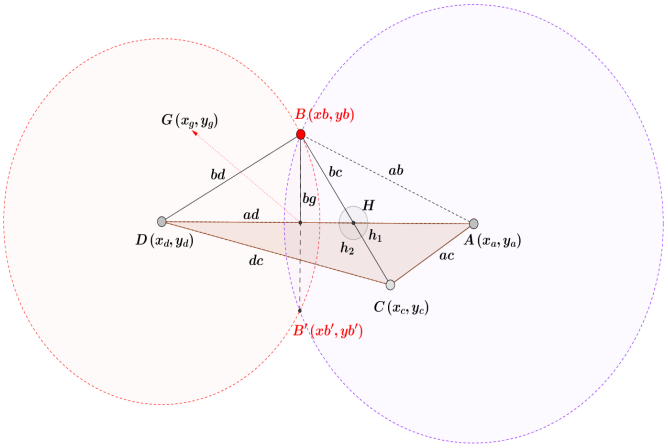


Figure 3: The distance between nodes (A, B and A, C) represents the radius of two circles

The following mathematical procedure will be used to find the actual coordinates of node B.

- The rules of sine and cosine used to derive the formulas used to find the length of the radius of the two circles as in Equations (5) and (6).

Law of Sine:

$$\frac{\bar{cd}}{\sin A} = \frac{\bar{ad}}{\sin C} = \frac{\bar{ac}}{\sin D} \quad (5)$$

Law of Cosine:

$$\bar{cd}^2 = \bar{ad}^2 + \bar{ac}^2 - 2 * \bar{ad} * \bar{ac} * \cos A \quad (6)$$

$$\bar{ac}^2 = \bar{ad}^2 + \bar{cd}^2 - 2 * \bar{ad} * \bar{cd} * \cos D$$

$$\bar{ad}^2 = \bar{cd}^2 + \bar{ac}^2 - 2 * \bar{cd} * \bar{ac} * \cos C$$

- The two radii are then used to calculate the intersection points B and B' of the radical line as in Equations (7) and (8).

$$x_b = x_g \pm \frac{\bar{bg}(y_d - y_a)}{2 * \bar{ad}} \quad (7)$$

$$y_b = y_g \pm \frac{\bar{bg}(x_d - x_a)}{2 * \bar{ad}} \quad (8)$$

- Finally, two different methods used to find the area of the triangle ABD.
  - The first method applies Heron's formula, seen in Equation (9).
    Assuming:
    $M = (\bar{ab} + \bar{ad} + \bar{bd}), N = (-\bar{ab} + \bar{ad} + \bar{bd}),$
    $P = (\bar{ab} - \bar{ad} + \bar{bd})\ and\ Q = (\bar{ab} + \bar{ad} - \bar{bd})$

$$Area = \frac{\sqrt{M * N * P * Q}}{4} \quad (9)$$

  - The second method applies the shoelace formula previously explained in Equation (3), and the result of one of the two points B and B' should yield an equal area as in Equation (10).

$$Area_{(Sides)} = Area_{(Coordinates)} \quad (10)$$

3) It is possible for two consecutive Bridging nodes to come one after another inside the path. The Friend node located after them can detect this, by comparing the hop count with the factor list items. The coordinate measurement for this case is accomplished in two stages. First, by computing the first Bridging node coordinates and then by using the discovered values for the other Bridging node.

4) Lastly, a particular case in which the path between the source and destination contains only two Bridging nodes, and as explained before the coordinates measurement require three Friend nodes. Therefore, when the Source node discovers this case, it creates a false RREQ to one of its neighboring Friend nodes. Once the source node receives the RREP back, it retrieves the coordinates of the Friend node and uses it to compute the coordinates of the Bridging nodes, using the previously explained procedure.

3.2 The Route Discovery

1) RREQ process: During the initial route discovery, the RREQ procedure is the same as in AODV routing protocol. Later when the source receives the RREP, if it detects an unusual distance between two nodes during the measurement process, then it rejects the route and starts a new route discovery.

   This procedure requires a mechanism to prevent the RREQ from following the same path by informing the Friend nodes inside the path to reject packets forwarded to them from nodes with surpassed distance. Therefore, two extra fields added to the RREQ message. The first field is called the S-list, which contains the list of rejected nodes. The second field is called the S-Flag, which is used to inform the other Friend nodes to distinguish it from initial RREQ.

   Once the RREQ is broadcasted, Friend nodes check the S-Flag field, and if it is set, then the node compares the address inside the S-list with preceding node. If a match is found, then it discard the packet otherwise, rebroadcast the RREQ.

2) RREP process: In this process, an extra field is added to the message format to hold the list of coordinates.

   - The destination node starts the process, by adding its coordinates and forward the RREP message to the previous node. Every Friend node receives the RREP repeat the same process as in Figure 4(1).
   - Bridging nodes are not aware of the algorithm, so they use AODV to process the RREP message shown in Figure 4(2).
   - When a Friend node receives the message from a Bridging node, it first checks the number of Friend nodes, preceding the Bridging node:
     - If there was two, then it starts the calculation using (Fr1 → Br1 → Fr2 → Fr3) otherwise, forwards this task to the next Friend node as in Figure 4(3).
     - If there was no other Friend node (i.e. The Friend node itself is the source), then it sends a special RREQ to another neighboring Friend node to get additional coordinates, which is required to measure between coordinates using the sequence (Fr1 → Fr2 → Br1 → Fr3) as in Figure 4(4).

   Assuming there were two Friend nodes before the Bridging node, then the next step is to check for the number of Bridging nodes by comparing the hop count with the factor list items [4]. If they were equal, then the one-step coordinate calculation is used. Otherwise, it uses the two-step procedure as seen in Figure 4(5).

   - If a Friend node received the RREP message and found that a Bridging node is without coordinates, then it will process it using (Fr1 → Fr2 → Br1 → Fr3) as in Figure 4(6).
   - This procedure continues until the RREP reaches the source node, which starts the distance measurement between nodes as seen in Figure 4(7).
   - If the distance between any two nodes exceeds the wireless transmission capability of devices, then the route is rejected, and the address of the nodes added to S-list of the RREQ. Otherwise, the route is accepted, and the source starts data transmission.

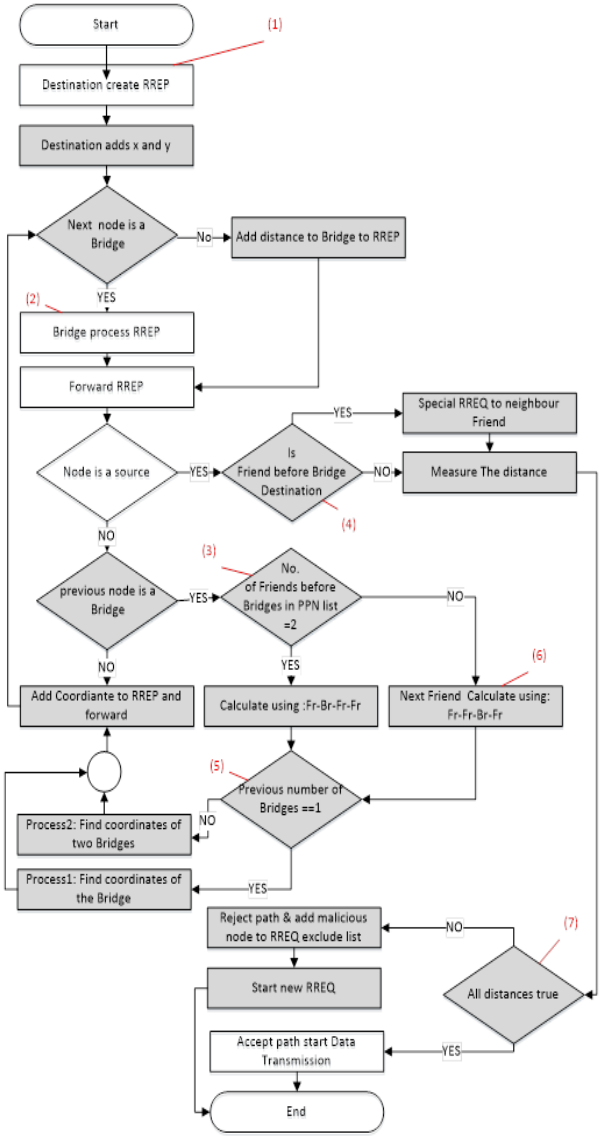


Figure 4: The RREP process for SIMAN and coordinates measurement

3) Wormhole attack detection: The example in Figure 5 demonstrates how the explained technique is used to eliminate different WH types. The network consists of ten Friend nodes, and eight Bridging nodes two of them 7 and 17 are WH nodes. The source node 3

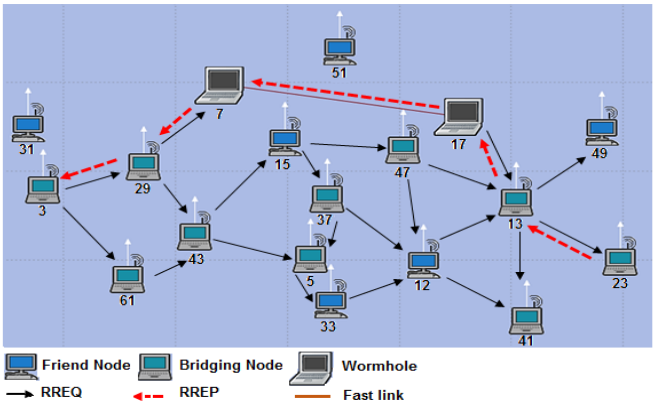


Figure 5: MANET scenario with two WH nodes

wants to send data to destination node 23, and for this purpose, it broadcasts a RREQ message. The two WH nodes make efforts to win the shortest path by processing packets quickly using their Ethernet connection (line connects two black laptops), and the attack comes in three types.

Closed WH attack: Both WH nodes in this attack are invisible/hidden, and any packet passed to them is copied to the output and forwarded to the next node without change. The algorithm detects this attack through the following procedure.

- The initial RREQ process is broadcasted by source node 3 using the AODV routing protocol.
- WH nodes 7 and 17 copy the content of the RREQ message to the output and forward it intact. Therefore, Friend nodes 29 and 13 think they are neighbors.
- Once the destination node 23 receives the RREQ, it creates the RREP message and add its coordinates, then forward the RREP.
- Friend nodes 13 and 29, respectively receive the RREP, and add their coordinates and forward it to the previous node.
- Upon the arrival of the RREP message, the source node measures the distance between nodes and realises the distance between Friend nodes 13 and 29 exceed the threshold, therefore rejects the route.
- Then it creates a new RREQ, and adds the two Friend node addresses to the S-list and sets the S-flag field.
- When both Friend nodes 13 and 29 discover their addresses in the S-list, they reject the RREQ and mark the path between them as invalid since they are not neighbors.

Half open WH attack: In this attack, one of the WH nodes is hidden (node 7), so it does not participate in the routing process, while the other WH (node 17) uses the AODV routing protocol and acts as a normal node. The algorithm detects the attack through the following procedure.

- WH node 7 copies the content of the RREP message received from node 17 to the output and forwards it to Friend node 29.
- Friend node 29 realise that two other Friend nodes 13 and 23 located before the Bridging nodes. Therefore, it uses one-step Bridging node with sequence $(\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3})$ to measure the coordinates.
- Friend 29 is unaware of WH 7 as the latter copies the content of the message to the output, so the hop count remains unchanged.
- Next, source node 3 receives the RREP, measures the distance between nodes inside the path, and discovers the abnormal distance between nodes 29 and 17. Therefore, it rejects the route and starts a new RREQ process by adding the address of 29 and 17 to the S-list.
- The RREQ propagates, and when Friend node 29 detects its address and WH node 17 in the S-list, inside the new RREQ, it drops the RREQ and marks the path with node 17 as invalid.
- In this way, the route that passes through WH node 17 rejected, and the node is eliminated from future routing process.

Open WH attack: When both WH nodes are visible, they act like normal nodes, in terms of processing and forwarding routing packets. The following steps show how the detection procedure is accomplished.

- The WH node 17 forwards the RREP message using the Fast Ethernet link, to WH node 7, which in turn forwards the RREP to the Friend node 29 using its wireless interface.
- When Friend node 29 receives the RREP, it executes the following steps:
  - Find the node addresses in the factor list and discovers that Friend nodes 13 and 23 located before the Bridging nodes, therefore, it executes $(\mathrm{Fr1} \rightarrow \mathrm{Br1} \rightarrow \mathrm{Fr2} \rightarrow \mathrm{Fr3})$ sequence measurement.
  - Compares the number of nodes in the factor list (3 hops) with a hop count (4 hops) and discovers that two Bridging nodes come one after another. Therefore, it uses the two-step measurement.
- When the source node receives the RREP message, it calculates the distance and detects the abnormal distance between WH nodes 7 and 17. Therefore, it rejects the route and starts a new RREQ process with WH nodes in S-list.

4 Algorithm Simulation

In this section, the enhanced algorithm is implemented to MANET nodes using Riverbed (OPNET) simulation software to examine the elimination of the WH and the performance of the network under attack.

The scenario consists of ten Friend nodes with six Bridging nodes (12, 15, 31, 33, 49, 51) and two WH nodes (nodes 7 and 17). Two Friend nodes 3 and 23 have raw data to exchange in both directions, as in Figure 5. Then the scenario is modified to have five different layouts, and nodes are placed randomly at various distances with a fixed data rate of 24Mbps. The full characteristics of the scenarios shown in Table 1.

Several simulations for the scenario are executed to compare the AODV and the enhanced SIMAN algorithm performance under three types of WH node attacks.

Riverbed's IP route report used to collect results that shows the number of hops and its sequence inside the established path. Furthermore, The RDT (Route Discovery Time) and End-to-end-delay for both algorithm simulation measured using various metrics like (Data rate, the distance between two node and topology layouts) to observe the impact of WH elimination on the performance.

Table 1: Simulation scenario parameters

Parameter		Value
Trajectory		Random mobility way-point Movement range: 2000m * 2000m
Distance between two node	- Nodes7 and 17 - Other Nodes	>300m <300m
Data rate	-Nodes7 and 17 - scenario-1 - scenario-2	Outbound (24Mbps), inbound (100-BaseT Ethernet link) 1,2,6,9,12,18,24 and 36 Mbps 24 Mbps
Packet size		512 Byte
Packet reception power threshold		-82.65 dBm
Transmission power		0.005 Watt
Active route time-out		3 sec
Buffer time-out		2 sec
Traffic		500MB, all explicit
Simulation Duration		300 sec

5 Results and Analysis

5.1 Route Discovery Analysis

Simulations were executed for various type of WH attacks for both AODV and SIMAN. The purpose was to examine the successful elimination of WH nodes by the enhanced SIMAN algorithm, through the number and the identity of hops involved in the process as in Figure 6.

Initially, the scenario was simulated without WHs using AODV to compare with results when the WH is introduced. The route report for IP traffic flow (blue dotted arrow) shows a 7 hops path (the nodes 3, 5, 12, 13, 23, 29, 43), and the distance between any two consecutive nodes is (225.4, 238.07, 251.8, 265.6, 272.8, 273.7) meters, respectively.

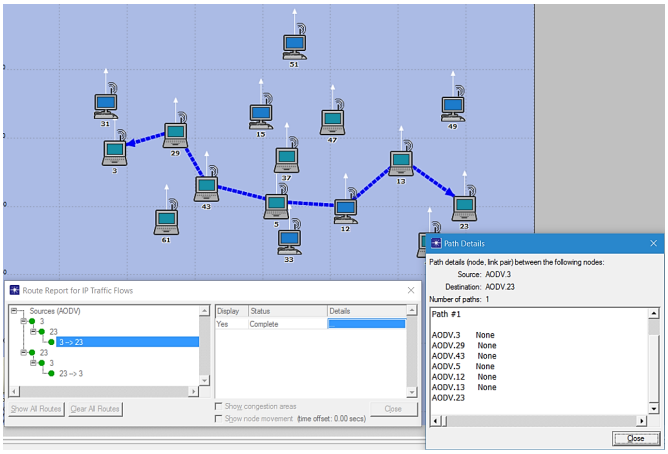


Figure 6: AODV route discovery without WH attack

Open WH attack: The simulation then was repeated for AODV with two visible WH nodes, and the result shows that the WHs managed to divert the route discovery using 6-hop paths (the nodes 3, 7, 13, 17, 23, 29) as illustrated in Figure 7. Using the coordinates values for the nodes inside the path, the distance between neighboring nodes was (238.07, 234.7, 544.1, 253.4, 272.8) meters, respectively.

Using the coordinate values for the nodes inside the path, the distance between neighboring nodes was (234.7, 238.07, 253.4, 272.8, 544.1) meters, respectively. The distance between the two WH nodes, 7 and 17, is 544.1m, which exceeds the maximum threshold distance between wireless nodes [8]. Then, the scenario was simulated again for the SIMAN algorithm, and the result shows that the same original path seen in Figure 6 was established before introducing the WH. Which means the algorithm managed to prevent the two nodes from winning the path, as shown in Figure 8.

Half open WH attack: Afterwards, one of the WHs (node 7) was made hidden to forward the packets

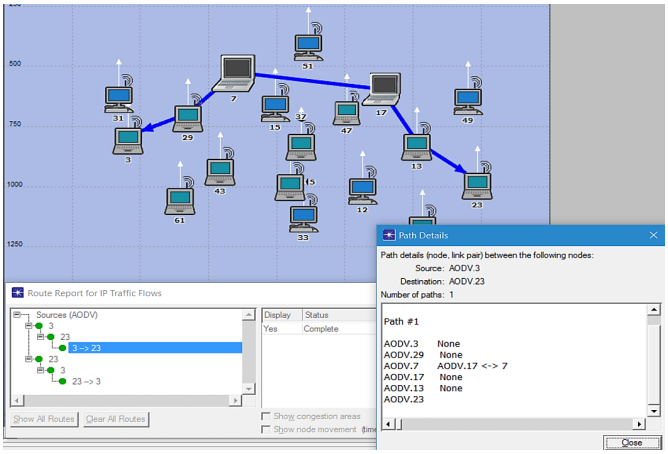


Figure 7: AODV route discovery with open WH attack

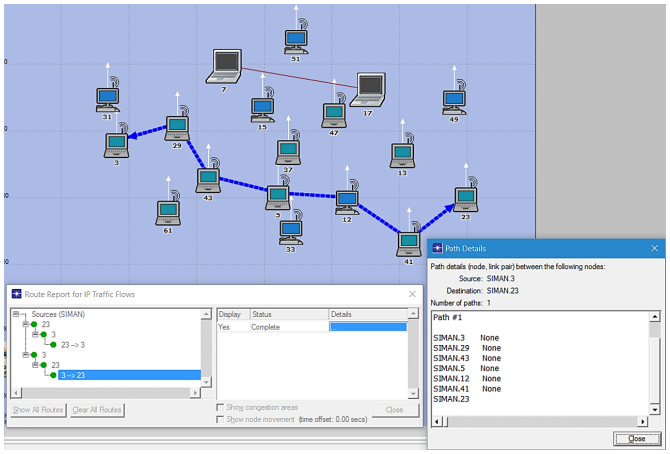


Figure 8: SIMAN route discovery with open WH attack

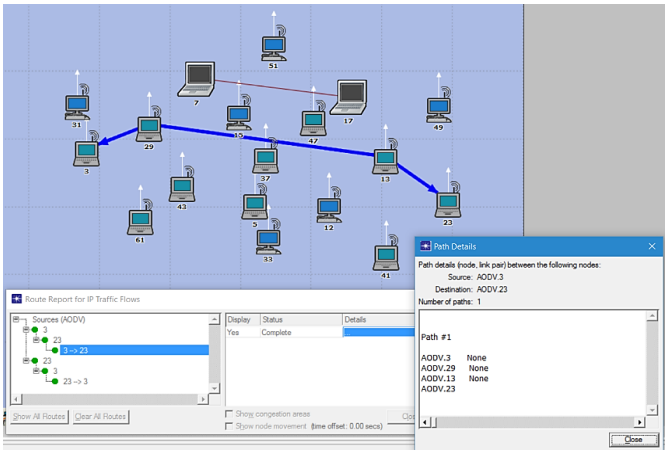


Figure 10: AODV route discovery with closed WH attack

received from Friend node 29 straight to the visible WH node 17 without any change. Then WH node 17 processes the packet using AODV routing protocol. The route report for AODV shows the path consists of 5 hops (nodes 3, 13, 17, 23, 29) as in Figure 9, with distances (238.07, 234.7, 713.7, 253.4, 272.8) meters, respectively. We note that the distance between the Friend node 29 and node 17 is 713.8 meter, which is an indication of hidden WH nodes existence. Subsequently, the same simulation was repeated for SIMAN, in which the outcome was the same as previously established paths seen in Figure 8.

Closed WH attack: In the next simulation, both WH nodes were hidden, so Friend nodes 29 and 13 assumed they are neighbors. The result of the AODV routing protocol shows a path consists of 4 hops (nodes 3, 13, 23, 29) as seen in Figure 10. The distances between these nodes are (238.07, 846.4, 253.4, and 272.8) meters, respectively. We note that the distance between the Friend nodes 29 and 13 exceeds the maximum transmission distance of two nodes (846.4 meters), which indicates the existence of hidden WH nodes inside the path. After that, the simulation was repeated for the SIMAN algorithm, and the result shows that SIMAN managed to eliminate the WH nodes, and used the same route as the previous simulations in Figure 8.

5.2 Route Discovery Time (RDT)

Represents the average round trip time required to receive a RREP message from the destination successfully. The next simulation measured the RDT for both AODV and SIMAN algorithm for various data rates and topology layouts for the three types of WH attacks:

1) Various Data Rates: The RDT results, seen in Figure 11, shows that it took SIMAN 1.28 sec on average more to establish the path in comparison to AODV. Because of the second route discovery process, as the first attempt was rejected because of WH nodes.

   Furthermore, the RDT in both algorithms increased for the open WH attack because the WH nodes need

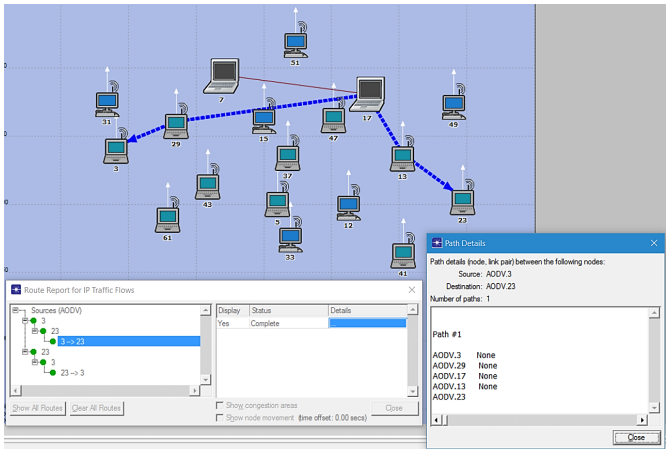


Figure 9: AODV route discovery with half-open WH attack

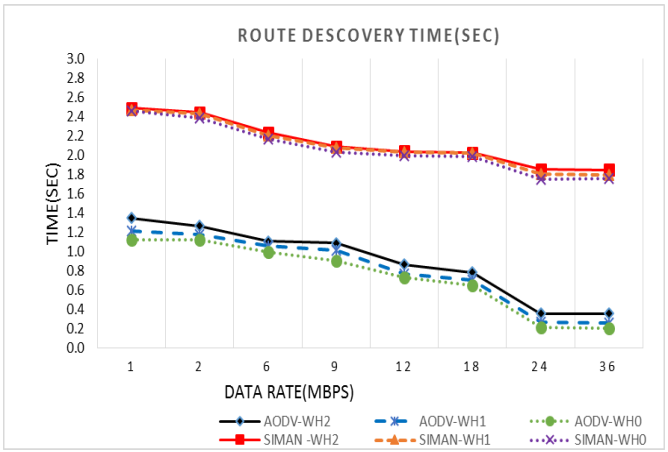


Figure 11: RDT with various data rates

to process packets rather than just forwarding them as in a close attack.

2) Various Topology Layouts: Simulation results for five different topology layouts (with WHs placed randomly in different locations) shows that, when using AODV routing protocol, the WH always divert the path inside the network. While for the SIMAN algorithm, the WH nodes are rejected in all topology layouts as detailed in Table 2.

Table 2: Comparison for number of hops in AODV vs. SIMAN for discovered routes in different layouts

Layout	Traffic 3 ←→ 23			
	AODV		SIMAN	
	Hops	Path	Hops	Path
Layout-1	6	3-43-17-7-51-23	7	3-43-33-5-31-47-23
Layout-2	5	3-17-7-51-23	4	3-5-31-23
Layout-3	4	3-7-17-23	7	3-61-29-5-47-41-23
Layout-4	5	3-43-17-7-23	6	3-12-33-31-23
Layout-5	7	3-5-17-7-12-29-23	8	3-13-43-61-47-49-29-23

Additionally, several different factors influence the RDT in the second scenario, as seen in Figure 12.

- In layout, 1 and 5 an increase of 2.89 sec on average in RDT noticed for SIMAN compared to AODV, due to several route discovery attempts conducted by the algorithm to prevent WH nodes from diverting the path. Likewise, one or more Bridging node coordinate calculation (two for layout-1 and one for layout-5) increases the RDT further.
- Moreover, the RDT in layout-2 took an average 2.46 sec more than AODV, despite having 4 hops inside the discovered route. This result represents a particular case (Sec.4 page 4), in which only two Bridging nodes are in the path. Thus, it requires the source node to send a false RREQ to a neighboring Friend node to get the extra coordinates required for the measurement.
- Finally, the SIMAN algorithm in layout-4 has a greater RDT (2.31 sec) compared to AODV. This is due to three Bridging nodes coordinates calculation that increases the processing time.

5.3 End to End Delay

Simulation result shows that WH attack has an impact on the delay encountered during data transmission. This delay is caused by the speed of processing/forwarding packets by WH nodes inside the selected route. As seen in Figure 13, SIMAN has 0.354 sec on average more delay to AODV, which is due to the number of hops inside the path (AODV-5 hops and SIMAN-6 hops). Because of SIMAN prevention of WH nodes from winning the path. Then the End to end delay was measured for the scenario with different topology layouts, and the result shows variable delay measurements for various topology layouts with an average advantage for AODV 0.248 sec. This advantage is due to different hop numbers inside routes and the WH nodes role in AODV to forward packets faster, as it is illustrated in Figure 14.

6 Conclusion and Future Work

In conclusion, the enhanced algorithm managed to use the existing routing protocol processes to share the node coordinates between nodes inside the discovered path. Which in result it helps toward improving the knowledge of the node's physical location inside the network and enabled the source node to reject routes that have unrealistic distances between two nodes.

Additionally, it prevents malicious attacks without using an extra key-based security solution. The results of distance measurements showed the elimination of several types of WHs introduced by a network scenario. This was observed through the RDT and end-to-end delay, which slightly increased due to SIMANs effort to eliminate and avoid WHs in path discovery. Moreover, several different topologies used with WHs placed in various locations. It was evident from the results that they win the path all the time with AODV routing protocols, while in SIMAN algorithm case simulation reports showed different paths constructed to avoids them.

This algorithm can serve as a platform for further research that can enhance MANET operation through helping the intermediate nodes to repair links by tracking and predict the direction of other nodes movement, which can be a valuable addition to the highly dynamic mobile network. Moreover, sharing other information like nodes remaining battery energy can help the source to select routes that last longer by avoiding nodes with critical battery energy.

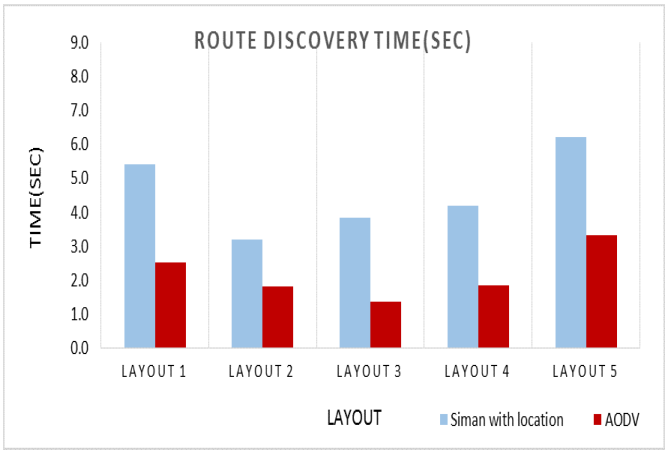


Figure 12: RDT for different topology layouts

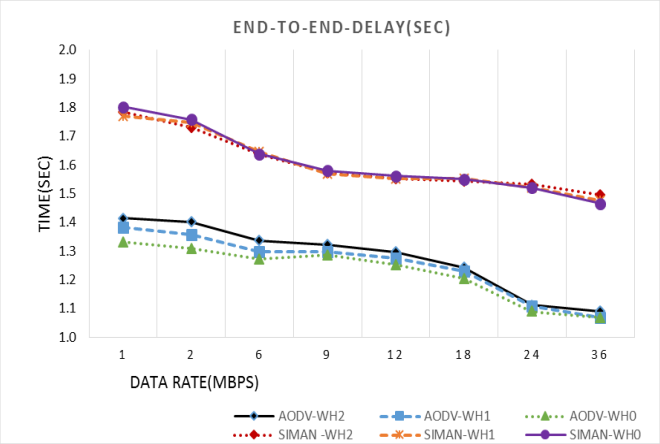


Figure 13: End to end delay for various WH attacks

References

[1] H. Asenov and V. Hnatyshin, "Gps-enhanced aodv routing," in *Proceedings of the International Conference on Wireless Networks (ICWN09)*, pp. 1–7, 2009.

[2] M. Imran, F. A. Khan, T. Jamal and M. H. Durad, "Analysis of detection features for wormhole attacks in manets," *Procedia Computer Science*, vol. 56, pp. 384–390, 2015.

[3] J. Jacob and S. Koyakutty, "An improved flooding scheme for aodv routing protocol in manets," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 3, no. 4, pp. 83–89, 2014.

[4] G. Kadir, T. Kuseler and I. A. Lami, "Smpr: A smartphone based manet using prime numbers to enhance the network-nodes reachability and security of routing protocols," *International Journal of Network Security*, vol. 18, no. 3, pp. 579–589, 2016.

[5] G. Kadir and I. A. Lami, "Siman: A smart identification of manet nodes used by aodv routing algorithm," in *3rd World Congress on Computer Applications and Information Systems (WCCAIS'16)*, pp. 1–7, 2016.

[6] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[7] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[8] Z. Lu and H. Yang, *Unlocking the Power of OPNET Modeler*, Cambridge University Press, 2012.

[9] E. Pagnin, G. Hancke and A. Mitrokotsa, "Using distance-bounding protocols to securely verify the proximity of two-hop neighbors," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1173–1176, 2015.

[10] V. Pierlot and M. V. Droogenbroeck, "A new three object triangulation algorithm for mobile robot positioning," *IEEE Transactions on Robotics*, vol. 30, no. 3, pp. 566–577, 2014.

[11] C. C. Pu, C. H. Pu and H. J. Lee. "Indoor location tracking using received signal strength indicator," in *Emerging Communications for Wireless Sensor Networks*, 2011.

[12] M. Saadoune, A. Hajami and H. Allali, "Distance's quantification algorithm in aodv protocol," *arXiv Preprint arXiv:1411.6320*, 2014.

[13] N. Sahu, D. S. Tomar and N. Pathak, "A modified aodv protocol to detect and prevent the wormhole: A hybrid approach," *International Journal of Computer Science and Network Security*, vol. 15, no. 2, pp. 115, 2015.

[14] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos and J. P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proceedings of the Second ACM Conference on Wireless Network Security*, pp. 193–200, 2009.

[15] A. Shrivastava and R. Dubey, "Wormhole attack in mobile ad-hoc network: A survey," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 293–298, 2015.

[16] B. K. Shrivash and C. Gupta, "A neighbor based efficient worm hole detection and prevention technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, pp. 894–901, 2015.

[17] Y. Wang, C. Westphal and J. J. Garcia-Luna-Aceves, "Using geographical coordinates to attain efficient route signaling in ad hoc networks," in *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'13)*, pp. 1–9, 2013.

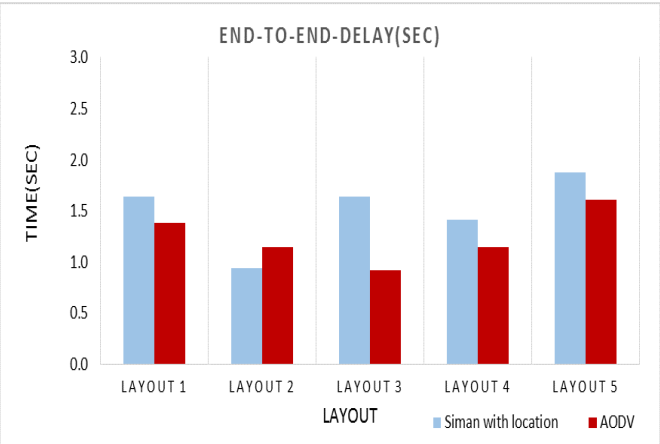


Figure 14: End to End delay for various topology layouts

Biography

Govand Kadir earned his Bachelor of Engineering degree in college of engineering from Baghdad University in 1992. He received his Master of Science degree in in Telecommunication and Computer network engineering in 2006 from London south bank university. In 2017, he completed his Doctoral degree in the Applied Computing Department at The University of Buckingham, UK. Dr. Kadir works since 2007 as a researcher and lecturer for the department of Computer Science and engineering at the University of Kurdistan-Hewler. He is a member of the IT academy sponsored by the council of ministers of Kurdistan regional government of Iraq. Mr Kadir, research focuses on the improvement of routing protocols for Mobile Adhoc Networks and provides protection against malicious devices in these networks.

Ihsan Alshahib Lami is a Reader/Professor in Computer Science at the University of Buckingham, UK. Ihsan worked in Industry for 18 years designing/managing processor and wireless connectivity chips. His current research teams focus on (1) the hybridisation/integration of GNSS and Wireless technologies for optimum localisation and Smart-phone solutions; (2) LTE and Cognitive wireless networks access/security solutions. Please visit http://www.buckingham.ac.uk/directory/dr-ihsan-lami/ for more details.

Security Quantification Method for Intrusion Tolerance Systems Based on Multi-recovery

Jian-Hua Huang, Liang-Jie Chen, Fan-Chao Li and Ze Fang
(Corresponding author: Liang-Jie Chen)

School of Information Science and Engineering, East China University of Science and Technology
No. 130 Meilong Road, Xuhui District, Shanghai, China
(Email: chenxifan1992@sina.cn)
(Received July 27, 2017; revised and accepted Nov. 22, 2017)

Abstract

Nowadays, virtualization has been widely used in the design of application systems. In this paper, we outline the characteristics of an intrusion tolerance system based on virtualization. The semi-Markov process of discrete time is used to model the system. The security of the system is analyzed and evaluated quantitatively from a number of perspectives such as time and space. Some new indicators are proposed to evaluate the security performance of the intrusion tolerance system more comprehensively and appropriately. We present the methods how to calculate the indicators. The simulation results showed that our methods are more accurate and comprehensive than the previous methods in describing the performance of such intrusion tolerance systems.

Keywords: Indicators; Intrusion Tolerance; Quantitative Analysis; Virtualization

1 Introduction

Intrusion tolerance [1, 5] is the popular third-generation network security technology. It assumes that the mission can be completed within a limited time even if there are intrusions in a system. The confidentiality, integrity, and availability of the system are still ensured in case attacks, failures and accidents have occurred. Classic intrusion tolerance models use the Byzantine fault tolerance (BFT) protocol to ensure system security. The BFT protocol requires 3f+1 replicas to ensure the continuality of a service. If attackers have enough time to attack the system, the redundant replicas can always be broken one by one to lead the failure of the intrusion tolerance mechanism. To address the problem, an approach called proactive recovery is used to recover replicas to their pristine states in order to block intrusions. Self-cleaning intrusion tolerance (SCIT) [9] is one of such approaches. In SCIT, the online replica providing a service is periodically forced offline to clean up malwares. A backup replica will go online to provide the service. The offline replica will be cleaned and recovered to a pristine state. Some solutions added intrusion detection mechanism to the system to trigger the reaction recovery. The online replica is immediately forced offline if a malicious intrusion is detected. The combination of the two recovery ways improves the security of self-cleaning intrusion tolerance. With the development of virtualization technology, a replica can be replaced by one instance of virtual machine images. The virtualization technology can quickly generate an instance for accelerating the recovery process and easily provide more replicas. Furthermore, providing several virtual machines in a physical server can reduce the implementation cost for intrusion tolerance and provides better scalability.

The main work of this paper is to analyze the security performance of an improved self-cleaning intrusion tolerance system based on virtualization. The system combines proactive recovery with reactive recovery. But the trigger conditions and recovery strategies of the two recovery methods are quite different. In order to refine the evaluation indicators, we propose MTTPR and MTTRR which correspond to the two recovery mechanisms respectively. Rotation recovery requires to provide backup replicas. We introduce the system virtual machine threshold to ensure the number of required replicas for system services. Instead of the single server level, we calculate the maximum tolerance time at the system level to evaluate the intrusion tolerance ability of the entire system. These security analysis parameters and their evaluation methods aim at evaluating the self-cleaning intrusion tolerance systems based on virtualization from new perspectives.

The rest of the paper is organized as follows. Section 2 briefly describes the relevant work. In Section 3, the semi-Markov model construction is described in detail. Section 4 introduces quantitative evaluation methods. Section 5 analyzes the experimental results. Finally, the summary is concluded in Section 6.

2 Related Work

Since Gong [21] proposed an extended intrusion tolerance distributed service model SITAR, intrusion tolerance gradually entered the people's vision and has been widely concerned. Various types of intrusion tolerance architecture have mushroomed. In 2003, Singh proposed the multi-replicas system of intrusion tolerance [19]. In 2006, Sord proposed the self-cleaning intrusion tolerance model (SCIT) [9]. In 2015, Zhang *et al.* designed an intrusion tolerance architecture for SCADA systems [22]. Nowadays, the intrusion tolerance architectures based on virtualization, such as SOA service architecture [13] and cloud-based SCIT model [14], have been widely used. Marco *et al.* proposed a multiple-replicas system which uses the Byzantine agreement to provide a theoretical basis for SCIT cluster security [18]. Iman *et al.* used the rotation model to serve cloud data centers citeMir2015Security. Georges [17] proposed an attack tolerance model serving for Web applications. Basing on the work, he further designed an intrusion detection and attack tolerance approach called CLARUS for cloud environments [16]. Syrine and Habib used intrusion tolerance in a cloud of databases environment [2, 3].

It is very important to analyze the security performance of intrusion tolerance systems before they are put into use. In order to describe the performance of an intrusion tolerance system better, F. Gong proposed a generic state transition model [6]. He divides the behavior of the system into nine different states. In 2004, Madan [11] *et al.* considered the relationship between the existence time of vulnerabilities and the probability of state transition, and proposed a semi-Markov process (SMP) model based on state transition matrix. They proposed the mean time to security failure as the security measure for evaluating the system. SMP based on state transition can more effectively describe the security attributes of intrusion tolerance systems than previous models. The presentation of MTTSF is of great significance in the security analysis of intrusion tolerance systems, which provides a basis for many researches. Inspired by the SITAR model and the SMP method, many scholars have also proposed their own methods. For example, Yang [8] proposed an evaluation approach based on attack behavior model and introduced the tolerability as a new quantitative indicator. Mir [12] proposed the combination of preventive recovery and the existing SCIT to improve the security of the system. He simulated the behavior of the system through the semi-Markov process, and quantified the cost of a single system recovery. Che [4] proposed a security quantitative analysis method for access control based on security entropy.

The shortcoming of state transition and SMP models is that the state transition probability and the mean sojourn time cannot be accurately determined. To address this problem, Sord used SMP to model SCIT [15] and introduced the concept of exposure window time for more accurate quantitative analysis. Based on this work, Gan [7] proposed a method for calculating evaluation parameters more accurately. This method considered the relationship among the exposure window time, attack success rate and the shielding rate. Luo [10] used SMP to analyse the intrusion tolerance capacity of systems. He proposed a kind of SMP model parameters algorithm. Tanha [20] designed a self-healing control center of critical infrastructures and analysed its security by using SMP.

Although the intrusion tolerance architectures based on virtualization have been well developed, the security evaluation on these architectures still uses several traditional methods. They only consider the states of a single virtual machine, but ignore the effect of recovery mechanism, multi-virtual machines, cluster and other characteristics. In this paper, some new security analysis parameters and evaluation methods are proposed to improve these shortcomings.

3 Intrusion Tolerance Architecture Based on Virtualization

3.1 Architecture

Virtualization technology can simplify software reconfiguration and allow multiple operating systems to run on the same physical platform at the same time. Applications can run in a separate space without affecting each other. The Low-cost and on-demand virtualization technology provides a good distributed environment for self-cleaning intrusion tolerance. The combination of proactive and reactive recovery ways improves the security of the system. Figure 1 shows a virtualization-based self-cleaning intrusion tolerance system combined with proactive and reactive recovery.

In Figure 1, each service implements its intrusion tolerance through self-cleaning mechanism. The Online VM is the primary replica which connects with the outside world via the network. It accepts requests from users and provides the appropriate services. In the architecture, there are two different kinds of recovery methods: proactive recovery and reactive recovery. The proactive recovery will make the online primary replica go offline at regular intervals. It will be replaced by a clean virtual machine to continue to provide services. When the intrusion detection system (IDS) detects a malicious behavior, the reactive recovery will be triggered to force the primary online replica into self-cleaning ahead of time. The interval time that the online replica provides services is called the online time To. If some requests have not yet been completed when the online VM is offline, the online VM has to go into the grace period to process the requests, but not accept any new requests. This period is called the grace time Tg. To and Tg together constitute the exposure time window. If a virtual machine is exposed to the network for a long time, it will be vulnerable to attacks. The virtual machine will go into self-cleaning after the grace period. Self-cleaning include deleting the malware and putting a patch. After the self-clean process,

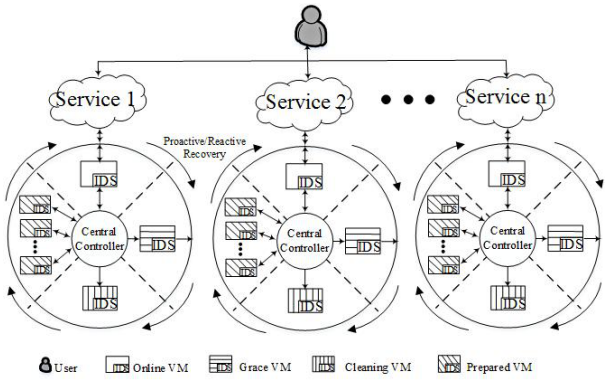


Figure 1: Intrusion tolerance architecture based on virtualization

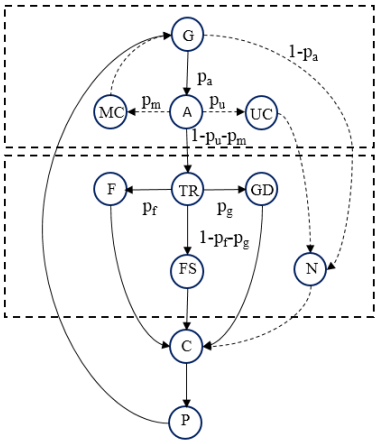


Figure 2: SMP model

the virtual machine is recovered to the initial clean and healthy state and the machine is ready for the next online service. There are several prepared VMs which are ready to go online. The combination of the two recovery methods can not only reduce the possibility of intrusions, but also will respond immediately after an attack. The mechanism improves the overall security of the system.

3.2 Modeling

The state transition model can clearly describe dynamic behaviors and state transition of a system, but it lacks the description of the state transition probability. The Markov process not only describes the states, but also describes the transition probability between adjacent states. Because the sojourn time in each state is associated with the malicious attack frequency, exposure window time, network environment and many other factors, the duration staying in each state is random and not exponential. It is appropriate to use the semi-Markov process of discrete time to describe this kind of self-clean intrusion tolerance system.

Based on the state transition model, this paper presents a semi-Markov state transition model, as shown in Figure 2. This model is used to describe the transition of the various states and the relationships between them. It is also used as a basic framework for quantitative analysis of security.

The states of the analyzed system include good state (G), attack state (A), masked compromised state (MC), normal recovery state (N), undetected compromised state (UC), triage state (TR), failed state (F), graceful degradation state (GD), fail-secure state (FS), self-cleaning (C), prepared state (P). The system is in good state (G) when it starts working. If no attack exists, it will enter the normal recovery state (N) which belongs to the grace period after the online time expires. When the system is attacked, it goes into the attack state A and then the intrusion detection mechanism will go into effect. If the detection mechanism cannot find the attack (minimum probability), the system will go into the undetected compromised state (UC). And it will go into the state N after the online time expires. When the attack is detected, if the system can shield damage through some preventive mechanisms (such as firewalls, repair vulnerabilities, etc.) to make the system unaffected, the system will enter the state MC. Then it will go into good state (G) after damage is completely shielded. Otherwise the system initiates the redundancy mechanism and enters the triage state (TR). Depending on the actual situation and the security policy, the system may choose to only keep the critical service and enter the graceful degradation state (GD). Or the system will stop all services into the fail-secure state (FS) to protect the data confidentiality and reliability. If the system has been significantly damaged and its confidentiality and reliability have failed, then it will enter the failed state (F). Finally, the offline virtual machine will start self-cleaning (state C). The system will enter the prepared state (P) after recovering to a secure and clean state.

States G, A, MC and UC together form the active period in the life cycle of a virtual machine. States TR, F, GD, FS and N form the grace period. States C and P correspond to the self-cleaning and prepared period respectively. The state transition diagram describes the complete life cycle of the virtual machines in detail. It lays a solid foundation for the numerical analysis and evaluation.

4 Quantitative Analysis

4.1 Availability Analysis

Based on the method in [11], system availability can be calculated.

Let $\{X(t) : t \geq 0\}$ be the underlying stochastic process with a discrete state space $X_s = \{G, A, MC, UC, TR, GD, F, FS, N, C, P\}$. To analyze a SMP, we need to determine a sets of parameters:

1) Mean sojourn time h_i in state $i \epsilon X_s$;

2) The transition probabilities p_i between different states $i \epsilon X_s$.

For computing the availability measure, we first need to compute the steady-state probabilities $\{\pi_i, i \epsilon X_s\}$ of the SMP states. π's in turn can be computed in terms of the embedded discrete time Markov chain (DTMC) steady-state probabilities v_i's and the mean sojourn times h_i's:

$$\pi_i = \frac{v_i h_i}{\sum_j v_j h_j}, i, j \epsilon X_s \tag{1}$$

The DTMC steady-state probabilities v_i's can be computed as:

$$\begin{aligned} \bar{v} &= \bar{v} \cdot Q, v \epsilon \{v_G, v_A, v_{MC}, v_{UC}, \\ &\quad v_{TR}, v_{FS}, v_{GD}, v_F, v_N, v_C, v_P\} \end{aligned} \tag{2}$$

Q is the DTMC transition probability matrix which can be written as:

$$Q = \begin{array}{c} \\ G \\ A \\ MC \\ UC \\ TR \\ GD \\ F \\ FS \\ N \\ C \\ P \end{array} \begin{array}{c} \begin{array}{cccccccccccc} G & A & MC & UC & TR & GD & F & FS & N & C & P \end{array} \\ \begin{bmatrix} 0 & p_a & 0 & 0 & 0 & 0 & 0 & 0 & \tilde{p_a} & 0 & 0 \\ 0 & 0 & p_m & p_u & p_{\tilde{mu}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & p_g & p_f & p_{\tilde{gf}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{3}$$

Where $\tilde{p_a} = 1 - p_a, p_{\tilde{mu}} = 1 - p_m - p_u$ and $p_{\tilde{fg}} = 1 - p_f - p_g$. In addition,

$$\sum_i v_i = 1, i \epsilon X_s \tag{4}$$

The transition probability matrix Q describes the DTMC state transition probabilities between the DTMC states as shown in Figure 2. Rewriting Equation (2) into the elemental form yields relationship between DTMC steady-state probabilities as:

$$\begin{aligned} &v_G = v_{MP} + v_P, v_A = v_G p_a, \\ &v_{MC} = v_A p_m = v_G p_a p_m, \\ &v_{UC} = v_A p_u = v_G p_a p_u, \\ &v_{TR} = v_A(1 - p_m - p_u) = v_G p_a(1 - p_m - p_u) \\ &v_{GD} = v_{TR} p_g, v_F = v_{TR} p_f, \\ &v_{FS} = v_{TR}(1 - p_g - p_f), \\ &v_N = v_G(1 - p_a) + v_{UC} = v_G(1 + p_a(p_u - 1)), \\ &v_C = v_P = v_G D + v_F + v_{FS} + v_N = v_G(1 - p_a p_m). \end{aligned} \tag{5}$$

Solving the above equations, in conjunction with the total probability relationship given by Equation (4) we obtain:

$$v_G = \frac{1}{2 + p_a(2 - 3p_m)} \tag{6}$$

Substituting Equation (5) into Equation (6) will yield the expressions for the remaining v's. The states $\{G, A, MC, UC, TR, GD, F, FS, N, C, P\}$ are assumed to have mean sojourn times $\{h_G, h_A, h_{MC}, h_{UC}, h_{TR}, h_{GD}, h_F, h_{FS}, h_N, h_C, h_P\}$, respectively. The SMP steady-state probabilities π's can now be easily computed by using Equation (1). In the case of calculating the steady-state probabilities, the availability of the system can be easily obtained:

$$Availability = 1 - \pi_F - \pi_{FS} - \pi_{GD} \tag{7}$$

4.2 Mean Time to Proactive Recovery and Mean Time to Reactive Recovery

The system presented in this paper has two recovery methods: proactive recovery and reactive recovery. [14] evaluated the recovery-based self-cleaning system by calculating MTTSF. In this paper, the security of the proposed system can be evaluated by calculating the mean time of two recovery methods. We refine the evaluation indicator by calculating mean time to proactive recovery (MTTPR) and mean time to reactive recovery (MTTRR).

Set the state space of proactive recovery method $X_p = \{G, A, MC, UC, N\}$ and the state space of reactive recovery method $Xr = \{G, A, TR, F, GD, FS\}$. The proactive recovery state transition matrix PRM can be obtained:

$$PRM = \begin{array}{c} \\ G \\ A \\ MC \\ UC \\ N \end{array} \begin{array}{c} \begin{array}{ccccc} G & A & MC & UC & N \end{array} \\ \begin{bmatrix} 0 & p_a & 0 & 0 & 1 - p_a \\ 0 & 0 & p_m & p_u & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{8}$$

MTTPR can be calculated as follows:

$$MTTPR = \sum_{i \epsilon X_p} V_i h_i \tag{9}$$

The reactive recovery state transition matrix RRM can be obtained:

$$RRM = \begin{array}{c} \\ G \\ A \\ TR \\ GD \\ F \\ FS \end{array} \begin{array}{c} \begin{array}{cccccc} G & A & TR & GD & F & FS \end{array} \\ \begin{bmatrix} 0 & p_a & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{\tilde{mu}} & 0 & 0 & 0 \\ 0 & 0 & 0 & p_g & p_f & p_{\tilde{gf}} \\ 0 & 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0 & \end{bmatrix} \end{array} \tag{10}$$

MTTRR can be calculated as follows:

$$MTTRR = \sum_{i \epsilon X_r} V_i h_i \tag{11}$$

Where V_i denotes the average number of times which state $i \epsilon X$ is visited before the DTMC reaches one of the absorbing states and hi is the mean sojourn time in state i. The visit count elements V_i can be obtained by solving the following equation:

$$V_i = q_i + \sum_j V_j PRM_{ji}, i, j \epsilon X_p \tag{12}$$

Where q_i is the probability that the DTMC starts in state i. In our case, we assume that G is the initial state, that is, $[q_i] = [1, 0, 0, 0, 0]$.

According to the above formulas, we can calculate MTTPR and MTTRR as:

$$MTTPR = \frac{h_G + p_a h_A + p_a p_m h_{MC} + p_a p_m h_{UC} + (1 - p_a) h_N}{1 - p_a p_m} \quad (13)$$

$$MTTRR = h_G + p_a h_A + p_a(1 - p_m - p_u) * (h_{TR} + p_g h_{GD} + p_f h_F + h_{FS}(1 - p_g - p_f)) \quad (14)$$

If proactive recovery is triggered, it means that there is no malicious attack or malicious attacks are masked before the damage occurs. The system is still in a healthy state. If reactive recovery is triggered, it shows that the system is compromised by malicious attacks and has to force the virtual machine to go offline. We can calculate the ratio of MTTPR and MTTRR:

$$R = \frac{MTTPR}{MTTRR} \quad (15)$$

The higher the ratio R is, the longer the system stays in the proactive recovery cycle. It means that the system is less vulnerable to malicious attacks and more secure. This parameter is important while evaluating the security of the system.

4.3 Virtual Machine Threshold N

Ideally, assuming that the system has an infinite number of virtual machines. Whenever an intrusion occurs, the online virtual machine will be forced to go offline to recover. There will be a clean virtual machine to replace it immediately. Therefore, the entire system can endless rotate and always guarantee services. But the reality is not nearly satisfactory. The number of offline virtual machine replicas may be limited sometimes. This paper introduces the virtual machine threshold N that meets the endless rotation of the system in a given environment.

Assuming that the deal-failure rate of virtual machines is μ, then the duration of the self-cleaning state is $T_C = 1/\mu$. It represents the time from the beginning of the virtual machine offline to the end of self-cleaning. After that the virtual machine is recovered to state P and ready to go online again.

Assuming that the total attack frequency is λ. The attack frequency which causes the system to enter the self-cleaning state is:

$$\lambda_C = \lambda p_a(1 - p_u - p_m) \quad (16)$$

Then the number of the attacks that cause the system to enter the self-cleaning state in time T_C is $\lambda_C T_C$.

Assuming that attacks are independent of each other. When attacks cause the system to enter the self-cleaning state, a new virtual machine must be enabled online. The number N of virtual machines must meet:

$$N \geq \lambda_C T_C + 1 \geq \frac{\lambda p_a(1 - p_u - p_m) + \mu}{\mu} \quad (17)$$

According to literature [15], the online time T_o has a great impact on p_a. The probability distribution of these attack behaviors satisfies the Poisson distribution. Therefore, the attack behaviors and the response of the system are determined as a Poisson process N(t) with a rate of λ. The probability being attacked by k times per unit time is

$$P(X = k) = (\lambda^k / k) e^{-\lambda} \quad (18)$$

The random variable Y denotes the interval between two attacks. It obeys the exponential distribution: $f(t) = \lambda e^{-\lambda t}$. In time t, we get the probability $P(Y \leq t) = 1 - e^{-\lambda t}$. When time t is equal to the online timT_o, $P(Y \leq T_o) = 1 - e^{-\lambda T_o}$. $P(Y \leq T_o)$ indicates the probability that the time interval between two attacks is less than the online time. When the attack frequency is λ, the probability pa that the system is compromised can be replaced by $P(Y \leq T_o)$. Equation (17) can be written as:

$$N \geq \frac{\lambda(1 - e^{-\lambda T_o})(1 - p_u - p_m) + \mu}{\mu} \quad (19)$$

So the ability of systems resisting intrusion in a particular environment can be evaluated by calculating the threshold value N and comparing with the actual number of virtual machines. If the number of virtual machines which the system provides for each service is greater than or equal to N, the system can resist the intrusion for a long time through the rotation mechanism. On the other hand, the smaller the N is, the stronger the resistibility of the system is and the less the resource required is.

4.4 Maximum Tolerance Time T

Assuming that the system does not meet the threshold N. It means that the system cannot provide enough virtual machine resources for rotation. All the virtual machines will enter the self-cleaning state. The system will not be able to continue to guarantee the services and go into the crash state. At this moment the system has to stop the services until the failed virtual machines are recovered. So there exists a maximum tolerance time T. It represents the total time that a system can provide for regular rotation. We can evaluate the persistence of a system against intrusion by the maximum tolerance time T.

When the number of actual virtual machines $n \geq N$ and $T = \infty$, the system can rotate continuously. When $n < N$ and $\lambda_C T \leq n - 1$, the system will not crash. It means that the number of attacks that cause the system to enter the self-cleaning state is less than the total number

of virtual machines. The maximum tolerance time T can be calculated:

$$T \leq \frac{n-1}{\lambda_C} \leq \frac{n-1}{\lambda p_a(1-p_u-p_m)} \tag{20}$$

When the number of actual virtual machines cannot reach the threshold, the constancy of the system to resist intrusion can be evaluated by calculating the maximum tolerance time T. The greater the T is, the stronger the ability for the system to resist the intrusion is.

5 Experimental Evaluation

Now we analyze a typical system with rotation recovery architecture. In this section we illustrate the evaluation of the security attributes through numerical examples. In order to reflect the relationships among the quantification parameters, we use the MATLAB software in the simulation experiment. The parameters involved include the state transition probabilities $p_i, i\epsilon\{A, MC, UC, GD, F\}$, the average sojourn time $h_j, j\epsilon\{G, A, MC, UC, TR, GD, F, FS, N, C, P\}$ and the online time T_o that can be used to express p_a.

5.1 Availability Analysis

Figure 3 shows the relationship between system availability and attack success rate p_a. It compares the model availability presented in this paper with the other two models. Curve 1 represents the rotation-based composite architecture proposed in this paper. Curve 2 represents the classical SCIT [15]. Curve 3 represents the improved SCIT in [12]. The results in the figure show that the availability of the three models decreases with the increase of the attack success rate. It indicates that p_a is the main factor affecting the availability of the system.When the system is in a more secure network environment ($p_a < 0.2$), the availability of our model is more than 0.95. Even in a more malicious network environment ($p_a > 0.8$), the availability can remain at 0.65 or more. This shows that our model has a high degree of tolerance. The availability of the proposed model is overall greater than the other two and the descending speed is slower. It indicates that the ability to deal with the intrusion has been improved. Compared with the other two models, the proposed model has a richer state space. It is the major reason for its performance improvement.

5.2 MTTPR/MTTRR

As shown in Figure 3, in a typical system based on rotation recovery mechanism, the greater the attack success rate p_a is, the more easily the system is compromised. Once the system is compromised and the detection mechanism detects the intrusion, the system will force the virtual machine to be offline for self-cleaning. Proactive recovery is converted to reactive recovery. Subsequently, the corresponding MTTPR will decrease and the MTTRR will increase. It results in a decrease of the ratio R. The higher the ratio R is, the longer the system stays in the proactive recovery cycle. It means that the system is less vulnerable to malicious attacks and more secure. The slope of the curve decreases with the increase of p_a, indicating that the change rates of MTTPR and MTTRR are also decreasing. The ability for the system to tolerate high-intensity intrusion is saturated and stabilized. When $p_a = 1$, the ratio R remains above 0.6. It indicates that the system can still maintain normal rotation under high-intensity intrusion. This parameter is important while evaluating the security of the system. If p_a=0, the system will only use proactive recovery and the ratio R will tend to infinity. Figure 4 only considers the case that the system is attacked. So we set $p_a\epsilon[0.1, 1]$.

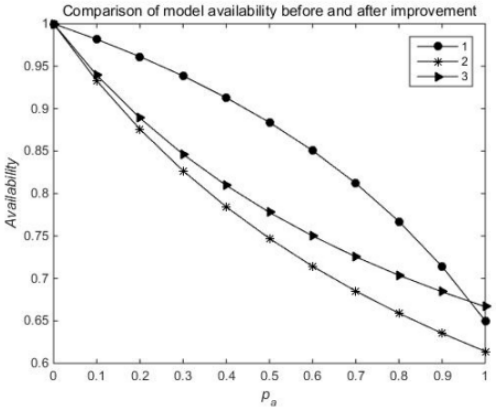


Figure 3: Comparison of model availability before and after improvement

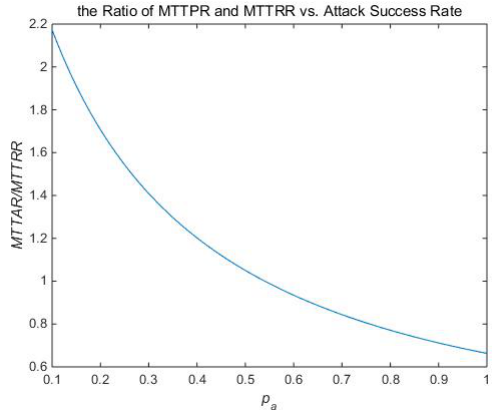


Figure 4: Ratio of MTTPR and MTTRR vs. attack success rate

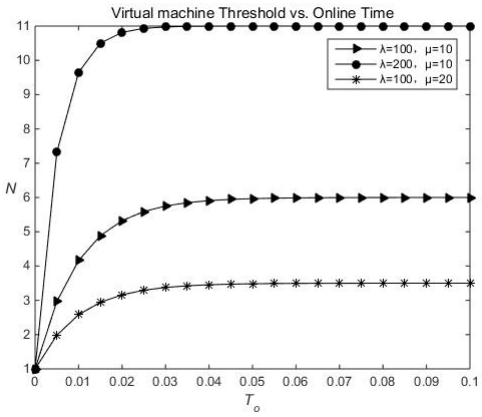


Figure 5: Virtual machine threshold vs. online time

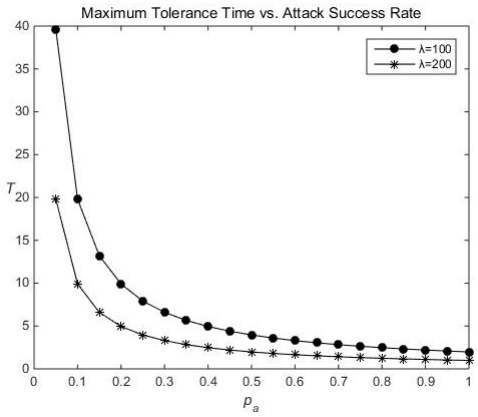


Figure 6: Maximum tolerance time vs. attack success rate

5.3 Threshold N

Figure 5 shows the relationship between the online time and the rotation virtual machines threshold. The following three cases are considered:

1) Attack frequency 100 times/unit time, recovery capacity 10 times/unit time;

2) Attack frequency 200 times/unit time, recovery capacity 10 times/unit time;

3) Attack frequency 100 times/unit time, recovery capacity 20 times/unit time.

With the increasing of online time T_o, the three curves are on the rise. The greater the threshold N is, the more virtual machines are required to ensure rotation. The requirement of virtual machine resources continues to increase. The λ of curve 2 is twice that of curve 1 and the N of curve 2 is always greater than the value of curve 1. It shows that the threshold is related to the attack frequency λ. The higher λ is, the higher the threshold is. It can be seen from the figure that the μ of curve 1 is twice that of curve 3 and the overall trend of curve 1 is greater than curve 3. It shows that the stronger the system recovery capability is, the less virtual machine resources are required. Therefore, in the application environment, the requirement of rotation virtual machines can be reduced by shortening the online time and improving the ability of system recovery.

5.4 Tolerance Time T

Figure 6 shows the relationship between maximum tolerance time and attack success frequency. The following two cases are considered:

1) Attack frequency 100 times/unit time;

2) Attack frequency 200 times/unit time.

Both curves show a downward trend, indicating that the maximum tolerance time T which the system can maintain the regular service will decrease with the attack success frequency pa increasing. The λ of curve 2 is twice that of the curve 1 and the maximum tolerance time T is one-half of curve 1, indicating that the increase of attack frequency will cause the system's tolerance time to drop. The simulation results show that the tolerance time decreases sharply with p_a when p_a is less than 0.5. Because the higher the attack frequency is, the faster the virtual machine rotates. The curve tends to be gentle when pa is greater than 0.5. Because the system's tolerance ability has reached saturation and the tolerance time has been reduced to a minimum. It means that the simulation system is less resistant to intrusion.

6 Conclusion

In view of the self-cleaning intrusion tolerance model based on virtualization, this paper builds a comprehensive SMP model which considers a variety of characteristics: the virtual machine rotation, the self-adaption, the combination of proactive and reactive recovery and etc. We add self-cleaning, prepared and normal recovery states to the model, so the architecture's unique life cycle is described in more detail. Most of the existing evaluation methods only evaluate single virtual machine behaviors and cannot be adapted to the comprehensive system. This paper focuses on modeling and evaluating the entire cluster architecture. We highlight the characteristics of virtual machine rotation from different perspectives such as time and space. The MTTPR, MTTRR, virtual machine threshold and maximum tolerance time are put forward. It enriches the methods of security evaluation of intrusion tolerance systems. The experimental results show that the improved model is more comprehensive to evaluate the security of the system than other models. The proposed indicators give us more way to evaluate the intrusion tolerance capability of the system, which provides a new way for the system security evaluation. But the evaluation process of these parameters needs to be analyzed and perfected by a lot of practice. We need to

further consider the dynamic self-adaptability of virtual machines and the evaluation effect of these parameters in more complex cloud environment. These still need to be resolved in future research.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61472139 and a research Grant made to East China University of Science and Technology by Shanghai Education Commission. The authors are also grateful to the anonymous referees for their insightful and valuable comments and suggestions.

References

[1] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[2] S. Chatti and H. Ounelli, "An intrusion tolerance scheme for a cloud of databases environment," in *International Conference on Network-Based Information Systems*, pp. 474–479, 2016.

[3] S. Chatti and H. Ounelli, "Fault tolerance in a cloud of databases environment," in *International Conference on Advanced Information Networking and Applications Workshops*, pp. 166–171, 2017.

[4] T. W. Che, J. F. Ma, N. Li, and C. Wang, "A security quantitative analysis method for access control based on security entropy," *International Journal of Network Security*, vol. 17, no. 5, pp. 517–521, 2015.

[5] M. Garcia, A. Bessani, I. Gashi, N. Neves, and R. Obelheiro, "Os diversity for intrusion tolerance: Myth or reality?" in *EEE/IFIP 41st International Conference on Dependable Systems and Networks*, pp. 383–394, 2011.

[6] K. Gosevapopstojanova, K. Vaidyanathan, K. Trivedi, F. Wang, R. Wang, F. Gong, and B. Muthusamy, "Characterizing intrusion tolerant systems using a state transition model," in *DARPA Information Survivability Conference and Exposition II (DISCEX'01)*, vol. 2, pp. 211–221, 2001.

[7] J. H. Huang and H. S. Gan, "Quantitative approach to dynamic security of intrusion tolerant systems," *Journal of Computer Applications*, vol. 31, no. 1, pp. 123–126, 2011.

[8] J. H. Huang and T. Y. Yang, "A method for quantifying the security of intrusion tolerant system," in *International Symposium on Computer Network and Multimedia Technology (CNMT'09)*, pp. 1–4, 2009.

[9] Y. Huang, D. Arsenault, and A. Sood, "Incorruptible system self-cleansing for intrusion tolerance," in *IEEE International Conference on Performance, Computing, and Communications Conference (IPCCC'06)*, pp. 490–496, 2006.

[10] Z. Luo, B. You, P. Wang, J. Su, and Y. Liang, "Analysis and optimization of system intrusion tolerance capacity based on markov," *International Journal of Network Security*, vol. 19, no. 6, pp. 1036–1043, 2017.

[11] B. B. Madan, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 1, pp. 167–186, 2004.

[12] I. E. Mir, S. K. Dong, and A. Haqiq, "Security modeling and analysis of a self-cleansing intrusion tolerance technique," in *International Conference on Information Assurance and Security*, pp. 111–117, 2016.

[13] Q. L. Nguyen and A. Sood, "Improving resilience of soa services along space-time dimensions," in *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, pp. 1–6, 2012.

[14] Q. L. Nguyen and A. Sood, "Designing scit architecture pattern in a cloud-based environment," in *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, pp. 123–128, 2011.

[15] Q. L. Nguyen and A. Sood, "Quantitative approach to tuning of a time-based intrusion-tolerant system architecture," in *3rd Workshop Recent Advances on Intrusion-Tolerant Systems*, pp. 132–139, 2009.

[16] G. Ouffoue, A. M. Ortiz, A. R. Cavalli, W. Mallouli, J. Domingoferrer, D. Sanchez, and F. Zaidi, "Intrusion detection and attack tolerance for cloud environments: The clarus approach," in *IEEE International Conference on Distributed Computing Systems Workshops*, pp. 61–66, 2016.

[17] G. Ouffoue, F. Zaidi, A. R. Cavalli, and M. Lallali, "Model-based attack tolerance," in *31st International Conference on Advanced Information Networking and Applications Workshops (WAINA'17)*, pp. 68–73, 2017.

[18] M. Platania, D. Obenshain, T. Tantillo, R. Sharma, and Y. Amir, "Towards a practical survivable intrusion tolerant replication system," in *IEEE International Symposium on Reliable Distributed Systems*, pp. 242–252, 2014.

[19] S. Singh, M. Cukier, and W. H. Sanders, "Probabilistic validation of an intrusion-tolerant replication system," in *International Conference on Dependable Systems and Networks*, pp. 615–624, 2004.

[20] M. Tanha, F. Hashim, and S. Subramaniam, "Secure and self-healing control centers of critical infrastructures using intrusion tolerance," *International Journal of Network Security*, vol. 17, no. 4, pp. 365–382, 2015.

[21] F. Wang, F. Jou, F. Gong, C. Sargor, K. Gosevapopstojanova, and K. Trivedi, "Sitar: A scalable intrusion-tolerant architecture for distributed services," in *Proceedings of DARPA Information Survivability Conference and Exposition*, vol. 2, pp. 153–155, 2003.

[22] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in scada

systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 669–683, 2016.

Biography

Jian-Hua Huang had received the B.S. and M.S. degrees from East China University of Science and Technology, Shanghai,China, and the Ph.D. degree in control theory and control engineering from East China University of Science and Technology, Shanghai,China. He has served as Associate Professor of Computer Science and Engineering at East China University of Science and Technology since 1998. His current research interests include computer networks, wireless sensor networks, information security, data mining, cloud computing, optimization and modeling. Dr. Huang has been a member of various network committees including Specialist Group of Shanghai Education and Research Network and Network Specialized Committee of Shanghai Higher Education Association. He is also the director of Development Center of Shanghai Education Network IPv6 Laboratory.

Liang-Jie Chen had received the B.Eng degree in software engineering from Fuzhou University, Fujian province, China. He is currently pursuing the M.Eng degree in computer science and technology from East China University of Science and Technology, Shanghai, China. His current research interests include intrusion tolerance systems and quantitative analysis.

Fan-Chao Li had received the B.Eng degree in computer science and technology from Nanjing Technology University, Jiangsu province, China. He is currently pursuing the M.Eng degree in computer science and technology from East China University of Science and Technology, Shanghai, China. His current research interests include intrusion tolerance systems and quantitative analysis.

Ze Fang had received the B.Eng degree from Hefei University, Anhui province, China. He is currently pursuing the M.Eng degree in computer science and technology from East China University of Science and Technology, Shanghai, China. His current research interests include intrusion tolerance systems.

Application of Video Watermarking Using Subdivision Technique to Enhance Information Security

Mahesh Gangarde, Janardhan Chitode and Shruti Oza
(Corresponding author: Mahesh Gangarde)
Department of Electronics Engineering, Bharati Vidyapeeth Deemed University College of Engineering
Satara Road, Pune 411043, India
(Email: maheshgangarde@yahoo.co.in, j.chitode@gmail.com)
(Received June 21, 2017; revised and accepted Oct. 21, 2017)

Abstract

This paper proposes an innovative technique of watermark video security using Watermark Sub-Division method. The main objective of this paper is to demonstrate Video Watermark Subdivision Algorithm (VWSA) to secure watermarked secret information. In this algorithm watermarked secret data is subdivided into suitable parts and pixel value of every part is embedded with the same pixel value of a selected frame of video and locates the respective offsets as secret key. At the receiver end the same pixel values are correlated with the Red, Green, Blue (RGB) plane of frames and watermark secret data is recovered based on the amount of correlations achieved. We have applied various types of attacks on watermarked video during transmission and recovered both original video and watermarked secret data without any loss of information. The simulation results demonstrate that the security parameters are improved and the embedded watermark is robust and invisible. Peak Signal to Noise Ratio (PSNR) and Similarity Index (SI) measurable parameters are also calculated to test the quality and matching performance between the original watermark and the extracted watermark to achieve imperceptibility.

Keywords: Attacks; Information Security; Video Watermarking; VWSA

1 Introduction

Nowadays internet plays a very important role in digital multimedia tools like YouTube, Facebook, WhatsApp, Twitter which contain videos for sharing secret information. When such information is sent from the transmitter to the receiver, the major concerns are security of secret watermark data, watermark embedding capacity and good recovery of both original video and watermark secret data. Hence it is always better to provide an information security model to all multimedia [8, 16] tools during transmission. Due to this requirement of digital multimedia, video watermarking can provide a perfect solution for this issue. With today's expanding development of digital multimedia, video watermarking technology plays an important role in copy control, video authentication [3] and copyright protection. Data security is the primary concern when using any media of communication. Our objective is to provide higher data security to protect the watermarked data [1] over the communication channel.

2 Related Work

In 2016, a hybrid algorithm was developed by Kunhu *et al.* which use both DCT and DWT. Index mapping table was used to convert the color watermark logo into the 3 bit index. Then 2-level wavelet decomposition was applied to the selected channel to a particular band which was then divided into 8x8 block and DCT was applied. Then, the location of some coefficients was selected for hiding [8]. Su *et al.* presented a blind watermarking technique which hid the watermark into the blue component of RGB image in the spatial domain. For embedding the watermark, the watermark was divided into four parts and then embedded into different locations of the host image by directly modifying pixel values in the spatial domain [17]. The paper [16] has suggested an effective watermarking technique to secure multimedia data. They explained video watermarking system with image as a watermark using alternative pixels flipped shared under wavelet. In 2008, Do *et al.* gave the concept of digital video watermarking technique using the pixel value histogram watermark which was more robust to camcorder recording attacks and geometric distortions to improve the robustness against geometric synchronization.

To make it imperceptible watermark is adjusted

roughly according to human visual system which shows that proposed technique was more robust to different attacks such as camcorder recording attack and video processing attacks such as MPEG compression. The proposed method was evaluated using different video sequences and it indicates that watermarked video quality is good with average PSNR equal to 45.64dB which is less secure [3]. The paper [2] has suggested the concepts of video watermarking against various attacks using Discrete Wavelet Transform (DWT) technique and Principle Component Analysis (PCA) transform to improve the robustness. The proposed method has applied various attacks on watermarked video to improve the performance against a wide range of attacks with average PSNR equal to 31.65dB and NC equal to 0.8786 which was not correlated to original video, hence it was less secure. Chaluvadi *et al.* has developed an efficient image tamper detection and recovery technique using dual watermarking technique.

The proposed algorithm used two copies of watermark; if one copy is destroyed, watermark is recovered with the other copy of watermark message by embedding more than one bit in 5-MSBs [4, 9]. The result of proposed technique was tested which showed that it is more efficient than Lee and Shingen's method with PSNR 45.85dB [1]. Na Wang *et al.* explained block-based watermarking technique for tamper detection and recovery with color image. In this proposed scheme, RGB channel is divided into blocks and the watermark insertion space is generated by manipulating Least Significant Bit of each targeted block to zero which is used for authentication and recovery codes. Simulation result showed that the proposed technique successfully identified the tampered position and recovered with visual quality with maximum PSNR value of 44.362dB [19]. An efficient video watermarking technique is proposed by Osama based on SVD in DCT domain. In this method video frames are transformed using DWT technique with two resolution levels and error correction code is applied.

In order to increase the robustness, the watermark is embedded with spatial and temporal redundancy [6, 12, 18]. The watermark was tested against different attacks and the proposed watermarking scheme was compared with other schemes [5]. In 2015, Majid *et al.* has presented blind video watermarking technique for verification of ownership using CDMA techniques with binary image as a watermark. In this technique watermark is scattered into different frequency sub-bands of wavelet and during extraction process original video is not required. The proposed technique has good robustness against different video watermarking attacks such as frame dropping, frame averaging and Gaussian noise and evaluated this method with security parameters like PSNR, MSE and SSIM [10]. As video copyright protection is strongly concerned, a robust video watermarking scheme is necessary. In order to design a robust [7], invisible, blind andnon-removable video watermarking scheme, a survey and investigation has been done on multimedia security issues and multimedia watermarking scheme.

Various watermarking scheme are compared and evaluated. Based on these, a new approach and procedures for multimedia security based on watermarking are proposed. At the same time, Sowmya [15] error correcting code is extracted from the video channel and embedded into the audio channel, which provide extra information for recovery of extracted watermark. Shojanazeri and Wan present the state of the art in video watermarking techniques. It provides a critical review on various available techniques. In addition, it addresses the main key performance indicators which include robustness, speed, capacity, fidelity, imperceptibility and computational complexity. The advancement of Internet services and various storage technologies, made video piracy as an increasing problem particularly with the proliferation of media sharing through the internet. This method performed better in JPEG compression of 80% as the PSNR equaled to 37.715dB and the NC for the extracted watermark from LL is 0.983 despite of HH sub band which is 0.162.The PSNR after resize is 41.207dB [13].

2.1 Main Contribution

The main contribution of this paper is to improve concealed watermark secret data security, perceptibility and its robustness. As video is made up of number of still images/frames, we have selected any frame to conceal secret watermark image using VWSA technique. During transmission of watermarked video we have applied five different types of attack on watermarked video and obtained important key security parameters before concealing, after concealing and after recovering from watermarked video. The values of key security parameter like PSNR, NC, MSE, SI and Histogram were not changed and we recovered secret watermark image without any loss of information. Thus it improves security, perceptibility and robustness of proposed security model for video watermarking using VWSA.The rest of the paper is organized as follows. Section 3 indicates proposed video watermarking using VWSA, Section 4 shows key security parameters and its importance and Section 5 gives different attacks on watermarked video, Section 6 indicates simulation results & discussion and in the last section conclusion and references are presented respectively.

3 Proposed Security Model of Video Watermarking

The input to proposed security model is any type of video. The input video is split into number of frames and audio. Before concealing watermark secret data we have divided it into number of small parts and every small part is concealed using VWS algorithm. In this paper, all embedding procedures are explained for single block of watermark secret image. We have obtained major security parameter like PSNR, MSE, NC and histogram of secret watermark

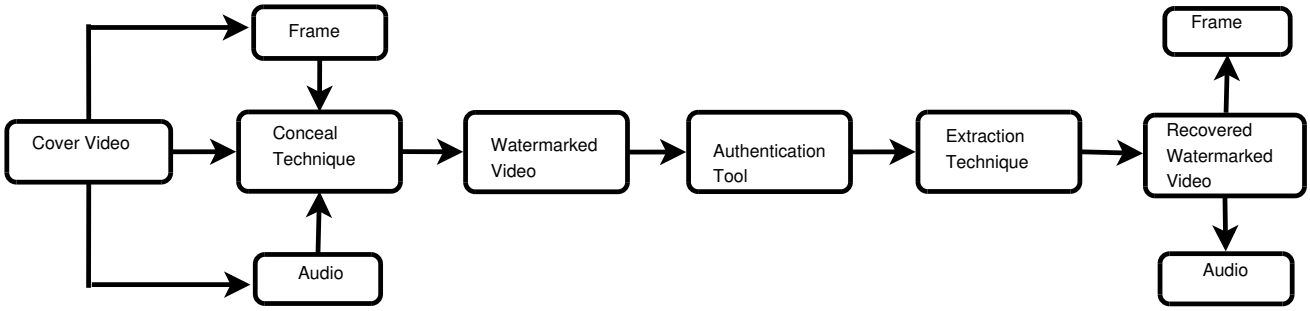


Figure 1: Block diagram of proposed video watermarking security model

data before embedding. Once concealing process has been done, watermarked video is obtained which is sent from transmitter to receiver. Authentication tool is used to cross check the incoming watermarked video in terms of PSNR, MSE, NC and histogram. If these major security parameters are matched with original watermark secret data, then it is sent to the receiver end, otherwise authentication tool stops the incoming watermarked video. We have used secret key which is known to both the parties. After matching the security parameters, authentication tool allows sending authenticate watermark video to receiver with watermark extraction process as shown in Figure 1.

3.1 VWSA for Video Watermarking

To improve the watermarked concealed capacity and security, we have divided secret watermark data into number of blocks and each block is embedded by using key structure. As video contains large number of frames,hence large numbers of locations are available to embed the secret data and hence embedding capacity is increased. When such watermarked video is sent from transmitter to receiver it is very difficult to understand in which frame of video secret watermark data is embedded, hence security of proposed technique is improved. In watermark subdivision technique, pixel values are located on the basis of matching between watermark pixel values and frame pixel values which forms secret key as shown in Figure 2. We have obtained the pixel values from watermark secret image and located those pixel values into selected frames of video to improve the embedding capacity and enhance the security of secret watermark information. The Figure 2 shows the working model of proposed video watermarking algorithm using VWSA technique which improves the conceal capacity and security of secret data. We have considered the color image as watermark data, converted it into its pixel values and found out those pixel values in cover video frame. An example shown in Figure 2, pixel value 5, 0 and 89 matched with frame pixel values by different locations. Record frame number and the locations of matched pixel values between secret watermark image with cover video frame in secret key structure shown in Matrix (d) which is used for higher data security or privacy. Continue this process till the matching of pixel values of watermark image with cover video frames.

3.2 Embedding Procedure with Example

The Algorithm 1 is explained with an example of first frame of cover video of size 8x8 as shown in Matrix (a) and watermark image of size 4x4 as displayed in Matrix (b). Let $w(i,j)$ and $f(i,j)$ be the pixel location in watermark and cover frame respectively. The pixel value at $w(1,1)$ is 251, will be searched row-wise in the selected frame of video. This value is found to be matched at $f(1,3)$ i.e. shown in bold in Matrix (c). So note that frame number and location of $f(1,3)$ in key structure displayed in Matrix (d) which occupies three locations of key structure. First two locations of key structure indicate the size of watermark secret image and the third location indicates the frame. Similarly the next pixel value of watermarked image $w(1,2)$ i.e. 250 will be searched in Matrix (a) and the match is found at $f(4,8)$ then stored respective frame number and pixel location in key structure. If watermarked pixel value is not found in first frame the search it in the next frame and continue. When match is found, the respective frame number and the location of that pixel stored in key structure and so on. Steps 6, 7, and 8 are explained respectively in detail as follows:

If $(f(i,j) == w(i,j))$ Note the frame number and pixel location in key structure elseif $(f(i,j) == (w(i,j)+1))$ Note the frame number and pixel location in key structure elseif$(f(i,j) == (w(i,j) \vee 1))$ Note the frame number and pixel location in key structure.

4 Key Security Parameters and Its Importance

4.1 Similarity Index (SI)

Similarity Index is used to find similarity between two images, the measurement of image quality is based on an initial uncompressed or distortion free image as reference [10]. In the proposed security model, we have obtained SI with respect to original video which is found to be similar to each other hence our proposed method is

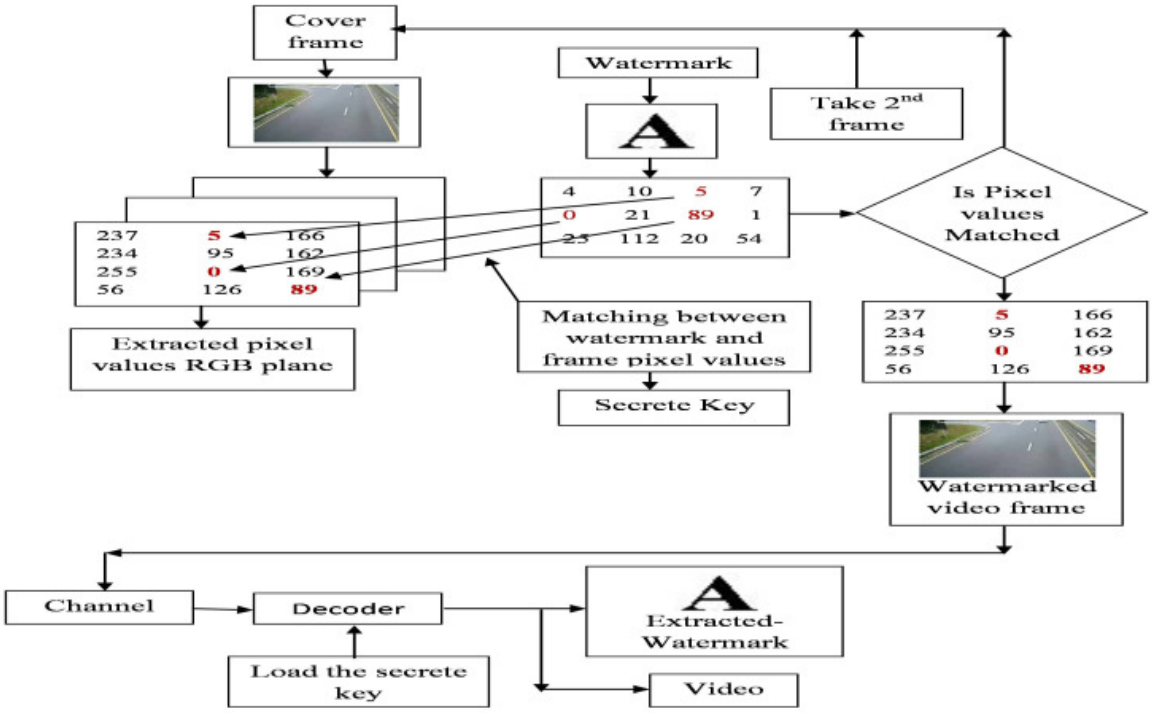


Figure 2: Process of embedding and extracting secret watermark image using VWS algorithm

255	224	251	235	234	245	250	251
168	225	209	215	249	202	238	122
123	231	206	253	251	199	219	215
111	244	236	255	240	200	237	250
125	249	245	250	251	123	231	206
229	251	202	238	122	126	244	236
217	240	199	219	215	125	249	202
246	248	200	237	250	236	252	254

Matrix (a). Pixel matrix of cover frame

251	250	209	215
123	244	201	215
228	255	251	189
112	236	238	250

Matrix (b). Pixel matrix of Watermark image

255	224	251	235	234	245	250	251
168	225	209	215	249	202	238	122
123	231	206	253	251	199	219	215
111	244	236	255	240	200	237	250
125	249	245	250	251	123	231	206
229	252	202	238	125	126	244	236
217	240	190	219	215	125	249	202
246	248	200	237	250	236	252	254

Matrix (c). Pixel matrix of Watermarked Frame

4	4	1	1	3	1	4	8	-	-	-

Matrix (d). Key Structure of size (3Q+2)

Figure 3: Pixel matrix and key structure

Algorithm 1 Algorithmic Steps

1: Begin
2: Obtain the cover video in RGB format.
3: Take color image as watermark data (32x32, 64x64, 128x128and 256x256).
4: Convert the secret image to gray scale image.
5: Search first pixel value of the gray scale image into first frame of video for matching the pixel values.
6: If it is not matched in the first cover frame then search in the next frame andcontinue this up to last frame.
7: When match is found then that frame number of video and location of pixel is stored in structure key.
8: If match is not found in all frames then watermarked pixel value is incremented by 1 i.e. w(i,j)=w(i,j)+1, then new pixel value i.e. w(i,j) is searched in all frames of the video starting from the first frame.
9: If again match is not found decrement watermark pixel value by 1 i.e. w(i,j)=w(i,j)-1, then again search in all frames.
10: Repeat steps vii and viii upto match condition, and after that perform step vi for storing the location of pixel in structure key.
11: Convert all matching pixel locations separately for R, G and B planes.
12: Repeat all above steps for all pixel values of watermarked image.
13: Generate the watermarked video with above watermark subdivision algorithm.
14: Reconstruct the watermark image by using respective locations from secret key structure.
15: End

more secure as shown in Equation (1):

$$SI = \frac{(2\eta_x\eta_y + a_1)(2\kappa_{xy} + a_2)}{(\eta_x^2 + \eta_y^2 + a_1)(\kappa_x^2 + \kappa_y^2 + a_2)} \quad (1)$$

Where η_x and η_y are the average of x and y respectively, K_{xy} is covariance of x & y, a_1 and a_2 are two variables to stabilize the division with weak denominator.

4.2 Peak Signal to Noise Ratio (PSNR)

PSNR is most commonly used to measure the quality of reconstruction of original secret data. Its typical range is 35dB to 70dB. A higher PSNR generally indicates that the reconstruction is of higher quality, which can be calculated using Equation (2):

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (2)$$

Where MAX is the maximum pixel value of the image, MSE [10] is the sum over all squared value differences divided by image size, determined by Equation (3):

$$MSE = \frac{1}{MN}\sum_{mn}(P(m,n) - Q(m,n))^2 \quad (3)$$

Where $P(m,n)$ and $Q(m,n)$ represents two images and M and N represents total number of pixels of secret frame of video and secret watermark image.

4.3 Normalised Correlation (NC)

Normalised Correlation shows the similarities between original image and secret image extracted from watermarked video.We have calculated the NC of selected frame of original video before embedding secret data and after embedding secret data which are exactly identical to each other as shown in Equation (4):

$$NC = \frac{1}{n}\sum_{xy}\frac{(f(x,y) - \overline{f})(t(x,y) - \overline{t})}{m_f m_t} \quad (4)$$

Where n is the number of pixels in *t(x,y)* and *f(x,y)*, $\bar{f}$ is the average of f and m_f is standard deviation of f. It measure immunity of watermark against attacks to remove or degrade it. Maximum Normalised Correlation indicates better Robustness [5].

5 Different Attacks on Watermarked Video

5.1 Histogram Equalization

It is used to remove the embedded data from watermarked video.The basic concept of histogram equalization is to enhance contrast of watermark histogram. Histogram equalization is an example of image enhancement technique [19]. To apply the histogram equalization attack we have modified the values of watermark image to stretch the histogram and controlled the desired number of grey scale value from the watermark image pixel value as shown in Figure 4.

5.2 Gaussian Noise Attack

In the proposed technique we have applied Gaussian noise [10] to original video and watermarked video. After Gaussian attacks our original and watermark video does not change, hence the proposed method is more robust against this attack as indicated in Figure 5.

5.3 Salt and Pepper Attack

Impulsive noise is also sometimes called as salt and pepper attack or spike attack. For selected frame of watermark videowe have obtained dark pixel in bright region and bright pixel in dark region. It is the process of removing the watermark image from watermarked video without attempting to break the security of the algorithm [3, 8]. It is a noise attack in which salt is considered as non-zero value 255 (salt) and pepper as 0 (pepper) as given in Figure 6.

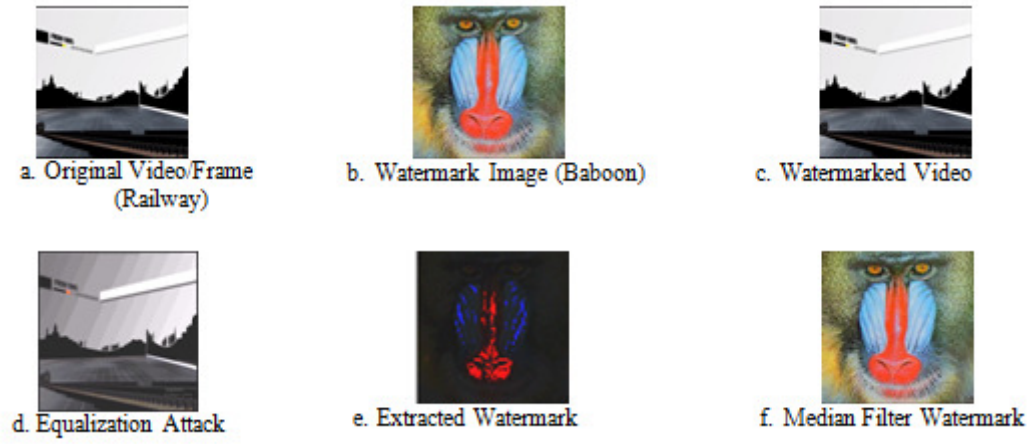


Figure 4: Historgram equalization

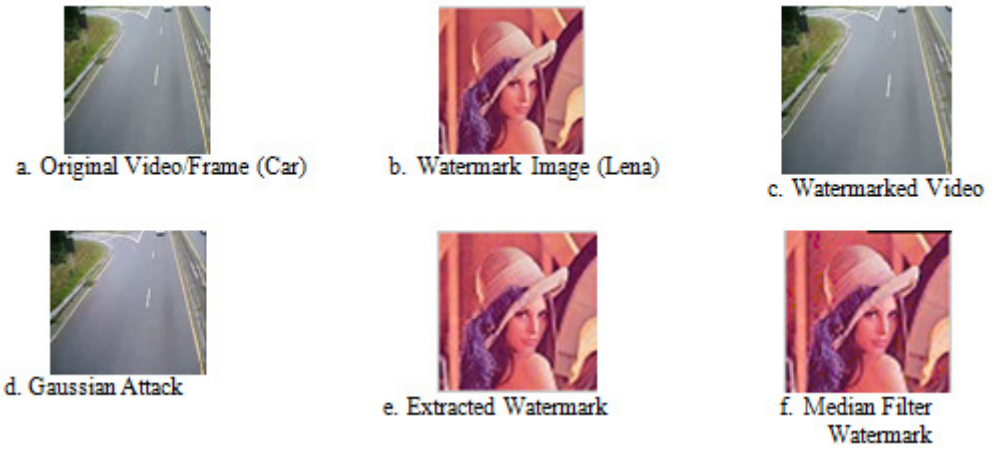


Figure 5: Gaussian attack

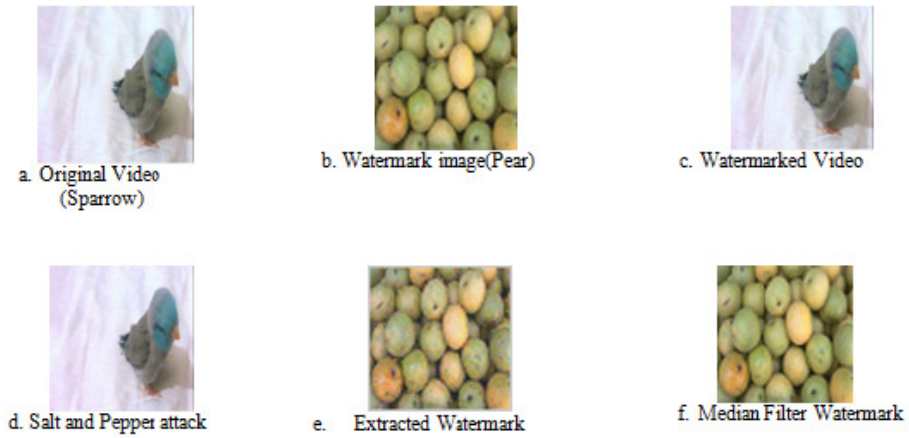


Figure 6: Salt and pepper attack

5.4 Contrast Enhancement Attack

Contrast enhancements improve the perceptibility of embedded data by enhancing the brightness difference between embedded data and their backgrounds. We have applied contrast enhancement attack [3] on selected frame of both original and watermarked video which looks identical as shown in Figure 7.

5.5 Speckle Noise Attack

Speckle attack is noise attack which is applied to test the robustness of the system [2, 14]. It is added to the watermarked video and calculated the PSNR between the original and watermarked video and in between the extracted and original watermark secret message to identify the effect of attack on the watermark after attacking process as shown in Figure 8.

6 Simulation Results and Discussion

We have simulated results through number of videos of different video formats like .Avi, .Flv, .Wmv and .Mp4 and watermark images like Lena, Baboon, Pepper and Pears of different sizes. Table 1 indicates frame wise analysis of SI for different video format. For .Avi video of frames 220 we have used Lena as secret data of size 64x64. For .Avi car video of frames 220, we have embedded Lena watermark image of size 64x64 with and without attack. The value of PSNR is 49.97dB without attacks while with attacks average PSNR is 25.06dB. We have applied median filter so noise in the pixel has been removed and we have obtained PSNR = 49.67dB. As we have embedded baboon image of same size (64x64) with attack and without attack, the PSNR value is 49.67dB without attack while 37.79dB with attack as shown in 9. We have applied median filter with all types of attack and last column shows the values with Gaussian attack. Table 2 gives the functionality comparison between Taun's method [11], Osama [5], Ranjeet [14] and our proposed video watermarking security model in terms of PSNR, SI, NC, attacks, robustness and perceptibility. As we have divided the secret watermark image into four equal parts and embedded it into selected frames of video, hence it is very difficult to understand in which frame, the secret data is hidden so security of watermark video is increased. We have observed five different attacks on watermark video during transmission and calculated PSNR, SI, NC, MSE and Histogram after recovering from watermark video which is identical to each other hence perceptibility of proposed algorithm has increased. We have observed results through .Avi, .Flv and .Mp4 video format having different frame size. We have embedded secret data as images into randomly selected frames of video to generate watermarked video. Median filter is used to remove the unwanted noise which is added during transmission. Hence we have applied median filter after applying different types of attacks. Hence we have recovered our secret data without any loss of information as indicated in Figure 9. Figure 5 indicates the effect of Gaussian attacks. The original .Avi car video of frames 220 of size 410Kb displays in Figure 5(a). Figure 5(b) is the watermark original secret Lena image of size 64x64 before embedding into video. Figure 5(c) is the watermarked video which is exactly identical to original Car video hence perceptibility of proposed system is increased. Figure 5(d) indicates the effects of Gaussian attacks on watermarked video and Figure 5(e) shows extracted secret Lena image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 5(f).

Figure 4 shows the effect of Histogram Equalization attacks. The original .Avi Railway video of frames 311 of size 746Kb is displayed in Figure 4(a). Figure 4 (b) is the watermark original secret Baboon image of size 64x64 before embedding into video. Figure 4(c) is the watermarked video which use exactly identical to original Railway video hence perceptibility of proposed system is increased. Figure 4(d) indicates the effects of Histogram Equalization attacks on watermarked video and Figure 4(e) shows extracted secret Baboon image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 4(f).

Figure 7 indicates the effect of Contrast Enhancement attacks. The original .Flv Dog video of frames 335 displayed in Figure 7(a). Figure 7(b) is the watermark original secret Tree image of size 128x128 before embedding into video. Figure 7(c) is the watermarked video which looks exactly identical to original Dog video before attack hence robustness of proposed system is increased. Figure 7(d) indicates the effects of Contrast Enhancement attacks on watermarked video and Figure 7(e) shows extracted secret Tree image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 7(f). Figure 8 indicates the effect of Speckle Noise attacks. The original .Flv Cat video of frames 410 is displayed in Figure 8(a). Figure 8(b) is the watermark original secret Pepper image of size 128x128 before embedding into video. Figure 8(c) is the watermarked video which are exactly identical to original Cat video hence the security of proposed system is increased. Figure 8(d) indicates the effects of Mean Noise attacks on watermarked video and Figure 8(e) shows extracted secret Pepper image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 8(f). Figure 6 indicates the effect of Salt and Pepper attacks. The original .Mp4 Sparrow video of frames 390 displays in Figure 6(a). Figure 6(b) is the watermark original secret Pear image of size 256x256 before

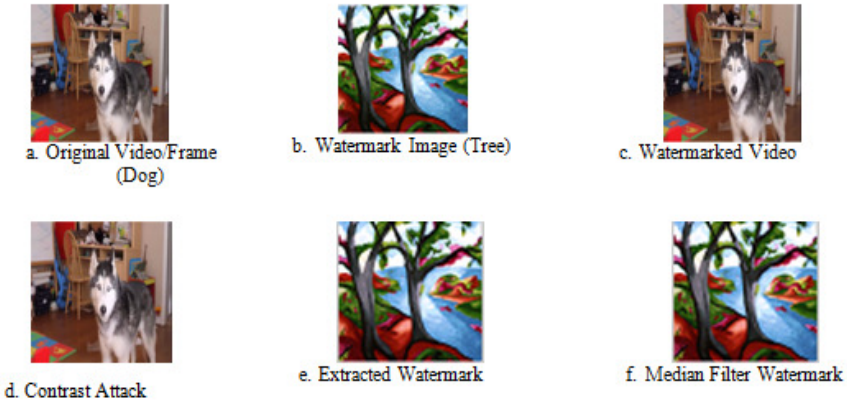


Figure 7: Contrast enhancement

Figure 8: Speckle noise attack

Video	Watermark Image	Size	Parameters	Without Attack	With Attack					
					Gaussian	Salt & Pepper	Histogram	Contrast Enhancement	Speckle Noise	Median Filter
CAR		64x64	PSNR(dB)	49.97	34.36	28.34	15.60	40.67	31.38	49.64
			NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99
			SI	0.98	0.85	0.79	0.76	0.98	0.93	0.98
RAIL WAY		64x64	PSNR(dB)	49.21	34.58	27.05	11.26	42.13	28.74	49.15
			NC	0.98	0.90	0.93	0.90	0.97	0.90	0.98
			SI	0.98	0.76	0.66	0.61	0.98	0.92	0.99
DOG		128x128	PSNR(dB)	50.51	33.40	27.72	18.58	38.84	32.10	49.77
			NC	0.99	0.99	0.99	0.99	0.99	1	0.99
			SI	0.96	0.84	0.71	0.81	0.96	0.94	0.97
CAT		128x128	PSNR(dB)	49.00	33.73	27.24	20.47	39.68	32.51	48.61
			NC	0.97	0.95	0.96	0.95	0.97	0.97	0.97
			SI	0.96	0.83	0.70	0.74	0.95	0.94	0.96
SPAR ROW		256x256	PSNR(dB)	50.62	34.49	27.30	10.79	40.11	28.56	49.95
			NC	1	1	1	0.99	1	1	0.99
			SI	0.97	0.83	0.69	0.57	0.96	0.96	0.98

Figure 9: Security parameters value with five different attacks and without attacks

embedding into video.we have recovered watermark video without any loss of secret information as shown in Figure 6(c). Figure 6(d) indicates the effects of Salt and Pepper attacks on watermarked video and Figure 6(e) shows extracted secret Pear image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 6(f).

The frame wise analysis is displayed in table 1 for frame numbers such as 21, 41, 61, 81, 101 and 141. Proposed method has been checked by applying five different attacks on watermark video during transmission with NC = 1 and SI = 0.987 which shows that proposed method is more robust than existing methods.

Table 1: Frame wise analysis SI for different video

Frames	Car	Railway	Dog	Cat	Sparrow
21	0.987	0.990	0.972	0.974	0.999
41	0.872	0.762	0.853	0.830	0.837
61	0.721	0.973	0.726	0.708	0.692
81	0.772	0.622	0.822	0.744	0.587
101	0.984	0.987	0.966	0.961	0.971
141	0.932	0.933	0.922	0.927	0.929

Figure 10 shows the histogram of original watermark image (Lena), histogram after embedding watermark (watermarked video) and histogram of extracted watermark. Figure 10(a) indicates Lena as watermark image and figure 10(b) shows its histogram. Watermarked video is indicated in figure 10(c) and figure 10(d) shows its histogram. Figure 10 (e) and figure 10(f)shows the recovered watermark and its histogram respectively. Hence our proposed watermarking system is more imperceptible to any existing techniques.

It is found that the proposed security approach is better than existing video watermarking techniques. Taun's method [11] used the DCT based watermarking using even-odd quantization method where the performance parameters were calculated for different video sequences and watermark under different attacks. The average value of PSNR and SI is 44.44dB and 0.8969 respectively; hence it recovers the secret data with some loss of information. Osama's method [5] applied effects of different attacks like scaling, cropping and rotation on video during transmission which is less secured. As the value of SI is 0.8969 the quality of recovered secret data has some distortion. In the suggested approach we have embedded watermark data as text and image into selected frames of video using video watermark subdivision technique, key security parameters PSNR, SI, NC, MSE are better than those are in Taun's [11], Osama's [5] and Ranjeet's [14] approach.

In SVD based DWT watermarking proposed by Osama, PSNR is compared for different DWT schemes [5]. The PSNR is calculated as 44.82dB and the performance is checked under 4 different attacks. Watermarking in spatial domain is projected by Ranjeet which uses LSB watermarking [14]. The PSNR is calculated for different RGB components of an image separately and the effect of three different attacks is evaluated. The PSNR is about 38.69 and the value of NC is 0.5206. The proposed method shows the average value of PSNR as 46.06dB, SI as 0.9870, and NC as 1 and MSE as 0.0858. The performance parameters are calculated for five different attacks. This shows that the proposed method is more robust than other three different methods. Taun and Osama applied four different attacks while Ranjeet applied only three. As the value of PSNR, SI, NC, MSE are found to be exactly same, the perceptibility, security of hidden data and robustness of proposed system is increased.The Figure 11 shows the average PSNR comparison of other schemes with proposed schemes. The DWT based SVD watermarking scheme proposed by Osama displays the value of PSNR as 44.82dB. Ranjeet's method gives the PSNR of 38.75 dB while 44.71dB is for the DCT based method explained by Tuan. In proposed method the PSNR is 49.89 dB.

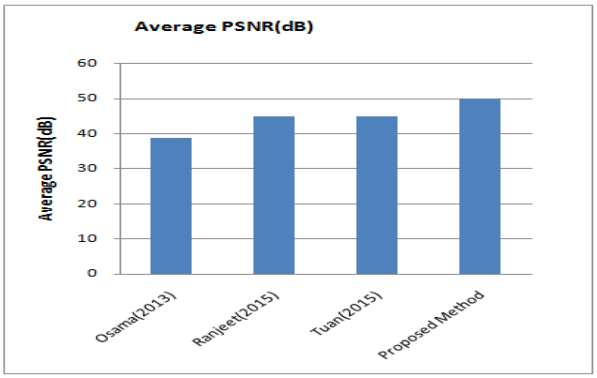


Figure 11: PSNR comparison of other schemes with proposed schemes

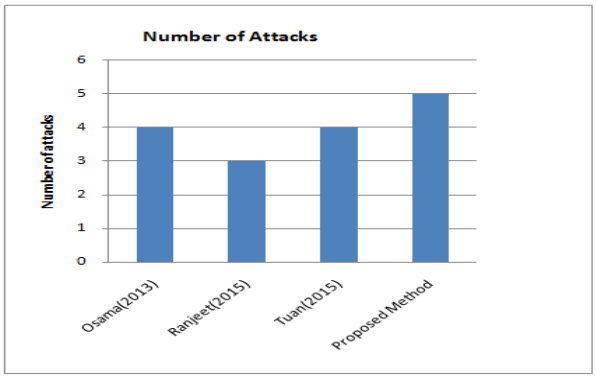


Figure 12: Robustness of other schemes and proposed scheme

Figure 11 shows that our proposed scheme offers better PSNR than other similar schemes. This indicates the quality of reconstruction of watermark is better in proposed method than other mentioned schemes; while Figure 12 shows the number of attacks performed by different techniques.

Method Proposed by Osama survives four different at-

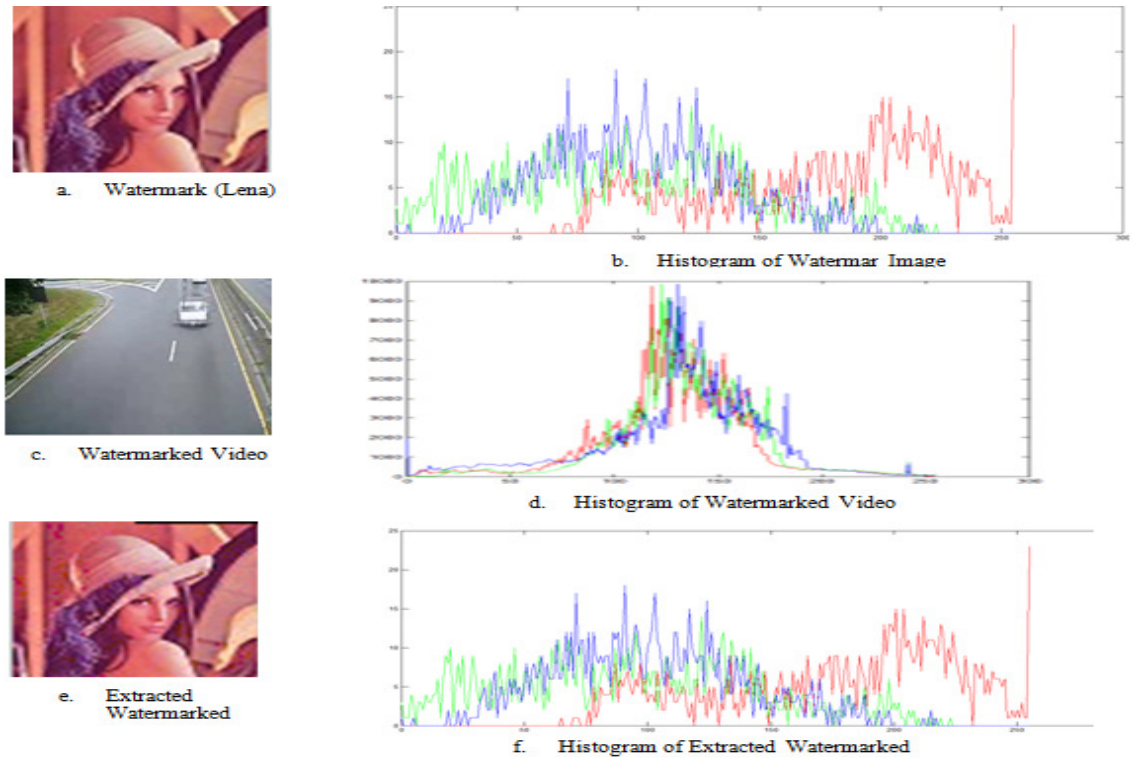


Figure 10: Histogram of watermark image, watermarked video and watermark (secret data) after extraction

tacks while three attacks are applied in Ranjeet's scheme based on LSB technique. Analysis of four different attacks is done by Tuan while the proposed method analyses five different attacks. It indicates that our proposed scheme has more robustness than other scheme.

7 Conclusions

We have presented innovative video watermarking technique to improve security of watermark embedding data with video watermark subdivision algorithm (VWSA). The video watermark technique is tested and verified using standard videos and sample watermark images. The key security parameters PSNR, MSE, NC, SI are calculated before embedding, after embedding and after recovering embedding data from watermarked video. We have applied five attacks on watermarked video during transmission and it is found that the proposed technique is more robust and imperceptible to these attacks. We have compared our result to existing techniques and it is better than existing techniques. In future it can be applied on more video formats with different embedding techniques.

References

[1] S. B. Chaluvadi and M. V. Prasad, "Efficient image tamper detection and recovery technique using dual watermark," in *World Congress on Nature & Biologically Inspired Computing (NaBIC'09)*, pp. 993–998, 2009.

[2] M. A. Chimanna and S. Khot, "Robustness of video watermarking against various attacks using wavelet transform techniques and principle component analysis," in *International Conference on Information Communication and Embedded Systems (ICICES'13)*, pp. 613–618, 2013.

[3] H. Do, C. D, C. H, and K. T, "Digital video watermarking based on histogram and temporal modulation and robust to camcorder recording," in *IEEE International Symposium on Signal Processing and Information Technology*, pp. 330–335, 2008.

[4] D. Essaidani, H. Seddik, and E. B. Braiek, "Asynchronous invariant digital image watermarking in radon field for resistant encrypted watermark," *International Journal of Network Security*, vol. 18, no. 1, pp. 19-32, 2016.

[5] O. S. Faragallah, "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 3, pp. 189–196, 2013.

[6] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–556, Jan. 2000.

[7] D. Jiang, J. Kim, *et al.*, "A spread spectrum zero video watermarking scheme based on dual transform domains and log-polar transformation," *Inter-*

Table 2: Comparison of proposed technique with existing watermarking methods

Parameters	Taun (2015)[11]	Osama (2013)[5]	Ranjeet (2015)[14]	Proposed method
PSNR	44.89	44.83	38.70	50.51
	44.72	44.82	38.69	49.97
	44.53	44.82	38.86	49.21
SI	0.8969	-	-	0.98
NC	-	-	0.5206	1
MSE	-	-	-	0.08
No. of attacks applied	04	04	03	05
Watermarking	Video	Video	Image	Video
Robustness	-	-	Yes	Yes
Perceptibility	-	-	-	Yes

national Journal of Multimedia and Ubiquitous Engineering, vol. 10, no. 4, pp. 367–378, 2015.

[8] A. Kunhu, K. Nisi, S. Sabnam, A. Majida, and A.-M. Saeed, "Index mapping based hybrid dwt-dct watermarking technique for copyright protection of videos files," in *International Conference on Green Engineering and Technologies (IC-GET'16)*, pp. 1–6, 2016.

[9] L. Laouamer, O. Tayan, "An efficient and robust hybrid watermarking scheme for text-images," *International Journal of Network Security*, vol. 18, no. 6, pp. 1152-1158, 2016.

[10] M. Masoumi, M. Rezaei, and A. B. Hamza, "A blind spatio-temporal data hiding for video ownership verification in frequency domain," *AEU-International Journal of Electronics and Communications*, vol. 69, no. 12, pp. 1868–1879, 2015.

[11] T. T. Nguyen, D. D. Nguyen, "A robust blind video watermarking in DCT domain using even-odd quantization technique," in *International Conference on Advanced Technologies for Communications (ATC'15)*, pp. 439–444, 2015.

[12] J. Qin, R. Sun, X. Xiang, H. Li, H. Huang, "Anti-fake digital watermarking algorithm based on QR codes and DWT," *International Journal of Network Security*, vol. 18, no. 6, pp. 1102-1108, 2016.

[13] H. Shojanazeri, W. A. W. Adnan, and S. M. S. Ahmad, "Video watermarking techniques for copyright protection and content authentication," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 5, pp. 652–660, 2013.

[14] R. K. Singh, D. K. Shaw, and M. J. Alam, "Experimental studies of LSB watermarking with different noise," *Procedia Computer Science*, vol. 54, pp. 612–620, 2015.

[15] K. N. Sowmya and H. R. Chennamma, *Video Authentication Using Watermark and Digital Signature - A Study*, pp. 53–64, Springer Singapore, 2017.

[16] B. Sridhar and C. Arun, "An enhanced approach in video watermarking with multiple watermarks using wavelet," *Journal of Communications Technology & Electronics*, vol. 61, no. 2, pp. 165, 2016.

[17] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, Jan. 2017. (https://doi.org/10.1007/s00500-017-2489-7)

[18] D. Vaishnavi, T. S. Subashini, "A secure and robust image watermarking system using normalization and Arnold scrambling," *International Journal of Network Security*, vol. 18, no. 5, pp. 832-841, 2016.

[19] N. Wang, C. H. Kim, "Color image of tamper detection and recovery using block based watermarking," in *IEEE 4th International Conference on Embedded and Multimedia Computing (EM-COM'09)*, 2009.

Biography

Mahesh Gangarde is pursuing Ph.D.(Electronics Engineering) from Bharati Vidyapeeth University College of Engineering, Pune. He has received B.E. from Shri Tuljabhavani College of Engineering, Tuljapur in 2002 and M.E. from Bharati Vidyapeeth University College of Engineering, Pune in 2009. His research area is image/video processing and security.

J. S. Chitode is a professor received the B.E. degree in Industrial Electronics Engineering from Bharati Vidyapeeth University, Pune, Maharashtra in 1991. He received M.E. degree from College of Engineering(COEP),Pune at University of Pune from Maharashtra, India in 1995. He has received Ph.D. degree in Electronics from Bharati Vidyapeeth Deemed University, India in 2009. Currently he is a professor in the Bharati Vidyapeeth Deemed University College of Engineering, Pune (India). His research interest includes Signal processing, Speech Synthesis, Digital Communication, etc. He is actively participating as a member of different professional research societies, like IEEE, ISTE, etc

Secure Stored Images Using Transparent Crypto Filter Driver

Osama Ahmed Khashan[1] and Nour Mahmoud Khafajah[2]
(Corresponding author: Osama A. Khashan)
College of Computing and Informatics, Saudi Electronic University[1]
Riyadh, Saudi Arabia
(Email: o.khashan@seu.edu.sa)
Computing Department, Community College, Imam Abdulrahman Bin Faisal University[2]
Dammam, Saudi Arabia
(Received May 6, 2017; revised and accepted Oct. 21, 2017)

Abstract

The threat of losing the privacy of stored images due to data breaches and malicious attacks has increased the security concerns to improve the protection of storage systems. However, the inherent features of images and the manual nature of the current encryption applications have proven to limit the prevention factors of encryption from being used more heavily in real-time. To overcome these limitations, several studies have highlighted the prominent effects of transparent encryption; nevertheless, the run-time processing in the current implementations of transparent cryptographic file systems is still limited and inefficient. In this paper, we describe the design and implementation of Crypto filter driver, a fully transparent and secure cryptographic file system for Windows platform. It can dynamically realize the processes of writing and reading file images on local disk, and transparently encrypt and decrypt them on the fly. The experiments are performed to measure the performance of the crypto filter driver over images of cryptographic service write and read. Besides the robust security level provided by the new crypto filter driver, the results showed high performance.

Keywords: File System Filter Driver; Image Encryption; Transparent Encryption

1 Introduction

The rapid technological progress in the multimedia domain leads to proliferation of huge volumes of image files to be stored on the disk drives, which in many circumstances can provide vital information. Unfortunately, the lack of security provisions for stored images may invite unwanted attackers to gain access and risk images' privacy.

Security in storage domain is a complex challenge due to the long-term requirement to storing data. Unlike transmission where the security is only needed for spontaneous time event, whereas the storage latency roughly indicates the amount of time which the attacker would need to analyse the security technique applied.

The nature of risks and threats today are increasingly getting more sophisticated, transformational, and malicious. Furthermore, the security provided by technologies such as firewall, anti-virus, intrusion detection and prevention systems are not self-protected from being attacked once an intruder gains privileges to the root security since they are all operated on the application level [16, 28].

Encryption is the most effective solution to frustrate malicious attacks and prevent inadvertent disclosure. It can effectively protect the confidentiality and integrity of stored images in the face of an intruder. Nevertheless, designing systems for storage domain using cryptographic approach is an error-prone, difficult and delicate task, and it may affect system performance if it is not properly implemented. Image encryption differs from text encryption due to the fact that images may encounter a larger space, and contains complex structures and high correlation between pixels. Therefore, encrypting and decrypting digital images involve high computational overhead and processing time, which makes it a major challenge for real-time implementations [19].

A large number of end user encryption applications are available to provide encryption for different user file types and platforms. Nevertheless, most of such encryption applications suffer from several limitations and they are always influenced by the security requirements. Performance failures occur once the encryption application is unable to meet a real-time requirement due to inadequate performance. The manual nature of applications to carry out encryption, decryption and key management. Furthermore, the routine use would increase the overhead incurred by user, which would make a user careless, or intentionally leave files in plain view. Therefore, when ex-

ecution depends on a particular software or user's direct control, it may introduce a dangerous encryption scheme.

Technology of transparent encryption is the most effective solution for storage security. However, applications must request the kernel response to perform different operations on their behalf. Inserting cryptographic service into the kernel as a basic part of the underlying file systems would offer a better functionality for transparent encryption than using any automatic user-space encryption applications. It can effectively handle huge volumes of stored data with efficient performance, high level of transparency, and it is simple to use. It also increases both the security and stability with an inability for superuser privilege to run any arbitrary code with the kernel control [11].

Transparent storage encryption can be carried out using either hardware-based or software-based approaches to perform the encryption for the entire disk data, or even a part of disk for individual files, directories, or individual partitions. Software-based encryption in this domain is more flexible and popular. Cryptographic file systems can significantly tackle the limitations related to the security and reliability by incorporating advanced encryption, authentication, and key management mechanisms. Cryptographic file system can be performed as a user space encryption layer using file system in a user space (FUSE) [7], or as a middleware layer inside the kernel [8]. It can also operate at the lower level of abstraction under the real file system either as a block device layer attached to the storage disk itself [4], or as a virtual disk driver [22,25] to provide encryption to the entire single or multiple disk's partitions.

As a part of our previous work, we have developed a transparent cryptographic file system for stored image files using FUSE technology, named ImgFS [11] for Linux platform. We also have improved the performance of the ImgFS by developing the Parallel-ImgFS [12] to overcome the cryptographic overheads and enhance the response time during image read / write operations. Parallel-ImgFS was implemented by exploiting the parallelism of the multi-core computers using block-based parallel encryption of image files. Although our implemented file systems can provide high-performance cryptographic solution; the task of reading or writing large stored image files with cryptographic service still suffers from heavy workloads due to the FUSE structure. FUSE generally suffers from a limitation of lower performance compared to other kernel file system layers. This is due to the additional overhead associated with the context switches when the FUSE passes between user space and the underlying file system [26].

In this paper, a new cryptographic file system called Crypto filter driver has been introduced for Windows platform to provide more effective transparent cryptographic service for stored images stored on disk on a per image file basis, which improves the efficiency. The developed crypto filter driver is implemented as a middleware layer inside the Windows kernel by using the file system filter driver technology. The main aim of developing this crypto driver is to attain a higher processing speed and to enhance the response time of encrypting and decrypting large image files. Moreover, to provide a systematic way to access, manage, and control all cryptography and key management operations. Therefore, we will evaluate the performance of the developed crypto filter driver over image files' read / write operations. Finally, we will compare the obtained computation results with our previous work results of ImgFS and Parallel-ImgFS versions.

The reminder of this paper is organized as follows. Section 2 presents a review of related work. Section 3 provides an overview of file system filter driver technology. Design and implementation details of the crypto filter driver are presented in Section 4. Section 5 discusses the performance evaluation. Finally, the conclusion of the paper is given in Section 6.

2 Related Works

The innovative idea of transparent services provided by the file system filter driver technology has stimulated much research in this area. Many works have been established using transparent encryption technology to provide user protection and information secrecy, and without any required change in the operating system functions. In our previous work [13] we proposed an efficient approach that can effectively trade-off between security and performance of spatial image encryption through performing a transparent partial encryption and shuffling of image blocks that was implemented inside a file system filter driver. Another proposed model by [21] for data leakage prevention. It used a double cache file system filter driver through allocating buffers in Windows kernel to manage and encrypt sensitive data that are accessed by authorized applications only. The authors of literature [34] proposed a framework model for real-time monitoring and access control to protect spatial geographical files. The filter driver focused on tracking and analyzing the copyright of protected data, and then performed transparent encryption or decryption when a user supplying the correct keys. Literatures [3,14] devoted to enhancing the security of office documents by using transparent encryption that was embedded inside the filter driver. A further proposed model for intelligent transparent encryption was discussed in [30]. It based on a filter driver to encrypt high secret level files that are evaluated and identified using a safety assessment program inside an intranet network. A prevention sensitive data leakage model proposed by [29] for transparent data encryption and real-time monitoring, which was implemented inside a filter driver for intranet environment.

Several authors have proposed models based on filter driver that play an equally important role in the field of information security as well as access control. Literature [27] proposed a transparent prevention system for illegal files access using an information flow detection algo-

rithm that was implemented inside a filter driver. A security service on cloud platform as a well established model proposed by [20] that based on a filter driver to provide transparent encryption and cloud authentication to protect and regulate virtual works. Digital rights management model was proposed by [32] using digital watermark together with a filter driver for the protection of spatial geographical files. The authors of literature [33] based on a filter driver to propose a backup model to monitor defined events belong to an application, and then back up such events or recover them when needed from the storage.

Most of these works are only proposals with less obvious implementation details, and without relative performance evaluation and testing process. Although such works might provide a satisfying solution for data security, there are still some inherent limitations in terms of transparency, flexibility, and efficiency. Current encrypting file systems provide encryption at a fine-grained level of encrypted folder or partition that include all sensitive files inside, and they do not support encryption on per specific file-type basis or specified program's file encryption. Therefore, once the file system is mounted over that folder or partition, all of its stored contents will be decrypted with extra performance overhead. On the other hand, all encryptions are performed using a single key that is stored along with data inside the local disk in plain view.

3 Overview of File System Filter Driver

File system filter driver is an optional driver tailored and attached above the file system driver inside the Windows kernel. Inside the Windows kernel space there is a set of drivers existing between user space applications and hardware devices that are grouped together in stacks and integrating with the I/O Manager. When a user threads an I/O request to open, create, read, write, or close a file, the system call request would be sent to the I/O Manager in the kernel space. In the following, the I/O Manager carries out the required processing, like parsing the filename, finding the physical location on the hard disk and creating the necessary buffers. In the end, it will build the required I/O Request Packet (IRP) before passing it down to the entry point of file system drivers. Drivers use a set of routines to handle with the IRPs through the different file system drivers' levels. Therefore, drivers read or write data from disk drivers, and then return the response back by I/O management to the user's process [31].

Windows uses a memory mapping mechanism to improve the efficiency of the file system. It maps a file into a memory space and accessing it whenever the file is needed. It uses a Fast Dispatch routine to process all fast I/O requests, and then stored data is taken out from the cache memory to the I/O Manager. Unfortunately, this leads to the difficulty of attaching any custom filter driver to capture the processes access the memory, or changing the control structure. On the other hand, Windows uses Dispatch routines to process the IRP requests that handle data obtained from disk partition by disk driver through swapping and paging activities, which are then returned to the I/O Manager [2]. This gives an opportunity to attach a filter driver to add new features, like caching, locking, compressing, security, recoverability, etc., or modify the behavior of other drivers. Therefore, whenever the IRP requests are sent to the local disk driver with a specified function call, the attached filter driver will effectively intercept these requests to carry out its task that was being designed, on the fly, before they reach the lower file system drivers. Figure 1 illustrates the structure of the file system filter driver in addition to the interaction between different kernel parts.

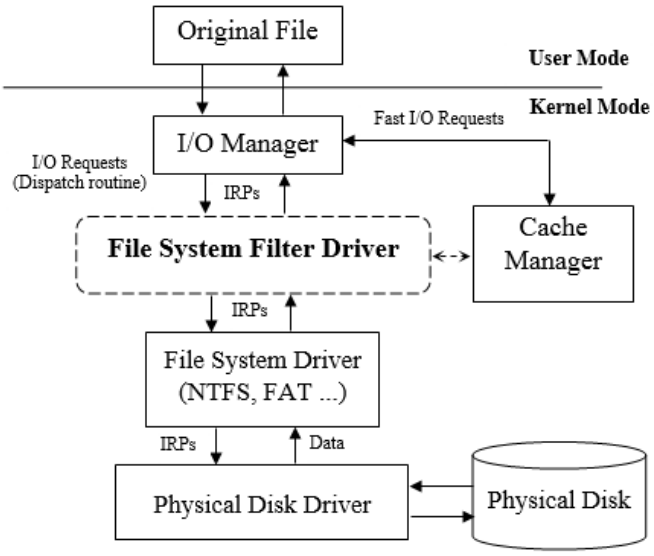


Figure 1: File system filter driver structure

4 System Design and Implementation

The overall objective of this study is to develop a crypto filter driver to provide mandatory encryption and decryption services for all image files stored on disk drive in high performance and secure execution. It has also managed to overcome the identified weaknesses related to other cryptographic filter driver based implementations.

The crypto filter driver will be able to automatically recognizing the image file once it detects that the process is trying to open or save an image file on a local disk. It will then be able to transparently encrypt or decrypt the image contents at the granularity of per image file level. All the operations will be performed in a dynamic and seamless way, neither adding overhead on the users for ciphering nor paying attention to the key management related problems.

4.1 Crypto Filter Driver Work Mode

The crypto filter driver is built on the top of the file system, therefore it can block all read and write requests related to the stored image files. When a user threads a request to write or read an image file through WriteFile() or ReadFile() system calls, the I/O Manager handles the request and builds the required IRP, and subsequently turns it directly to the underlying file system drivers. Once the IRP passes through the crypto filter driver, it exposes the logical structure of the IRP by reading the file object and header attributes to recognize whether it is for read or write an image file on a disk. With the write and read destination addresses, the crypto driver is able to encrypt or decrypt image data before it is written on disk or sent back to the user mode.

In our system, the crypto filter driver mounts itself over any file system driver and listens to all requests trying to read or write images from its associated disk partition by disk drivers. Therefore, all image files stored at the secure partition are considered confidential (automatically encrypted), and are not allowed to leak. Other files created by normal processes will not be encrypted or decrypted.

There are two methods to determine image file formats. The first method is by using the filename extension by determining the format of an image file based on the portion of the filename. However, this approach suffers from security concerns when an image format is renaming and treating as a different format, or hiding the image file extension. The other method is by using the metadata contained in the header of the file. Each file header contains a magic number that can uniquely distinguish the format of the file. Other metadata in the image header store information about image file, colour space, resolution, and other authoring information. Although this approach take longer time to identify a file format, it offers a secure way to guarantee that a file format will be identified correctly. The crypto filter driver is designed to recognize image files based on the magic numbers contained on the file header. To do this we use a list that contains most of the image magic numbers from both of well-known compressed and uncompressed image formats [10].

The pre-processing operation that is carried out by the crypto driver is to detect the image file by reading its magic number, and if that magic value is included in the list, the image file will be considered for encryption process. This makes the crypto driver most convenient to work with image applications.

Image encryption and decryption processes are carried out in the complete dispatch routines of IRP_MJ_WRITE and IRP_MJ_READ, respectively, through the completion routine set by IoSetCompletionRoutine(). When the requirements are determined for reading or writing an image file from a place on a local disk under the mount of the crypto filter driver, the image file will be considered to be added into a created encryption linked list. The File Control Block (FCB) is used to represent the confidential image files opened, and it is stored in the image file object. Consequently, the file system will generate a memory area for each image file to save image contents, regardless of how many times the image file is opened since each image has only one FCB. All opened confidential images are stored in the encryption-linked list. Therefore, when an image file is opened, the FCB pointer will be gotten from the file object that is available in the IRP. Then, the FCB pointer will be compared to an encryption file table to determine its availability. If the pointer is encountered, the FCB will be immediately added into the encryption-linked list. Confidential image file read or write is associated with adding or deleting FCB from the encryption linked list. Consequently, the corresponding image file's content will be placed into a local buffer to apply encryption or decryption operation.

4.2 Encryption and Decryption Processes

Inside our implemented crypto filter driver, there are two modules, cryptographic and key management. Figure 2 shows the implementation architecture of the image crypto filter driver.

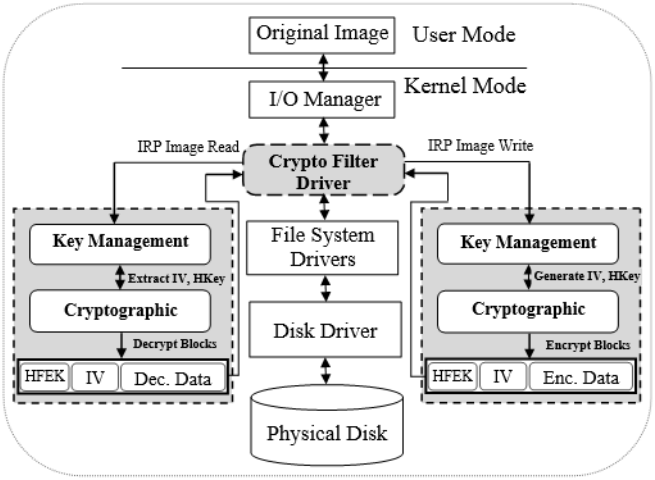


Figure 2: Crypto file system architecture

When the crypto driver realizes a new image in the list needs to be encrypted, it immediately initializes the encryption algorithm and other encryption parameters, which are realized on the cryptographic module. The whole image contents are firstly divided into a number of blocks of fixed size, each with 16 bytes. Obviously, each block should be checked that it has a perfect 16 bytes size; otherwise, the block will be padded while it is being written. Thereby, all image blocks would be encrypted sequentially one block at a time, except the image file header, which will be excluded from being encrypted or decrypted.

We picked AES as a fast symmetric encryption algorithm [5] with default 128-bit key length. Furthermore,

we chose the cipher block chaining (CBC) as an operation mode. Although the use of symmetric algorithms may provide a lower performance for the image encryption process compared with other image encryption methods, the security level provided by the symmetric ciphers is higher [15]. Thus, a trade-off between performance and security can be achieved with the usage of the symmetric ciphers.

In order to guarantee of achieving a better security level, the uniqueness requirement for the initialization vector (IV) across all image files is considered. Therefore, a unique IV of 64 bits is generated randomly each time a new image file is created. After completion of image blocks encryption, the random generated IV is attached to the header of the image file. Upon completing the encryption process, a tag is added to the head or tail of the image file. This method leads to easily identifying the encrypted image when it is read from disk during responding to the read dispatch routine in order to satisfy the decryption process.

Similarly, reading or copying stored image is performed transparently in reverse order. In the IRP_MJ_CREATE routine, the crypto driver extracts the file object from IRP stack. It then checks whether the file has an encryption tag. If the IRP is related to a stored image in a place under the crypto driver mounting point, the driver immediately responds by adding the file to the decryption list. Key management module is used firstly to extract the IV from the image file header. After that, the cryptographic module initiates the AES encryption cipher and related parameters, and then uses the associated encryption key to decipher all image blocks. The padded bytes are then removed from blocks, if exist. Once the plain image is generated, it will be directly sent back to the I/O Manager and then to the caller in the user space.

4.3 Key Management Process

The security of any cryptographic system is relied on the stringent level of the applied key management. Losing or forgetting encryption keys due to a long storage period leads to losing access to all stored data on a disk. In addition, storing keys in plain form on disk would increase the keys chances to be stolen or leaked out easily. In such study, we enforce the security of encryption keys, to overcome the key issues of authenticated encryption schemes identified by [9]. Furthermore, we allow the crypto driver to use and manage the encryption keys of all stored images in a fully transparent manner. It also addresses the limitations of current key management schemes that are operated manually on a per-file system basis.

Key management module involves the operations of creating, using and retaining the encryption keys. Using a single key to encrypt all image files is not secure, once the attacker successes to obtain the secret key for one file; he would be able to recover all other encrypted files. Therefore, in our scheme, each image is encrypted using a different file encryption key (FEK), hence, it is impossible to find two similar ciphered images related to the same plain image. We enhance the security of FEK with security margins afforded by HMAC [18], where the security analysis of HMAC is proved in [1, 17]. The FEK for each image is created by HMAC-MD5 of a common used symmetric key of 16-byte length and a hashed code of the image corresponding IV that is produced using MD5-128.

In order to ensure the integrity of the secure stored images, an embedded signature that is generated by hashing the FEK (HFEK) using MD5-128 to ensure that the image file has not been tampered or replaced by attackers during storage. The generated HFEK is then stored as an extended attribute on the header of the image file. Thus, as soon the encrypted image file is being retrieved from the disk, it would be loaded into a local buffer. The key management subsequently extracts the HFEK from the header file and the 'check_signiture()' function will check the file signature to verify that the image file has not been tampered, before the read operation is executed. When the image signature is verified, the cryptographic module will shift by 256 bits of image file header to read 16 bytes image block, and then calls the 'file_decrypt()' function to decrypt it using the corresponding FEK. The process is repeated with all subsequent image blocks and the result will be stored temporarily into a buffer in order to be returned later to the caller in the user space.

5 Performance Evaluation

In this section, several experimental tests were performed sequentially to evaluate the performance of the crypto filter driver over the write and read operations of image files with cryptographic service. A set of experimental image samples of large sizes and different formats were used. The experiment machine was installed with Windows 7 of 32-bit version, and WDK. It had an Intel Core i3- 2120, 3.3 GHz CPU. The system RAM was of size 4 GB, and the hard disk size was 320 GB of 7200 rpm.

We used Windows System Assessment Tool (WinSAT) [23] and Geekbench [6] benchmarks to run a series of tests and to evaluate the performance of the machine (in execution time) over the normal image file's write and read on the standard NTFS, against the performance of image write with encryption and read with decryption, respectively, on the implemented crypto filter driver. Each test was repeated fifteen times in each benchmark and the average of their values was taken. The standard deviation of the calculated results was not high and the intervals were always less than 6%. To ensure the accuracy of the obtained results, we flushed the cache after each test using the CcFlushCache() routine [24].

We measured the computational times of write and read operations on a number of large experimental image files using the crypto filter driver. We, respectively, wrote and read an image file of size 25 MB from places on local disk under the mount of the crypto filter driver and NTFS, and the elapsed writing and reading times were

recorded. The tests were regularly repeated by increasing the size of the image file up to 500 MB, where the sample of image files (above 250 MB) are uncompressed images of type BMP (Windows bitmap).

The recorded times include the total time for the operations of write/read image into local buffer, encrypting or decrypting image blocks, in addition to the time for extracting or saving keys on the header of image file. Figure 3 and Figure 4 show the comparison of total times measured (in seconds) for writing and reading image files using the standard NTFS and the crypto filter driver, respectively.

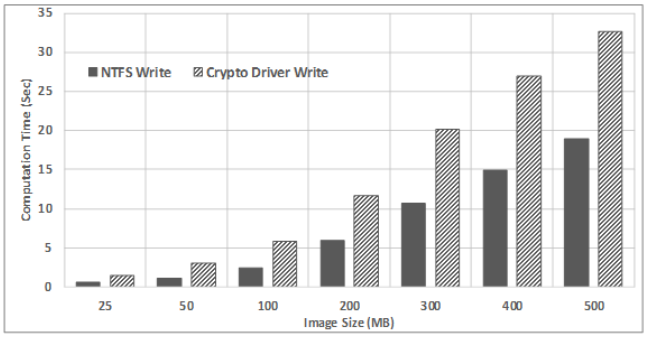


Figure 3: Comparison of computation times spent for writing images using Crypto filter driver and NTFS

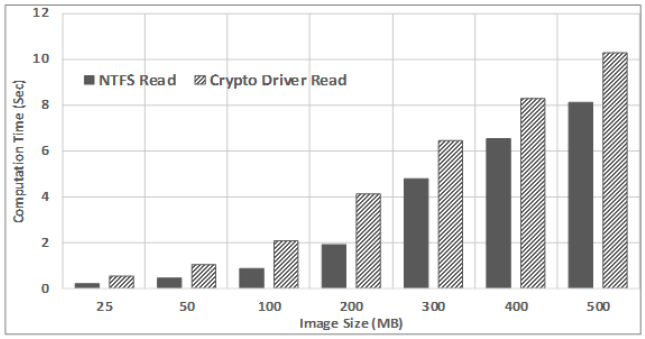


Figure 4: Comparison of computation times spent for reading images using Crypto filter driver and NTFS

From the evaluation results, it was noted that the crypto filter driver could always achieve an average speed of 16 MB/s for writing image files with encryption on the local disk, in comparison with the normal write using NTFS which could achieve the average speed of 35 MB/s. It was also observed from the results that the crypto filter driver could achieve the average speed of 48 MB/s for reading image files with decryption. Compared with the normal read on the standard NTFS, it could always achieve 91.7 MB/s as the average of reading speed.

Several major processes executed during image write and read operations in the crypto filter driver. These processes include of searching image blocks of fixed 16-byte size, writing/ reading image blocks into local buffer, the workload time for generating and loading encryption keys into/from the image file header, in addition to the actual encryption/ decryption time of all image blocks.

We measured the computational time elapsed for generating keys and saving them on the image file header during image write operation throughout the crypto filter driver mount time. It took in average 0.35 second from the image write time. We also measured the average time elapsed to load and re-generate the keys during image read operation, and it took about 0.27 second from the total image read time. Table 1 illustrates the times spent by the write-related processes and actual encryption, the read-related processes and actual decryption times elapsed during image write and read operations, respectively, in the crypto filter driver.

Table 1: Computational times elapsed for the write-, read-related processes, actual encryption, and actual decryption

Image size (MB)	Time (sec)			
	Write-related processes	Actual encrypt	Read-related processes	Actual decrypt
25	0.58	0.91	0.32	0.21
50	0.93	2.13	0.39	0.64
100	1.57	4.27	0.61	1.49
200	2.96	8.62	0.93	3.24
300	4.53	15.44	1.25	5.19
400	6.06	20.59	1.59	6.73
500	7.11	26.03	1.91	8.38

Following that, we compared the performance of the crypto filter driver over the write and read operations with our previously implemented cryptographic FUSE-based file systems, namely ImgFS and Parallel-ImgFS. Figure 5 and Figure 6 show the measured computation times for writing and reading images on ImgFS, Parallel-ImgFS and Crypto filter driver, respectively, using the same experimental image samples.

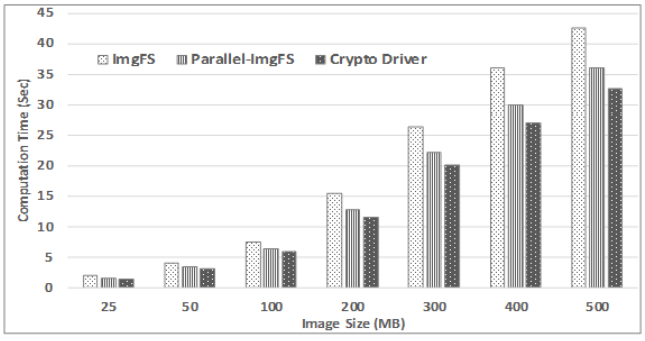


Figure 5: Comparison of computation times for writing images with encryption using ImgFS, Parallel-ImgFS, and Crypto filter driver

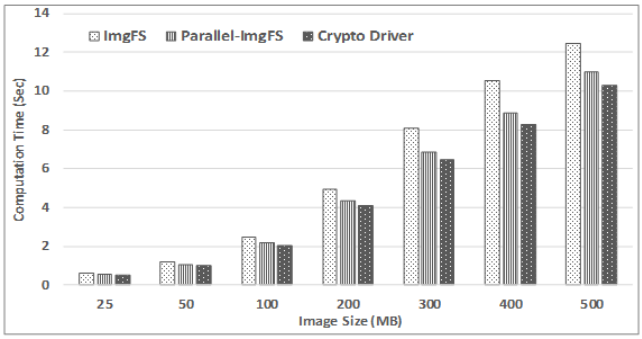


Figure 6: Comparison of computation times for reading images with decryption using ImgFS, Parallel-ImgFS, and Crypto filter driver

From the results, it was noted that the crypto filter driver could achieve higher performance (lower execution time) for both write and read operations than Parallel-ImgFS and ImgFS. When calculating the average performance, the crypto filter driver always took about 48% of the normal write time and about 57% of the normal read time for writing and reading image files, respectively. As a result, the new crypto filter driver has successfully enhanced the response time of writing and reading image files with an efficiency of 9% and 6% of the Parallel-ImgFS write and read performance, respectively.

6 Conclusion

In this paper, we designed and implemented crypto filter driver based on the file system filter driver technology that was running inside the Windows kernel. The crypto filter driver can effectively provide mandatory, automated and transparent encryption scheme for all stored images during system run time with an improved user's convenience. The system is perfectly suitable to work with image applications that might provide important information. It is more convenient to work with medical imaging systems, military image databases, scientific images, geography image sensing and personal image albums.

We have shown the implementation details of the crypto driver in order to make up the shortcomings of the existing cryptographic filter driver based implementations. It has successfully managed to reduce the response time from the forced decryption of all stored files when other cryptographic file systems are mounted, by supporting a decryption to be on per-image file basis. Key management was also perfectly suited to provide different keys for different encrypted images and without storing keys in plain form on disk.

The experimental results indicated that while the new crypto filter driver managed to provide a higher level of security, it could achieve higher processing speed with a reduced response time. It is always able to gain an average speed of 16 MB/s and 48 MB/s, respectively, for writing and reading image files with cryptographic service. In comparison with our previous FUSE-based works, the crypto filter driver could achieve higher response times of images' write and read of about 9% and 6%, respectively.

References

[1] M. Bellare, "New proofs for NMAC and HMAC: Security without collision resistance," *Journal of Cryptology*, vol. 28, no. 4, pp. 844-878, 2015.

[2] California Software Labs, *I/O File System Filter Driver for Windows NT*, Technical Report XP002548991, California Software Labs, Pleasanton, California, 2002.

[3] J, Chen, and J. Ye, "Research on the file encryption system based on minifilter driver," in *The 13th International Conference on Man-Machine-Environment System Engineering, Berlin, Heidelberg*, vol. 259, pp. 175-182, 2014.

[4] R. Dowdeswell, and J. Ioannidis, "The CryptoGraphic disk driver," in *Proceedings of the Annual USENIX Technical Conference (USENIX'03)*, pp. 179-186, 2003.

[5] D. Elminaam, H. Abdual Kader, and M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," *International Journal of Network Security*, vol. 10, no. 3, pp. 213-219, 2010.

[6] Geekbench 4, Jan. 13, 2017. (`http://geekbench.com/index.html`)

[7] V. Gough, *EncFS Encrypted Filesystem*, Jan. 27, 2017. (`http://www.arg0.net/encfs`)

[8] M. A. Halcrow, "eCryptfs: An enterprise-class encrypted filesystem for Linux," in *Proceedings of the 2005 Linux Symposium*, pp. 201-218, 2005.

[9] M. Hwang, and C. Liu, "Authenticated encryption schemes: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, 2005.

[10] G. Kessler, *File Signatures Table*, Sep. 3, 2017. (`http://www.garykessler.net/library/file_sigs.html`)

[11] O. A. Khashan, A. M. Zin, and E. A. Sundararajan, "ImgFS: Transparent cryptographic storage images using file system in user space," *Frontiers of Information Technology & Electronic Engineering*, vol. 16, no. 1, pp. 28-42, 2015.

[12] O. A. Khashan, A. M. Zin, and E. A. Sundararajan, "An optimized parallel encryption for storing image files using filesystem in userspace," *International Journal of Advancements in Computing Technology*, vol. 6, no. 2, pp. 126-135, 2014.

[13] O. A. Khashan, and A. M. Zin, "An efficient adaptive of transparent spatial digital image encryption", in *The 4th International Conference on Electrical Engineering and Informatics (ICEEI'13)*, vol. 11, pp. 288-297, 2013.

[14] N. M. Khafajah, K. Seman, and O. A. Khashan, "Enhancing the adaptivity of encryption for storage electronic documents," *International Journal of Technical Research and Applications*, vol. 2, no. 1, pp. 28-32, 2014.

[15] O. A. Khashan, A. M. Zin, and E. A. Sundararajan, "Performance study of selective encryption in comparison to full encryption for still visual images," *Journal of Zhejiang, University Science C*, vol. 15, no. 6, pp. 435-444, 2014.

[16] S. Kim, W. Park, S. Kim, S. Ahn, and S. Han, "Integration of a cryptographic file system and access control," *Intelligence and Security Informatics, Springer, Berlin, Heidelberg*, vol. 3917, pp. 139-151, 2006.

[17] J. Kim, A. Biryukov, B. Preneel , and S. Hong, "On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1," in *International Conference on Security and Cryptography for Networks*, pp. 242-256, 2006.

[18] H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, 1997.

[19] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos," *International Journal of Network Security*, vol. 20, no. 1, pp. 110-120, 2018.

[20] Z. Liang, S. Jia, J. Chen, and P. Chen, "Security of virtual working on cloud computing platform," in *IEEE Asia Pacific Cloud Computing Congress*, pp. 72-75, 2012.

[21] J. Liu, S. Chen, M. Lin, and H. Liu, "A reliable file protection system based on transparent encryption," *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 123-132, 2014.

[22] Microsoft, *BitLocker Drive Encryption Overview*, Jan. 6, 2017. (`https://technet.microsoft.com/en-us/enus/library/cc732774(v=ws.11).aspx`)

[23] Microsoft, *Windows System Assessment Tool (WinSAT'17)*, Jan. 8, 2017.(`https://technet.microsoft.com/en-us/library/cc770542(v=ws.11).aspx`)

[24] Microsoft Developer Network, *Device and Driver Technologies*, Jan. 9, 2017. (`https://msdn.microsoft.com/en-us/library/windows/hardware/ff539082(v=vs.85).aspx`)

[25] A. Patrascu, M. Togan, and V. Patriciu, "Deduplicated distributed file system using lightweight cryptography," in *IEEE International Conference on Intelligent Computer Communication and Processing (ICCP'15)*, pp.501-506, 2015.

[26] A. Suresh, G. Gibson, and G. Ganger, *Shingled Magnetic Recording for Big Data Applications*, Technical Report CMU-PDL-12-105, Parallel Data Laboratory, Carnegie Mellon University, May 2012.

[27] W. Tang, Y. Xu, G. Wang, and Y. Zhang, "An illegal indirect access prevention method in transparent computing system," in *The International Conference on Algorithms and Architectures for Parallel Processing*, vol. 9532, pp. 264-275, 2015.

[28] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.

[29] Z. Xiaosong, L. Fei, C. Ting, and L. Hua, "Research and application of the transparent data encryption in intranet data leakage prevention," in *International Conference on Computational Intelligence and Security (CIS'09)*, pp. 376-379, 2009.

[30] P. Zhang, and Z. Wei, "Application of intelligent transparent encryption model on intranet security," in *IEEE International Conference on Information Theory and Information Security*, pp. 268-270, 2010.

[31] C. Zhang, Y. Wu, Z. Yu, and Z. Li, "Research and Implementation of File Security Mechanisms Based on File System Filter Driver," in *IEEE Annual Reliability and Maintainability Symposium*, 2017.

[32] L. Zheng, L. Feng, Y. Li, and X. Cheng, "Research on digital rights management model for spatial data files," in *The 2nd International Conference on Information Engineering and Computer Science*, pp. 1-4, 2010.

[33] Z. Zhongmeng, and Y. Hangtian, "A data backup method based on file system filter driver," in *The 2nd World Congress on Software Engineering (WCSE'10)*, vol. 2, pp. 283-286, 2010.

[34] G. Zhu, Z. Liangchen, L. Guonian, and Z. Liangchen, "The access control technology of spatial data files based on file system filter driver," in *The 11th IEEE International Conference on Communication Technology (ICCT'08)*, pp. 734-737, 2008.

Biography

Osama Khashan received his B.S degree in Computer Science from Irbid National University, Jordan in 2005, M.S in Information Technology from University Utara Malaysia in 2008, and the Ph.D in Computer Science from the National University of Malaysia in 2014. He is currently an assistant professor in the College of Computing and Informatics, Saudi Electronic University, KSA. His research works focus on information and network security, digital image processing, and performance analysis.

Nour Khafajah received her B.S degree in Computer Science from Al-Balqa Applied University, Jordan in 2011, and the M.S in Information Security and assurance from the Islamic Science University of Malaysia in 2014. She is currently a lecturer in Imam Abdulrahman Bin Faisal University, KSA. Her research intrests in information and cyber security.

Android Malware Identification Through Visual Exploration of Disassembly Files

Yong-liang Zhao[1] and Quan Qian[2,1,3]
(Corresponding author: Quan Qian)

School of Computer Engineering & Science, Shanghai University[1]
Shanghai Institute for Advanced Communication and Data Science, Shanghai University[2]
99 Shangda Road, Shanghai, China
(Email: qqian@shu.edu.cn)
Materials Genome Institute of Shanghai University[3]
No. 99, Shangda Road, Shanghai, China
(Received Apr. 28,2017; revised and accepted Aug. 20, 2017)

Abstract

Android malwares are the most serious threats for the current mobile Internet. In this paper, we propose a static analysis approach which does not need to understand the source code of the android applications. The main idea is as most of the malware variants are created using automatic tools. And there are special fingerprint features for each malware family. Depending on decompiling the android APK, we innovatively map the Opcodes, API packages and high level risky API functions into an integrated three channels of a RGB image respectively. And then use convolutional neural network to identify each family's features. The experimental results show that the proposed method successfully identified the entire 14 malware datasets with accuracy 90.67%, precision 93.36%, recall rate 93.95% and F1 93.56% on average.

Keywords: Android Malware; Deep Learning; Malware Identification; Visual Analysis

1 Introduction

With the rapid development of mobile internet, mobile devices, especially smartphones, are not only as important tools for people to communicate with the outside world, but also as personal digital assistants or enterprise digital assistants to plan or organize their users' work and also private life. So, mobile security has become increasingly important in mobile computing. According to the statistical analysis of AliMobileSecurity, although the number of mobile malwares and infections in 2015 showed a certain degree of decline,still 18% devices were infected with different kinds of virus or trojans. Moreover, the professional virus attacks over the year have been significantly upgraded, such as the abuse of system vulnerabilities, security reinforcement technology, especially the social engineering. All of these make the traditional mobile virus interception technology being encountered unprecedented challenges.

Although the number of malwares is increasing every year,most of the variants are modified or generated based on the original malicious code [6]. In most cases, hackers use automated or module reuse tools to generate malwares automatically. These variants often share the same ancestor's work, resulting in the high degree of similarity among variants. So, how to recognize the fingerprints among different variants is the main task we should pay more attention to.

About the mobile operating systems, there are Android, iOS, Symbian OS and Windows phone. Considering the open source and widespread applications, in this paper we mainly focus on Android system. We introduce a new method to classify the android malwares. For each malware sample, we extract the Opcode feature and map it into R channel of RGB image, OS API feature into G channel and risky API feature into B channel, then we merge three channels into one combined feature image and use the deep learning algorithm for further classification. The rest of the paper is organized as follows: Section 2 gives a brief introduction of the related work. Our main contributions, the image based feature integration and deep learning based classification are described in Sections 3 and 4. The experimental results are shown in Section 5. Section 6 summarizes the whole paper and give some directions for future work.

2 Related Work

According to code state for analysis, malware detection methods can be typically divided into two categories: static analysis and dynamic analysis. In static analysis, the codes of the sample are examined comprehensively

by disassembling or decompiling the malware binary files without executing it, which can prevent operating system from malicious damages. The advantages of static analysis are that we can get a complete view of what a given malware does. However, in most cases, static analysis is not a trivial task since hackers use code obfuscation, such as binary packers, encryptions to evade detection. Furthermore, static analysis does not allow a high degree of automation, since in most cases, it is done by hand and sometimes very time-consuming. Considering about the dynamic analysis, it can analyse the behavior of the malware during executing it in a debugger. Currently, sandbox-based dynamic analysis is one of the most popular solutions. A sandbox executes a malware sample in a controlled environment which can monitor and record information of system calls and behaviors dynamically. The main limitations of dynamic analysis, especially the sandbox-based solutions, are the overwhelming detailed reports for human analysts to face. How to make the malwares behavior more easier accessible. How to guarantee the high degree of execution path coverage are two critical factors. Furthermore, in contrast to static analysis, dynamic analysis can be automated to a high degree, though it has high computation complexity.

2.1 Android Malware Detection Using Static Analysis

Static analysis involves extracting information from the application's manifest of the Android application's bytecode. The features often used in static analysis include API calls, requested permissions, used permissions, control flows, data flows, hardware components, application components, intents, network addresses, *etc.*

Sanz *et al.* [15] presented PUMA, a system used the permission application requests upon installation to detect whether the application is malicious or not. Machine learning models including simple logistic regression, Naive Bayes, Bayes Net, SMO, IBK, J48, Random Tree (RT) and Random Forests (RF) are evaluated on a dataset consisting of 357 benign and 249 malicious applications. The best overall accuracy reaches by Random Forests 86%.

Lee *et al.* [17] presented a detection mechanism using runtime semantic signatures, which showed high family classification accuracy. They used three sets of elements to construct the signatures. The first set is binary patterns of malicious API calls instructions, runtime semantics of control and data flow. The second set is the malware family characteristics including family common strings, constants, methods, and classes. The third set is weights that each behavior belongs to a family. Experiments on 1,759 Android malwares including 79 variants of 4 malware families show that the proposed method can obtain 99.89% accuracy on detecting the malware family of a particular variant.

Arp *et al.* [1] proposed DREBIN, which was a similar approach to the method proposed by Peng *et al.* [8]. Eight different static feature sets are extracted including hardware components, requested permissions, application components, filtered intents, restricted API calls, used permission, suspicious API calls, and network addresses. Experiments on evaluation of 123,453 benign applications and 5,560 malware samples, DREBIN can detect 94% of the malware.

Zhang *et al.* [12] implemented DroidSIFT. They extracted a weighted contextual API dependency graph as program semantics to construct feature sets. Graph similarity metrics are introduced to uncover homogeneous application behaviors. Experiments on 2,200 malware samples and 13,500 benign samples are performed using Naive Bayes. The results show that DroidSIFT can detect 93% of malware instances.

Yang *et al.* [2] developed DroidMiner, which used static analysis to automatically learn the malicious program logic from known Android malwares. A two-tiered behavior graph is constructed in DroidMiner. The upper tier is a component dependency graph (CDG) in which each node represents an activity, a service or a broadcast receiver. The lower tier uses component behavior graphs (CBG) to present each component's lifetime behavior functionalities. From the behavior graph, different malicious patterns, named modalities, can be mined. In particular, function modality representing an ordered sequence of API functions, and resource modality representing a set of sensitive resources, are extracted and converted to a modality vector by DroidMiner. The vectors are then fed into several machine learning classifiers including Naive Bayes, SVM, decision trees, and random forests for malware detection. The best algorithm of DroidMiner can achieve a 95.3% detection rate on a dataset of 2,466 malwares. It can also reach 92% for classifying malwares into their proper families.

2.2 Android Malware Detection Using Dynamic Analysis

Dynamic analysis records the execution of an application and tries to identify malicious behavior. It is well known for being resilient to obfuscation techniques. However, dynamic analysis introduces more overhead because it requires running the application first and then deciding whether it is malicious based on run-time behavior. As a consequence, it is mostly applicable for offline malware detections. Besides that, the other deficiency of dynamic analysis is code execution path coverage. Since some malicious behaviors are triggered by special conditions, dynamic analysis will not record an application's malicious behavior if the conditions are not matched.

Ham *et al.* [20], proposed a method that was very similar to CrowDroid. They also aggregated real-time system calls to create a histogram using Linux strace tool. They discovered that some system call patterns only occurred in malicious applications and some only in benign ones. Different from the K-means used in CrowDroid, Ham *et al.*, applied a discrimination algorithm based on Euclidean distance on 1,260 malware samples published

by Genome [19]. But no classification accuracy was reported yet.

Tchakounté *et al.* [18] scrutinized system call invocations initiated by the malicious code at the moment the user runs it using the Linux strace tool. With their tool they discovered new scenarios of how the users are lured to aid the malicious developer.

Wei *et al.* [21] recorded system call invocations by manually installing and executing each application on a real Android phone. N-gram vectors are generated from the system call invocations and fed into a SVM and a naive Bayes for classification. Experiments on 96 benign applications and 92 digital book malware samples show their methods can reach 94% accuracy.

Dimjasevic *et al.* [3] proposed MALINE, which also records system call invocations for Android malware and converts them into two representations. One is histogram and the other is a variant of the Markov Chain representation. Experiments on 4,289 malwares and 12,789 benign applications show that they can achieve 93% detection accuracy.

So, there have been some relative work on Android malwares using static or dynamic methods. But different from the existing work, our contributions are as follows:

1) Proposing a new method that recognize the malware without understanding its source code and execution behavior.

2) Using visualization techniques to transform the Opcodes to family images.

3) Integrate the Opcodes sequence features, API calls features and high risky API calls features to three different RGB channels.

4) Using CNN network to train the malware feature images and get an excellent identification results.

3 Visual Representation for Android Malwares

Nataraj *et al.* [13], proposed a method for visualizing and classifying malwares using image processing techniques, which transform windows platform malware binaries to gray-scale images. In 2015, Little Boat *et al.* won the championship of Kaggle, a famous Microsoft Malware Classification Challenge. It is interesting that the championship team with three people did not engage in security, and the methods used are very different from our common methods. They use gray-images, n-gram and the PE-header features, and use machine to learning classify the malwares. Without understanding the malware's source code, it shows great potential that image based methods for malware detection.

Based on this idea, we propose a method mapping Android applications to RGB images. We extract three features: Opcode, sensitive API calls, and risky API requests. And integrate them into one RGB color image.

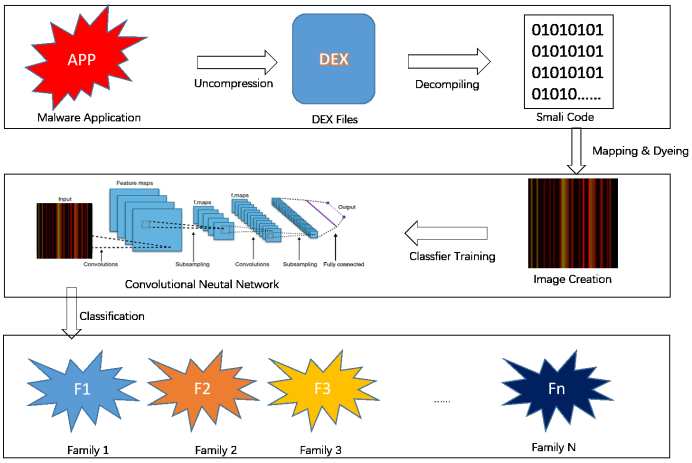


Figure 1: The whole procedure of the malware family identification

3.1 System Architecture

Figure 1 shows the working flow of our method. Firstly, we decompile the application and extract the Opcodes; Secondly, mapping the different Opcodes to pixels in R channel of the RGB image, and then colouring some sensitive API packages in G channel, highlighting the risky API functions in B channel. Thirdly, merging the three R, G, B channels to generate the feature image. Finally, using machine learning to model the features and identify different family fingerprints automatically.

3.2 Android Malware Decompilation

An Android application is commonly written in Java and compiled to Dalvik bytecode which contained in a .dex file. This file can be just-in-time compiled by the Dalvik virtual machine or compiled once into a system-dependent binary by ART on the Android paltform. Table 1 is the structure of the .apk file that the Android applications are packaged in. It contains the Dalvik executable .dex file. The Androidmanifest.xml used to describes the content of the package, including the permissions information. The native code (optional) in form of executables or libraries is usually called from the .dex file. Also, it contains the digital certification for authentication and the resources that the app uses, for instance, image files, sounds, *etc.*

The .dex file is a binary container for the bytecode and the data within the classes. The structure of a .dex file is showed in Table 2. This file is partitioned into a number of sections. After the header and before the data section, it contains the actual code. There are several identifier lists that contain offsets pointing to the corresponding entries in the data section. Due to the data section is the section that contains the actual code, and other sections are just for complimentary descriptions. So, for malwares family identification, we extract the fingerprint features from the data section to reduce the interferences of other sections.

Table 1: The structure of apk file

File or directory	Function
META-INF/MANIFEST.MF	The Manifest file
META-INF/CERT.RSA	The certificate of the application
META-INF/CERT.SF	The list of resources and SHA-1 digest of the corresponding lines in the MANIFEST.MF file
lib/	The directory containing the compiled code that is specific to a software layer of a processor
res/	The directory containing resources not compiled into resources.arsc (see below).
assets/	A directory containing applications assets, which can be retrieved by AssetManager.
AndroidManifest.xml	An additional Android manifest file, describing the name, version, access rights, referenced library files for the application.
classes.dex	The classes compiled in the dex file format understandable by the Dalvik virtual machine.
resources.arsc	A file containing precompiled resources, such as binary XML for example.

Table 2: The structure of dex file

Name	Format	Description
header	header_item	The header
string_ids	string_id_item[]	String identifiers list. These are identifiers for all the strings used by this file, either for internal naming (e.g., type descriptors) or as constant objects referred to by code.
type_ids	type_id_item[]	Type identifiers list. These are identifiers for all types (classes, arrays, or primitive types) referred to by this file, whether defined in the file or not.
proto_ids	proto_id_item[]	Method prototype identifiers list. These are identifiers for all prototypes referred to by this file.
field_ids	field_id_item[]	Field identifiers list. These are identifiers for all fields referred to by this file, whether defined in the file or not.
method_ids	method_id_item[]	Method identifiers list. These are identifiers for all methods referred to by this file, whether defined in the file or not.
class_defs	class_def_item[]	Class definitions list. The classes must be ordered such that a given class's superclass and implemented interfaces appear in the list earlier than the referring class. Furthermore, it is invalid for a definition for the same-named class to appear more than once in the list.
call_site_ids	call_site_id_item[]	Call site identifiers list. These are identifiers for all call sites referred to by this file, whether defined in the file or not.
method_handles	method_handle_item[]	Method handles list. A list of all method handles referred to by this file, whether defined in the file or not.
data	ubyte[]	The Data area, containing all the support data for the tables listed above. Different items have different alignment requirements, and padding bytes are inserted before each item if necessary to achieve proper alignment.
link_data	ubyte[]	Data used in statically linked files. The format of the data in this section is left unspecified by this document. This section is empty in unlinked files, and runtime implementations may use it as they see fit.

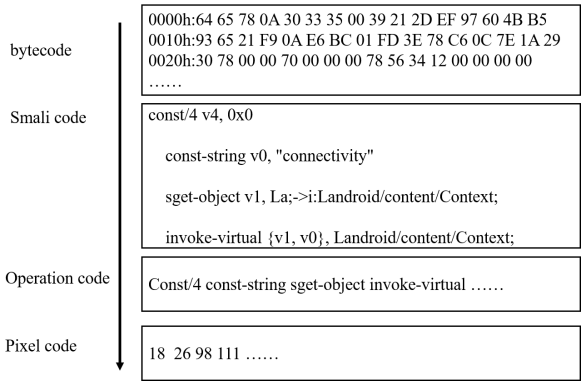


Figure 2: An example of mapping the Opcodes to pixel values in R channel of an image

3.3 Opcode Feature Extraction

Feature extraction is the basis for malware family identification. In this paper, we try to use RBG image to describe the Android malware features. The motivation is, for RGB image, there are three channels and we can use these three channels to represent different malware features integrally and simultaneously. Besides that, once we got the featured images, we can use some image processing techniques, *i.e.*, deep learning, to do feature modelling.

First of all, we should map the Opcode into R channel of RGB image. Android OS has a total of 255 Opcodes, coding from the 0x00 to 0xFF according to different functions. Here, we adopt a method similar to Nataraj *et al.* [13], mapping the Opcode to pixels by converting its hex value (encoded in Android OS) to decimal value. An example is given in Figure 2.

3.4 API Colouring

Application program interface (API) is a set of procedures, protocols, and tools for building software applications. API calls are applied in Android application development in order to implement functionalities conveniently. For example, if we want to get the phone number, we should call: $android.telephony.TelephonyManager \rightarrow getLine1Number$. API calls are also an important clue for malware identification. Wu *et al.*, [4] proposed DroidMat, which detects malware by characterizing applications using the manifest file, API call tracing and it reaches 97.87% classification accuracy. Lee *et al.*, [17] presented a detection method using runtime semantic signatures from malicious API call instructions, control and data flow, the family common string, constants, methods and classes. It reaches the 99.89% accuracy. So, the API calls are very important for malware identification.

In Android system, the API calls are usually given in parameters of a function call instruction as shown in Figure 3.

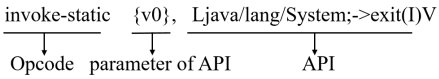


Figure 3: An API call example of a Android instruction

In order to extract the API call features, we divide them into 58 classes by their packages, as shown in Table 3. Among them, 18 classes are related to high level securities needed to focus on as shown in Table 4. They involve user privacy or device hardwares, such as camera, microphone, *etc.*

Table 3: Android APIs classification

Package Name (first level)	Package Name (second level)
android	Account animation app appwidget bluetooth content databse drm gesture graphics hardware inputmethodservice location media mpt net nfc opengl os preference provider renderscript sax security service speech support telephony text util view webkit bytecode system
java	Beans io awt lang math net nio security sql text util
javax	Crypto net security sql xml
junit	Framework runner
org.apache	Http
org	Json w3c xml
dalvik	System

3.5 Highlight the Risky APIs

In previous section, we summed up security related 18 classes from 58 Android OS classes. But the granularity is too coarse. In order to highlight some high level risky behavior, we should refine the granularity to concrete methods or functions. Therefore, 41 high level risky methods from Android OS API are extracted as shown in Table 5. And these features will be shown in B channel of the RGB image.

3.6 RGB Image Creation

In previous section, we extract opcodes, API calls, risky API features, and map them to different pixel values. After that we should integrate all the three features into a integrated RGB image as combined features. For example, if an operation is as follows:

$$invoke\{v0, v1\}, Landroid/content/Context; \rightarrow$$
$$getSystemService(Ljava/lang/String); Ljava/lang/object$$

Table 4: High level security related API classes and pixel values for G channel

#	API Package Name	Description	Pixel value
1	android.account	Account Manager	6
2	android.app	Contains high-level classes encapsulating the overall Android application model	18
3	android.bluetooth	Provides classes that manage Bluetooth functionality, such as scanning for devices, connecting with devices, and managing data transfer between devices	30
4	android.graphics	Provides low level graphics tools such as canvases, color filters, points, and rectangles that let you handle drawing to the screen directly	42
5	android.hardware	Provides support for hardware features, such as the camera and other sensors	54
6	android.media	Used to play and,in some case,record media files	66
7	android.location	Define location-based and related services	78
8	android.nfc	Provides access to Near Field Communication (NFC) functionality, allowing applications to read NDEF message in NFC tags	90
9	android.telephone	Provides APIs for monitoring the basic phone information, such as the network type and connection state, plus utilities for manipulating phone number strings	102
10	android.content	Contains classes for accessing and publishing data on a device	114
11	android.database	Contains classes to explore data returned through a content provider	126
12	android.net	Classes that help with network access, beyond the normal java.net.* APIs	138
13	java.net	Net connection relative	150
14	android.os	Provides basic operating system services, message passing, and inter-process communication on the device	162
15	android.service	Notification relative	174
16	dalvik.system	Dynamic loading relative	200
17	java.lang	Classes loading relative	212
18	others	other package	0

Then, we define the *Opcode* is *invoke*, and the parameters are $Landroid/content/Context;\rightarrow\ getSystemService$. Algorithm 1 shows how to merge the three different sort of features.

Algorithm 1 Map Opcode to RGB image

```
Begin
Accept the data Opcode,parameters.
R_pix ⇐ Call getPixelValue(Opcode)
if parameters is SensitiveAPI/*given in Table 4*/ then
    G_pix ⇐ Call getGPixelValue(parameters)
else
    G_pix ⇐ 0
end if
if parameters is RiskAPI /*given in Table 5*/ then
    B_pix ⇐ Call getBPixelValue(parameters) /*get from Table 5*/
else
    B_pix ← 0
end if
Image ⇐ Call merage(R_pix,G_pix,B_pix)
End
```

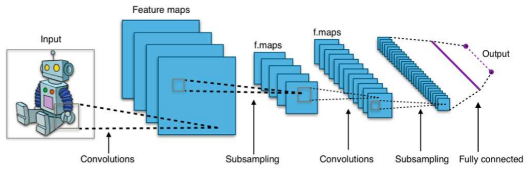
4 Features Modelling and Machine Learning

Traditional machine learning techniques were limited in their ability to process natural data in their raw form, for example, the pixel based image data. Deep learning allows computational models that are composed of multiple processing layers to learn representations of raw data with multiple levels of abstraction [11]. Deep learning techniques, powered by advanced computation ability and large datasets, have shown great performance in strategic games like Go [16], ImageNet competition [14], language translation and speech recognition. A very important paper published recently in Nature [5] also validates that deep constitutional neural network exhibits very high melanoma classification ability. In this paper, the author utilized a GoogleNet Inception v3 CNN architecture with well trained weights on 1.28 million ImageNet data. The final layer is removed and finely tuned to the author categorized dataset containing more than 13,000 images which was collected from a combination of open-access dermatology repositories. The experimental results show it has exceeded the common well trained dermatologists (72.1% vs 66.0%)

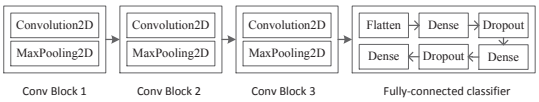
In this paper, we adopt Convolutional Neural Network (CNN) to identify the previous Android malware images. For CNN, Fukushima [7] proposed a calculation model for *CNN* in 1980 firstly based on local connections between neurons and hierarchical transformation. Based on this model, LeCun *et al.* [9] proposed the first real *CNN* multilayer network structure learning algorithm and used it for handwritting digit recognition. The model can automatically extract local features of image with strong adaptability. Parameters sharing makes it more similar to the

Table 5: High level risky API and its pixel values for B channel

API class	Method or function	Description	Pixel value
java.lang.Runtime	exec	execute script	220
android.content.Intent	startActivity	mail	210
android.app.PendingIntent	send	delayed trigger	200
android.app.AlarmManager	Set	delayed trigger	200
android.content.pm.PacakageManager	removePackageFromPrefe	uninstall application	190
android.database.sqlote.SQLiteDatabase	execSQL	database related	180
android.content.ContentResolver	delete	delete data	170
android.app.AcitivityManager	killBackgroudProcess	kill process	160
android.media.MediaRecorder	MediaRecorder	sound record	150
java.net.HttpURLConnection	connect	internet connection	140
java.net.URLConnection	connect	internet connection	140
org.apache.http.impl.client	DefaultHttpClient	internet connection	140
android.content.BroadcastReceiver	abortBroadcast	intercept SMS	63
android.telephony.PhoneStateListener	onCallStateChanged	monitor phone status	130
android.content.Intent	getAction	monitor broadcast	120
javax.crypto.Cipher	getInstance	encryption/decryption	110
javax.crypto.Cipher	Init	encryption/decryption	110
javax.crypto.Cipher	doFinal	encryption/decryption	110
android.telephony.TelephonyManager	getLine1Number	get phone number	100
android.content.pm.PacakageManager	getInstallerPackageName	get application information	90
android.content.pm.PacakageManager	getInstalledPackages	get application information	90
android.content.pm.PacakageManager	getInstalledApplications	get application information	90
android.location.LocationManager	getLastKnownLocation	get location information	80
android.telephony.TelephonyManager	getCellLocation	get location information	80
android.telephony.TelephonyManager	getSubscriberId	get IMSI	71
android.telephony.TelephonyManager	getDeviceId	get IMEI	70
android.telephony.SmsManager	sendTextMessage	send SMS	64
android.telephony.gsm.SmsManager	sendMultipartTextMessage	send multipart SMS	62
android.telephony.SmsManager	sendMultipartTextMessage	send multipart SMS	62
android.telephony.gsm.SmsManager	sendDataMessage	send multimedia message	61
android.telephony.gsm.SmsManager	sendTextMessage	send multimedia message	61
android.telephony.SmsManager	sendDataMessage	send multimedia message	61
android.telephony.gsm.SmsManager	getDisplayOriginatingAddress	read SMS	60
android.telephony.gsm.SmsManager	getDisplayMessageBody	read SMS	60
dalvik.system.DexClassLoader	loadClass	dynamic loading	50
dalvik.system.PathClassLoader	loadClass	dynamic loading	50
android.content.ContentResolver	update	tamper	40
android.content.ContentResolver	insert	insert	30
android.ContentResolver	query	traverse	20
android.content.Intent	setDataAndType	install	10



(a) Structure of the LeNET network



(b) Structure of our used CNN network

Figure 4: Structure of the LeNET network and the used CNN network

biological neural network and reduces the complexity of the network model.

The CNN structure (Figure 4(b)) used in this paper is modified from Lenet-5 [10] as shown in Figure 4(a). Our architecture consists of three sets of convolutions, activation, and pooling layers, followed by a fully-connected layer, activation, another fully-connected, and finally a softmax classifier. The convolution layer will learn 20 convolution filters, where each filter is of size 5x5. The input dimensions of this value are the same width, height, and depth as our input images. If each input feature image is shown as x_i, learn-able weight value w_{ij}, then the output feature image is:

$$y_j = b_j + \sum_i w_{ij} * x_i \tag{1}$$

Where "*" is a convolution operator, and b is a learn-able bias parameter.

The purpose of convolution layer is to extract different features from the input layer. The first layer can only extract convolution low-level features such as edges, lines, angles, *etc.*, more layers of the network can extract more complex features from low-level features in iteration.

The output feature image adopts an activation function $R = h(y)$ for non-linear mapping. The original LeNet architecture used $Tanh$ activation functions rather than $ReLU$. But in this paper we use $ReLU$. The reason is that $ReLU$ tends to give much better classification accuracy. The comparison results will be discussed in Section V. The $ReLU$ is defined as:

$$f(y) = \max(0, y) \tag{2}$$

and the $Tanh$ is defined as:

$$R = \frac{e^y - e^{-y}}{e^y + e^{-y}} \tag{3}$$

Activation function can enhance the non-linear characteristic of the decision function and the whole neural network, but does not change the Convolution layer itself.

The $ReLU$ activation function followed by 2x2 max-pooling in both x and y directions with a stride of 2 to reduce training parameters. It divides the input image into several rectangular regions, and outputs the maximum value for each subregion. The max-pooling layer will constantly reduce the size of the data space, so the number of parameters and the amount of computation will drop. Also, it can control the overfitting during training to a certain extent. Typically, the CNN convolutional layer is periodically inserted into the pool layer.

After the third subsampling layer (S2), we flatten the output feature image to vector and link it to three fully connected layers whose dimensions are 512, 256, 13 (number of malware categories) respectively. And after the first two fully connected layers, there is a dropout layer whose probability is 0.5 to avoid overfitting. The first two fully connected layers adopt $ReLU$ as activation function and the last one (Loss Layer) uses $softmax$, which is defined as:

$$\sigma(Z)_j = \frac{e^{Z_j}}{\Sigma_{k=1}^{K}} for\ j = 1, ..., K. \tag{4}$$

The $softmax$ is used to determine how the training process "punishes" the difference between the predicted results and the actual results of the network.

5 Experiments and Analysis

The experimental dataset is downloaded from the Drebin Dataset of Techinische Universität Braunschweig [1]. The dataset contains 5,560 applications and we choose 14 representative families to do our experiments. The malware samples distribution of the experimental dataset is shown in Table 6. The experimental programs are written in Python, and the hardware environment is Intel Core i7-3370 and 12GB main memory.

Table 6: The experimental android malware samples

#	Malware family	Number of samples
1	FakeInstaller	925
2	DroidKungFu	666
3	Plankton	625
4	Opfake	612
5	BaseBridge	327
6	Iconosys	152
7	Kmin	147
8	FakeDoc	131
9	DroidDream	81
10	MobileTx	69
11	FakeRun	61
12	SendPay	59
13	Gappusin	58
14	Imlog	43

5.1 The Fingerprint Image of Malware Family

In order to train the model by CNN preferably, different malware feature images should zoom into the same size, here 64x64. As shown in Figure 5, images generated by malware variants from the same family have some specific similar textures in some area. Figure 6 shows an example of the difference between Opcode features and the features after combined three channels. It shows that the combined features can describe more details of each malware family.

Based on this feature image, the identification results of our method are shown in Table 7. To evaluate the results scientifically, we use the Accuracy, TPR (true positive rate, also call Recall), FPR (false positive rate), Precision, F1, and receiver operating characteristic curve (ROC). All the metrics have the following definitions:

$$
\begin{aligned}
Accuracy &= \frac{TP+TN}{P+N}, \\
TPR &= \frac{TP}{TP+FN} \\
FPR &= \frac{FP}{FP+TN}, \\
Precision &= \frac{TP}{TP+FP} \\
F1 &= \frac{2 \times Precision \times TPR}{Precision + TPR}
\end{aligned}
$$

Where, TP is the number of true positive predictions, FP is the number of false positive predictions, and FN is the number of false negative predictions. And the F1 score is as a weighted average of the precision and TPR. The F-measure or balanced F-score (F1 score) is the harmonic mean of precision and TPR. From the experimental results, we can see that our algorithm performs well at Opfake family at 96.91%. Since there are only 58 samples in *Gappusin* family, and the identification result is not as good as other families.

5.2 The Identification Accuracy of Different Feature Representations

Figure 7(a) shows a comparison of the identification accuracy between the Opcode feature and the combined features (Opcde feature, API feature and risky API feature). It shows that the combined features perform better than just Opcode feature on malware family identification. That is to say, the API call and the risky API functions can significantly improve the texture features on different families to some degree. Although for different families, the improvements are not the same, but the effect is positive.

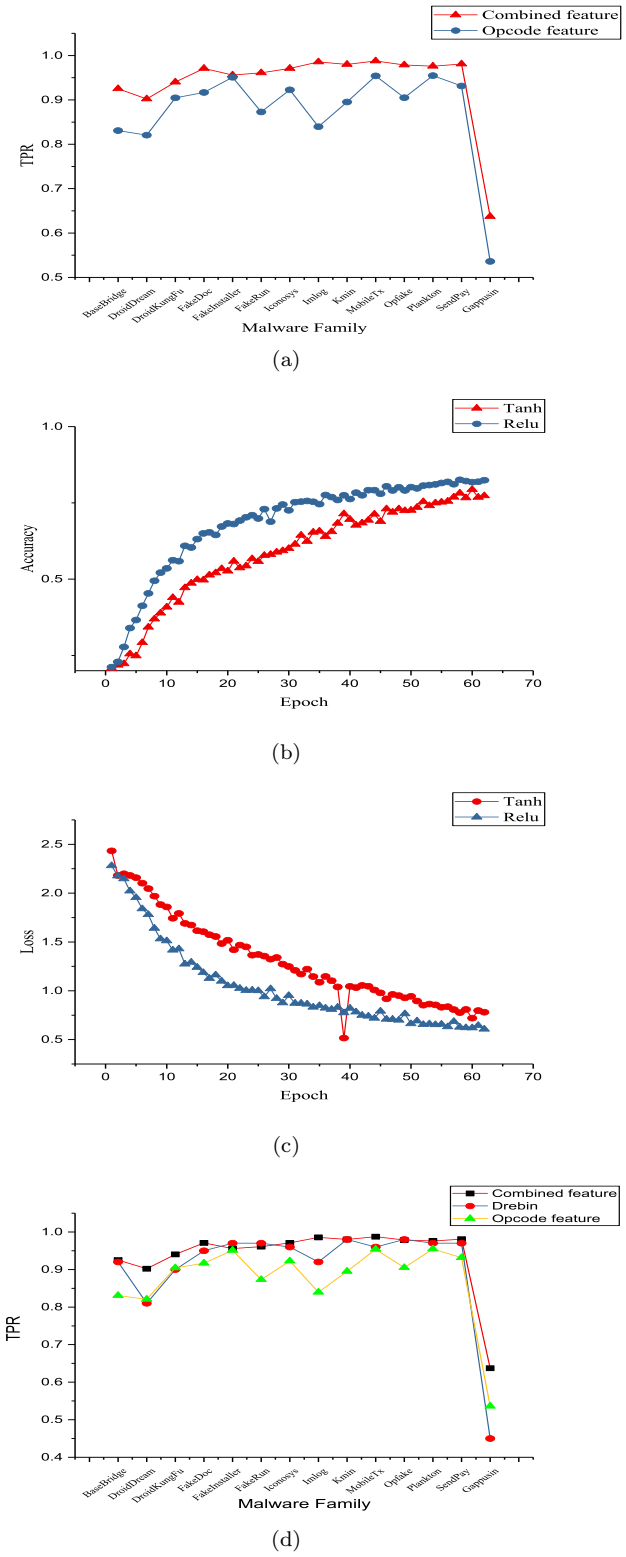
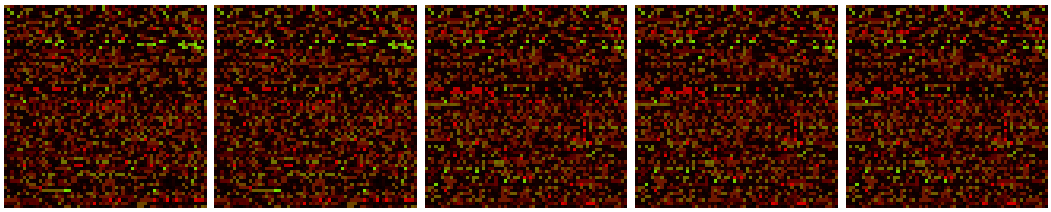


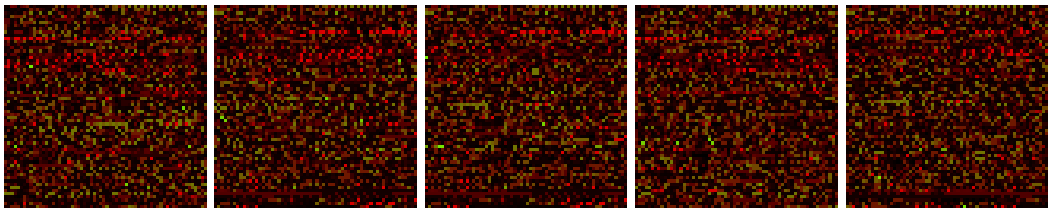
Figure 7: (a) Comparison of the TPR between the combined features and Opcode feature (only R_channel); (b) Comparison of different activation functions for identification accuracy; (c) Comparison of different activation functions for loss; (d) Comparison of TPR between Combined feature, Opcode feature and Drebin's method

Table 7: Experimental results with different metrics

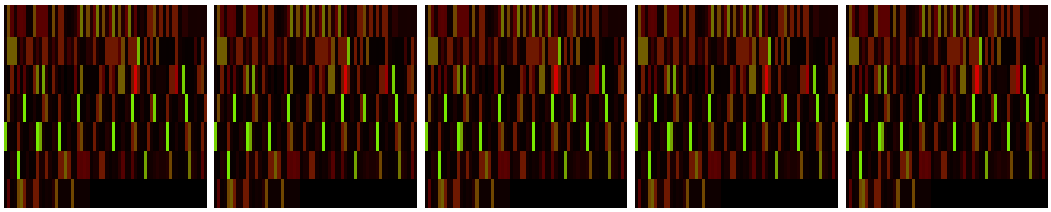
Malware Family	Accuracy	TPR	FPR	Precision	F1
BaseBridge	0.9338	0.9253	0.0020	0.9807	0.9520
DroidDream	0.8966	0.9021	0.0020	0.9492	0.9250
DroidKungFu	0.8855	0.9402	0.0460	0.9015	0.9200
FakeDoc	0.9362	0.9710	0.0010	0.9419	0.9560
FakeInstaller	0.9629	0.9560	0.0070	0.9911	0.9730
FakeRun	0.8977	0.9610	0	0.9180	0.9390
Iconosys	0.9495	0.9710	0.0500	0.9617	0.9660
Imlog	0.8710	0.9857	0.0	0.8604	0.9190
Kmin	0.9619	0.9800	0.0010	0.9727	0.9760
MobileTx	0.9293	0.9876	0.0	0.9192	0.9520
Opfake	0.9691	0.9787	0.0070	0.9795	0.9790
Plankton	0.9698	0.9760	0.0060	0.9821	0.9790
SendPay	0.9647	0.9809	0.0010	0.9880	0.9840
Gappusin	0.5663	0.6373	0.0	0.7245	0.6780
Average	0.9067	0.9395	0.0090	0.9336	0.9356



(a) BaseBridge family

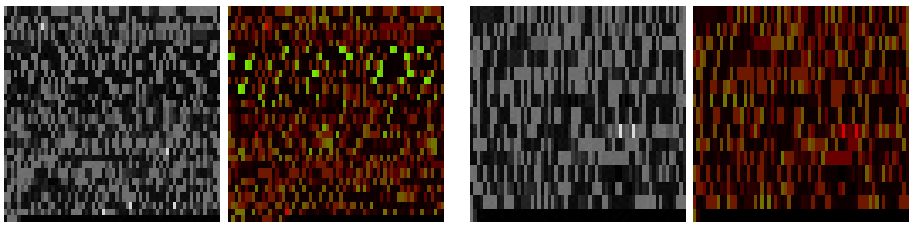


(b) DroidDream family



(c) Iconosys family

Figure 5: The fingerprint feature images of different malware families



(a) Iconosys family (b) FakeInstaller family

Figure 6: Examples of the difference between Opcode features and combined features of three channels

5.3 Comparison of Different Activation Functions on Accuracy

In neural networks, the *neuron* is a computational unit that takes as input x_1, x_2, x_3 , and outputs $h_{W,b}(x) = f(W^T x) = f(\sum_{i=1}^{3} W_i x_i + b)$, where $f : \Re \mapsto \Re$ is called the activation function. The activation function affects the training speed and final result of the whole model. It is very important for the generation of the whole model.

Tanh and *Relu* are the two typical activation functions, we use both of them in our experiment, and the effect of each function are compared in Figure 7(b) and Figure 7(c). From Figure 7(b), it shows that the *Relu* can get a better accuracy than that of *Tanh*, and the convergence rate of *Relu* is faster than that of *Tanh*. Figure 7(c) shows the effects of different activation functions on misclassification rate (loss) on the testing dataset, we can see that *Relu* is better on over-fitting than that of *Tanh*.

5.4 Comparison With the Drebin Method

Figure 7(d) shows the true positive rate (TPR) comparison among combined feature, Opcode (on R_channel) feature and Drebin's method. We can see that although Opcode feature shows the similar performance with Drebin in some family, while for the overall performance, the Opcode feature is still better than Drebin's. Furthermore, when considering the combined features, the overall detection rate has improved a lot. We can get that in most cases, the combined features are better than that of Drebin and Opcode only.

For *ROC* curve, in Figure 8, we can get similar conclusions that for different malware families, using combined features, the *ROC* curve is closer to the upper left corner of the coordinates. That is to say that using combined feature we can get better results in general.

6 Conclusions and Future Work

In this paper we propose a malware identification algorithm which combines malware visualization method and machine learning techniques. First of all, we extract the Opcode features, API calls features and high risky API function features. Then we adopt convolutional neural network to train the fingerprint images and identify the malware families. The experimental results show that the classification accuracy can be 96.91% at best and the average accuracy is higher than DREBIN [1] on the same malware dataset. Besides that, the experimental results show once again that Android malware variants in the same family have some common textures in feature image.

About the future work, we can consider the following directions:

1) Using parallelization techniques to accelerate classification and detection speed.

2) Study further to detect effectively when malwares using packing, encryption, anti-debugging, anti-dissembling techniques.

3) Integrate the proposed static method with dynamic analysis to extend the robustness and adaptability of the detection system.

Acknowledgments

This work is partially sponsored by National Key Research and Development Program of China (2016YFB0700504), Shanghai Municipal Science and Technology Commission (15DZ2260301), Natural Science Foundation of Shanghai (16ZR1411200). The authors gratefully appreciate the anonymous reviewers for their valuable comments.

References

[1] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, "Drebin: Effective and explainable detection of android malware in your pocket," in *Network and Distributed System Security Symposium*, pp. 1–12, 2014.

[2] Y. Chao, X. Zhaoyan, G. Guofei, V. Yegneswaran, and P. Porras, "Droidminer: Automated mining and characterization of fine-grained malicious behaviors in android applications," in *European Symposium on Research in Computer Security*, pp. 163–182, 2014.

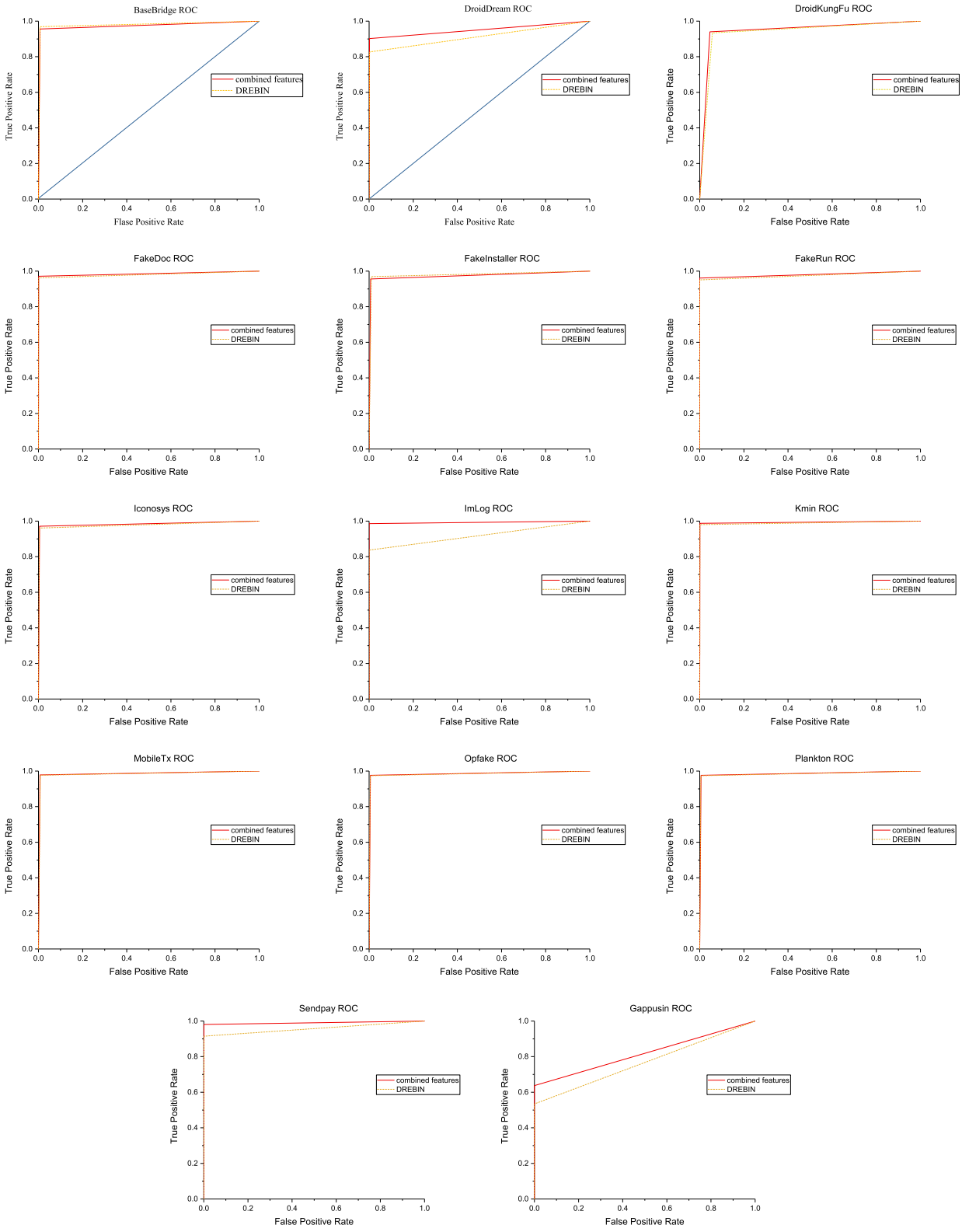


Figure 8: ROC curve of different malware families with different algorithms

[3] M. Dimjaševic, S. Atzeni, L. Ugrina, and Z.Rakamaric, "Android malware detection based on system calls," *University of Utah, Technical Report*, UUCS-15-003, 2015.

[4] W. Dong-Jie, M. Ching-Hao, W. Te-En, L. Hahn-Ming, and W. Kuo-Ping, "Droidmat: Android malware detection through manifest and API calls tracing," in *Proceeding Seventh Asia Joint Conference Information Security*, pp. 62–69, Aug. 2012.

[5] A. Esteva, B. Kuprel, R. Novoa, J. Ko, S. Swetter, H. Blau, and S. Thrun, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, pp. 115–118, 2017.

[6] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwisle, B. Graveland, D. Mckinney, and J. Mulcahy, "2010 symantec internet security threat report," *Volume*, no. 5, pp. 277–278, 2011.

[7] K. Fukushima, "Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position," *Biological Cybernetics*, vol. 36, no. 4, pp. 193–202, 1980.

[8] P. Hao, C. Gates, B. Sarma, L. Ninghui, Q. Yuan, R. Potharaju, C. Nita-Rotaru, and L. Molloy, "Using probabilistic generative models for ranking risks of android apps," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 241–252, 2012.

[9] Y. LeCun, B. Boser, J. Denker, D. Henderson, R. Howard, W. Hubbard, and L. Jackel, "Backpropagation applied to handwritten zip code recognition," *Neural Computation*, vol. 1, no. 4, pp. 541–551, 1989.

[10] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.

[11] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[12] Z. Mu, D. Yue, Y. Heng, and Z. Zhiruo, "Semantics-aware android malware classification using weighted contextual api dependency graphs," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1105–1116, 2014.

[13] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: Visualization and automatic classification," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, pp. 4, 2011.

[14] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, *et al.*, "Imagenet large scale visual recognition challenge," *International Journal of Computer Vision*, vol. 115, no. 3, pp. 211–252, 2015.

[15] B. Sanz, L. Santos, C. Laorden, X. Ugarte-Pedreror, P. Bringas, and G. Álvarez, "Puma: Permission usage to detect malware in android," in *International Joint Conference CISIS´ 12-ICEUTE´ 12-SOCO´ 12 Special Sessions*, pp. 289–298, 2013.

[16] D. Silver, A. Huang, C. Maddison, A. Guez, L. Sifre, G. V. D. Driessche, J. Schrittwieser, L. Antonoglou, V. Panneershelvam, M. Lanctot, *et al.*, "Mastering the game of go with deep neural networks and tree search," *Nature*, vol. 529, no. 7587, pp. 484–489, 2016.

[17] L. Suyeon, L. Jehyun, and L. Heejo, "Screening smartphone applications using behavioral signatures," in *IFIP International Information Security Conference*, pp. 14–27, 2013.

[18] F. Tchakounté and P. Dayang, "System calls analysis of malwares on android," *International Journal of Science and Technology*, vol. 2, no. 9, pp. 669–674, 2013.

[19] Z. Yajin and J. Xuxian, "Dissecting android malware: Characterization and evolution," in *2012 IEEE Symposium on Security and Privacy (SP'12)*, pp. 95–109, 2012.

[20] H. You-Joung and L. Hyung-Woo, "Detection of malicious android mobile applications based on aggregated system call events," *International Journal of Computer and Communication Engineering*, vol. 3, no. 2, p. 149, 2014.

[21] W. Yu, Z. Hanlin, G. Linqiang, and R. Hardy, "On behavior-based detection of malware on android platform," in *Global Communications Conference (GLOBECOM'13)*, pp. 814–819, 2013.

Biography

Yong-liang Zhao is a master degree student in the school of computer science, Shanghai University. His research interests include cloud computing, big data analysis, computer and network security especially in android platform.

Quan Qian is a full Professor in Shanghai University, China. His main research interests concerns computer network and network security, especially in cloud computing, big data analysis and wide scale distributed network environments. He received his computer science Ph.D. degree from University of Science and Technology of China (USTC) in 2003 and conducted postdoc research in USTC from 2003 to 2005. After that, he joined Shanghai University and now he is the lab director of network and information security.

Secure and Efficient Cloud Data Deduplication Supporting Dynamic Data Public Auditing

Hua Ma, Xiaoyu Han, Ting Peng and Linchao Zhang
(Corresponding author: Xiaoyu Han)

School of Mathematics and Statistics, Xidian University
No. 2, South Taibai Road, Xi'an 710071, P.R. China
(Email: xyhan0723@163.com)
(Received May 27, 2017; revised and accepted Oct. 21, 2017)

Abstract

Secure data deduplication, which can reduce the amount of storage cost in the cloud by eliminating duplicate data copies, has been widely used in industry and academia. At the same time, as the outsourced cloud storage server is not fully credible, it will cause data destruction when the user puts the the encrypted data in the cloud. Therefore, we present a secure and efficient cloud data deduplication scheme supporting dynamic data public auditing. Compared with the prior systems, our system has two advantages. Firstly, the proposed scheme has a high performance in terms of data equality test by using the decision tree, as the server can reduce the time complexity of deduplication equality test from linear to logarithmic over the whole data items in the database. Secondly, the proposed scheme can reduce the computation cost of searching a data block from linear to logarithmic by using relative index of a node and also support data modification, insertion, append and deletion procedure.

Keywords: Cloud Storage; Deduplication; Public Auditing

1 Introduction

Cloud computing is a pay-per-use model that provides available, convenient, and on-demand network access to configurable computing resource sharing pools (resources including networks, servers, storage, applications and services). These resources can be quickly provided with very little management effort or little interaction among the service provider.

Among them, cloud storage is a networked storage model that data is stored in a virtual storage pool, usually maintained by the third party. Cloud storage provides customers with a lot of benefits, including cost savings and simplified convenience, and so on. These benefits make more and more customers store their personal data in the cloud. The analysis shows that the amount of data will reach 40 trillion gigabytes in 2020, of which 70% are stored in the cloud. Among these remote stored files, most of them are identical. Data deduplication, a special data compression method, has been widely used in cloud to optimize storage space by reducing the amount of data storage [5, 14, 20]. Nevertheless, the problem, that the same file encrypted by different users lead to different ciphertexts, makes cross-user deduplication impossible. The convergence encryption(CE) can implement this, because the key is derived from the file, regardless of who performs the encryption algorithm. However, existing solutions in use unfortunately have either security or privacy issues. Such as offline dictionary attacks as the keys are derived deterministically from the file F $(i.e., K_A(= K_B) = H(F))$, where H is a conventional hash function used to map any length of messages into a fixed-length value.

At the same time, the users put the data in the cloud and need to consider the data security. Because the Cloud Service Provider (CSP) may take the initiative to delete the data that the client does not frequently access, so it is necessary for users to ensure the integrity of data in the cloud. In other words, any change about the data in the cloud without the consent of the user, such as data loss, corruption, modification, or disclosure, should be detected by the user. However, as the user's computing power is limited, the user decides to authorize the task of auditing to a Third Party Auditor (TPA), which enables that the user can efficiently perform integrity verifications even without the local copy of data. TPA replaces the user to perform the integrity of data and do not need to download the entire file.

We also consider that the user may want the cloud to protect their data to prevent unauthorized users from accessing. So we use a key distribution mechanism to process the convergence key [16, 26].

In this paper, we propose a secure and efficient cloud data deduplication scheme supporting public auditing. Our main contributions can be summarized as follows.

- A secure and efficient cloud data deduplication

scheme is achieved [13, 24], and can reduce the comparison times of the equality-testing algorithm from linear to nearly logarithmic.

- An auditing entity can help clients audit the integrity of data stored in the cloud even without the local copy of data files [9]. At the same time, the computational cost of searching the data block can reduce efficiently from linear to logarithmic. In addition, the scheme supports the dynamic operation of data.

- A scheme of data deduplication by using a key encapsulation mechanism [16, 26], which means that the key of the file is re-encrypted with the attribute, and the user can decrypt the ciphertext only if the user has a private key associated with the attribute.

In Section 2, we give the relevant knowledge of deduplication and auditing. In Section 3, we give the bilinear pairings, computational Diffie-Hellman problem, Path-PRV-CDA2, modified Merkle Hash Tree, Boneh-Lynn-Shacham signature and equality test over deduplication decision tree. Section 4 gives system structure and the threat model. Our detailed scheme is shown in Section 5. The dynamic operation of the modified $\mathcal{MHT}$ tree will be showed in Section 6. The Section 7 gives the security. The Section 8 gives the performance analysis. We make a conclusion in Section 9.

2 Related Works

In this section, we will elaborate on the work related to our scheme from two aspects.

2.1 Secure Deduplication

Convergent encryption, which can not only guarantee the confidentiality of data, but also achieve data deduplication. Specifically, each data file will be encrypted with a so-called convergence key that derived from the cryptographic hash value of the file contents. This gives rise to the same data file to be encrypted to get the same ciphertext, which makes it possible to reduce the redundant data. Bellare *et al.* [5] proposed a novel cryptographic primitive called Message-Locked Encryption (MLE), where the formal definition and security model of deduplication is given. However, both of them do not meet semantic security because of content-guessing attack. If the adversary wants to specify a distribution of plaintexts, the tag that is deterministic from the message will leak unnecessary information. To strengthen the security, Abadi *et al.* [1] proposed a modified primitives, named random Message-Locked Encryption (R-MLE) which can support an equality-testing algorithm defined on the ciphertexts. However, the equality-testing algorithm is very inefficient, which is the only problem. To enhance the security of deduplication and protect the data confidentiality, Bellare *et al.* [4] proposed an improved deduplication scheme, which can resist the online brute-force attack by running an oblivious pseudo-random function (OPRF). In the scheme, users generate the key by the aid of a secret parameter which is produced by a third-part key server. To prevent the data from being leaked to the third-part server, Bellare and Keelveedhi extended their prior work and proposed a new primitive named Interactive Message-Locked Encryption (iMLE) [3]. In their model, security depends on whether the message is related to the public parameter or not. After that, Jiang *et al.* [13] introduced a new primitive called μR-MLE2, which generates a key that does not depend on the third party, and can resist content-guessing attack. The most important is that the time of deduplication test is reduced from linear to logarithmic.

2.2 Integrity Auditing

Ateniese *et al.* [2] put forward the concept of provable data possession (PDP), which makes sure that the cloud server owns indeed the data and does not need to download all the data. PDP implements mainly through randomly extracting a set of data blocks from the cloud server. Zhang *et al.* [28] proposed a secure provable data possession scheme, which can resist forgery attack and replay attack, under the Chosen-Target-CDH problem and the CDH problem. Proof of retrievability (POR) [19] is also a part of the data integrity verification. Compared with PDP, POR can also achieve the recovery of data. Ling *et al.* [17] proposed an efficient and secure one time password authentication scheme for wireless sensor networks. Xu and Chang [25] recommended to use the polynomial commitment to reduce the communication cost of [19]. Stefanov *et al.* [21] made a protocol to the frequent changes in the authentication file system. Hsien *et al.* [10] presented a survey of data integrity based on public auditability and provided the approach to analyze security and efficiency. Hwang *et al.* [11] proposed a scheme with a mechanism to locate the problematic data blocks when the cloud data as a whole fails the auditing. Ming *et al.* [27] implemented a more secure and efficient auditing mechanism in the cloud. Cao *et al.* [8] showed that there are two flaws in one scheme for cloud storage auditing with verifiable outsourcing of key updates. However, these protocols only adapt to the static operation of the data and do not support the dynamic one. Liu *et al.* [18] considered dynamic data update when the data is shared with multiple users, but only described the inserted operation. The scheme [12, 23] supports the dynamic operation of the data, the time of integrity verification is $O(m)$. The computational complexity of integrity verification is proportional to the amount of data in the cloud. When the amount of the data in the cloud increases, the computational complexity will increase linearly. Garg *et al.* [9] improved it by using Relative Index and Time Stamped Merkle Hash Tree ($\mathcal{RITS}--\mathcal{MHT}$), which can guarantee that it can not only support the dynamic operation of the data, but the computation cost of searching the node

can reduce from linear to sub-linear.

3 Preliminaries

In this section, we give bilinear groups and computational Diffie-Hellman problem, Path-PRV-CDA2. At the same time, in order to achieve the integrity of the data, we give the modified Merkle Hash Tree ($\mathcal{MHT}$), Boneh-Lynn-Shacham ($\mathcal{BLS}$) signature and equality test over deduplication decision tree.

3.1 Bilinear Pairings

Suppose that G and G_T are the multiplication cycle groups of prime order p. When the map $e : G \times G \to G_T$ satisfies the following properties, we say that e is a bilinear map [6, 22]:

1) **Bilinearity**: For all $u, v \in G, a, b \in Z_p$, we can deduce that $e(u^a, v^b) = e(u, v)^{ab}$;

2) **Non-degeneracy**: $e(g, g) \neq 1$;

3) **Computability**: For all $u, v \in G$, we can compute $e(u, v)$ in an efficient algorithm.

3.2 Computational Diffie-Hellman Problem

The Computational Diffie-Hellman problem (CDH) [6] is that, given $g, g^a, g^b \in G$, it is difficult to compute g^{ab}, where a, b is the random number in Z_p^* and g is the generator of G.

3.3 Path-PRV-CDA2

In the decision tree, the user interacts with the server, calculates 1 bit path decision and sends it to the server. The definition of Path-PRV-CDA2 [13] is based on the definition of PRV-CDA2 [1].

3.4 Modified Merkle Hash Tree

Modified $\mathcal{MHT}$ [9] is a binary search tree, where each node stores two parts of information, one is the hash value of the data block and the other is the relative index of the node. Apart from the leaf nodes, the hash value of each node is the concatenation of the hash value of its child nodes. By verifying the hash value of root node, we can assure the integrity of data. In modified $\mathcal{MHT}$, the relative index of leaf nodes is set to 1. Suppose that the index value of a node's two child nodes is r_a and r_b, then its index value is $r_a + r_b$.

Figure 1 shows a modified $\mathcal{MHT}$ with 8 leaf nodes. For example, if the auditor wants the cloud server to prove the integrity of the data block $d[3]$, the cloud server will give the auditor the Auxiliary Information (AI) as $AI(d[3])$:

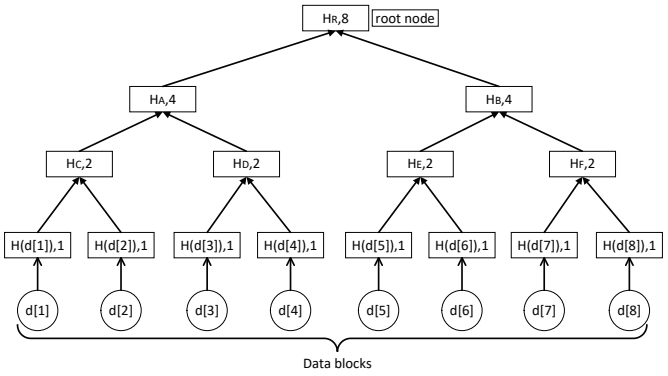


Figure 1: Modified merkle hash tree ($\mathcal{MHT}$)

$\{(H_C, L), H(d[3]), (H(d[4]), R), (H_B, R)\}$. Now the auditor verifies the integrity by using the root node H_R as follows:

Compute $H_D \leftarrow (H(d[3]) \parallel H(d[4]))$.

Compute $H_A \leftarrow (H_C \parallel H_D)$.

Finally compute root $H_R \leftarrow (H_A \parallel H_B)$.

3.5 Boneh-Lynn-Shacham Signature

Boneh-Lynn-Shacham Signature ($\mathcal{BLS}$) [7] is a short signature scheme, which is used for authentication the signer of a message. Its security is based on the CDH problem. $\mathcal{BLS}$ signature can aggregate multiple signatures about many blocks of message into a single signature. Therefore, $\mathcal{BLS}$ signature of n data blocks $(d[1], d[2], \cdots, d[n])$ in file F are generated as follows:

$$\phi = \prod_{i=1}^{n} (H(d[i]))^k$$

$H : \{0,1\}^* \to G$ is a hash function and G is a prime order group having generator g. The $\mathcal{BLS}$ signature specifically contains three parts in the following:

Let $k \in Z_p$ be the private key and g^k is the public key.

Generate a signature ϕ for file F: $\phi \to H(F)^k$.

Input the file F and signature ϕ, verify $e(\phi, g) \stackrel{?}{=} e(H(F), g^k)$.

3.6 Equality Test Over Deduplication Decision Tree

Jiang *et al.* [13] proposed an interactive deduplication decision tree in Figure 2. Generally speaking, the user requests the server to return the tag of current node. The user checks whether there is a copy, if it is, users just get a link related to file from the cloud without uploading the encrypted data. Otherwise, the user uploads the data to the cloud. In general, give $h(F)$, some relevant information and 1-bit path decision $b = B(g^{r_i \cdot h(F)})(B(x)$ denotes

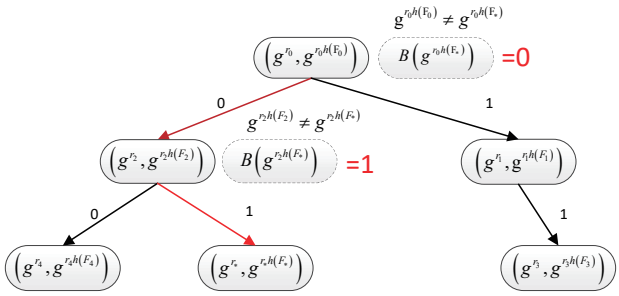


Figure 2: Deduplication decision tree

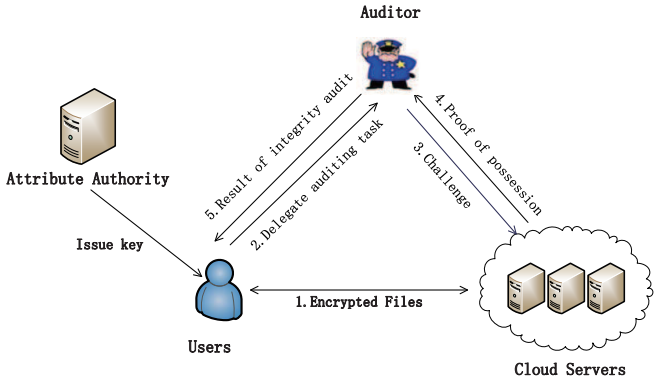


Figure 3: The system model

the bitwise exclusive or of the digest of x). If $b = 0$, the server moves it to the left child node. Else if $b = 1$, the server moves it to the right child node. The algorithm can be described as follows.

- User $\leftrightarrow$ Server: The user owns file F_* and requests the cloud server to return the tag τ_i of the current node, $\tau_i = (g^{r_i}, g^{r_i h(F_i)})$. (In general, if the node is the root one in the tree, and the corresponding tag is $\tau = (g^{r_0}, g^{r_0 h(F_0)})$.

- User: The user detects whether the cloud has the same one as himself. That is to say, the user verifies whether the equation $g^{r_i h(F_*)} \stackrel{?}{=} g^{r_i h(F_i)}$ holds.

- User $\rightarrow$ Server: When the equation is established, it means that the user finds a duplication. Otherwise, he calculates $b = B(g^{r_i h(F_*)}) \in \{0, 1\}$ and gives it to the server.

- Server: When the server gets 0, the user moves the node to the left child. Otherwise, the node is transferred to the right child. The user then continues to interact with the server and finds that one of the following cases occurs. One is that, when the server traverses the entire tree, it does not find the same data as the user. The other is that, the server finds a copy of the data.

4 Problem Formulation

4.1 System Architecture

In our system, we include four entities: the user, Cloud Service Provider (CSP), Third Party Auditor (TPA) and attribute authority (AA). The relationship among them is shown in Figure 3.

- The user has a lot of files and will generally put them in the cloud to save their own storage and reduce the computing cost.

- Cloud Service Provider (CSP) is a system that provides file storage and business access capabilities truthfully. Users often pay the cloud to enjoy this service.

- The Third Party Auditor (TPA) helps the user detect the integrity of the outsourced file in the cloud, since the cloud may delete files that is rarely used by the user or that has been corrupted to save storage.

- The attribute authority (AA) is an entity which can send the user a key related to the user's attribute to encapsulate the encryption key.

Our system contains two phases: data deduplication phase and public auditing phase.

1) Data deduplication phase: At this stage, the user detects whether CSP has the same file. We mainly have two situations to consider.

   - When CSP has already stored the data, users do not have to upload the file and only obtain a link to the file.
   - The user uses the message locked encryption to encrypt the file and uploads it to the cloud. After that AA employs the key encapsulation mechanism to encapsulate the key.

2) Public auditing phase: We introduce it mainly in four parts. They are BlockSigGen, Challenge, GenProof and VerifyProof, respectively.

   - **Keygen**(1^λ): The user inputs a security parameter λ and outputs key pair (k, g^k). Here, k is the private key, g^k is the public key.
   - **BlockSigGen**$(k, H(ct_{d(i)}), u)$: The user inputs k, the hash value of encrypted file block $H(ct_{d(i)})$, a random number u, and outputs the signature of the block is ϕ_i. The set of signatures for each encrypted block is represented as $\theta = \{\phi_i\}$, $i \in \{1, 2, \cdots, n\}$.
   - **Challenge**: TPA replaces the user to detect the integrity of data in the cloud. TPA takes several blocks of file randomly and sends them to the CSP.

- **GenProof**(ct_F, θ, C): When CSP received the challenge information C from TPA, CSP inputs encrypted File ct_F, all signature set θ, challenge information C to produces the proof P_f. Finally, CSP sends the proof to TPA.
- **VerifyProof**(C, P_f, g^k): TPA inputs the challenge Information C, proof P_f, public key g^k, and verifies the results. If it holds, it indicates that the data stored in the cloud is complete. Otherwise, we conclude that the data has been tampered or even lost.

4.2 Threat Model

We consider some threats about the users' data in the following.

- The user authorizes the task of auditing to TPA to ensure the integrity of data in the cloud. Although TPA is credible, he will be curious about the data stored in the cloud.
- CSP may delete data that is occasionally accessed by the user, or CSP may damage the data due to their own processing error without informing the user.
- The previous administrator in the cloud could break into and corrupt the integrity of data. And if the certificate of legitimate user is lost, the other users will use the certificate to destroy the data or even delete the data.

5 Our Detailed Construction

In this section, we construct a secure and efficient cloud data deduplication scheme supporting dynamic data public auditing. Our scheme mainly includes four entities which has been showed in Figure 3. Firstly, AA defines the set of public attributes [15] and sends the user a key related to the attribute. The key which is used to re-encrypt the convergence key to implement the key encapsulation. Then, the user sends a tag to CSP to decide whether the cloud stores the file or not.

5.1 Data Deduplication Phase

This phase intends primarily to detect whether the cloud has the same data by using the equality test over deduplication decision Tree.

- The user has the file F_* and the tag of F_* is $\tau_* = (g^{r_*}, g^{r_* h(F_*)})$. After that, the user requires CSP to return the tag $\tau_i = (g^{r_i}, g^{r_i h(F_i)})$ of current node. The user then detects whether there exists the same file by checking $g^{r_i \cdot h(F_*)} \stackrel{?}{=} g^{r_i \cdot h(F_i)}$, where r_i and r_* are selected randomly. If the equation is verified to be equal, it means that there is a duplicate one stored in the cloud, it is unnecessary for the user to upload the file.
- Otherwise, the user sends b ($b = B(g^{r_i h(F_*)}) \in \{0, 1\}$) to CSP, if $b = 0$, CSP moves the node to the left, otherwise it moves the node to the right. The algorithm terminates when CSP has traversed the entire tree and can not find the same data. Therefore, the user is authorized to upload the ciphertext to the cloud. Specifically, the user computes $k_F = Hash(pp, F)$, $ct_F = Enc_{pp}(k_F, F)$, and gives ct_F to CSP, where $Enc(\cdot)$ is the symmetric encryption algorithm, pp is the public parameters. The convergent keys k_F is encrypted with the key associated with the attribute. The user can get the convergence keys to decrypt the ciphertext only if he has the attribute.

5.2 Public Auditing Phase

TPA replaces the user to check the integrity of data in the cloud and returns the results to the user. Detailed details are as follows.

- **KeyGen**: The user first randomly selects the private key $k \in Z_p$ and the public key $\eta = g^k$. After that, the user divides the encrypted file into n blocks.
- **BlockSigGen**: Generally speaking, the user generates $\mathcal{BLS}$ signature for each encrypted block $ct_{d[i]}$ of the file is $\phi_i = (H(ct_{d[i]}) \cdot u^{ct_{d[i]}})^k$, where $ct_{d[i]} = Enc_{pp}(k_{d[i]}, d[i])$, $i \in \{1, 2, \cdots, n\}$ and a random element $u \in G$. Here $H(ct_{d[i]})$ indicates the hash value of the encrypted file block. The user generates a $\mathcal{MHT}$ and a root nodes H_R with $H(ct_{d[i]})$ as a leaf node for all $i \in \{1, n\}$ (H_R is the root node of the encrypted data block). The signature for the root node is expressed as $\rho = H(R)^k$. After that, the user sends $\{ct_F, \theta, \rho\}$ to CSP for storage.
- **Challenge**: In order to ensure that their files are intact, the users upload the files to the cloud and delegate the task of verifying the integrity of data to TPA. Then TPA randomly extracts a portion of the file from CSP, and CSP responds to the extracted data. TPA randomly selects Q and b_i, and sends $C \leftarrow (i, b_i)_{i \in Q}$ to CSP, where $Q = \{r_1, r_2, \cdots, r_k\} \in [1, n]$ and $i \in Q$.
- **GenProof**: When receives the challenge message C, CSP starts to search ith node in the hash tree ($i \in C$). We determine whether the search node exists in the hash tree by validating the root node. For example, we need to search for file block $d[4]$, CSP can use all the auxiliary information on the path of the search node. The auxiliary information(AI) is expressed as: $[(H_C, 2, L), (H(d[3]), 1, L), (H_B, 4, R)]$, where L represents the position of node on the left, R is represented as the position of the node on the right. SIB specifies the number of sibling nodes on the left. When the detection of the node passes, CSP continues to search for the other nodes on the hash tree. Otherwise CSP terminates the auditing and

computes:

$$\phi \leftarrow \prod_{i=r_1}^{r_k} \phi_i^{b_i} \in G.$$

and

$$\mu \leftarrow \prod_{i=r_1}^{r_k} b_i D[i] \in G.$$

After that, P_f is sent to TAP by CSP, $P_f = \{\mu, \phi, (H(ct_{d_i}), AI(i)_{i\in Q}, \rho, SIB)$. Here $AI(i)$ is the auxiliary information of i on the path from the node $H(ct_{d[i]})$ to the root node.

- **VerifyProof**: TPA establishes the root node of the tree and verifies the root node by detecting whether the following equation holds or not:

$$e(H(R), g^k) = e(\rho, g). \quad (1)$$

Here, $H(R)$ is the hash value of the root of the encrypted data block. Finally, TPA sends the verification results to the user. On authentication verification successes, TPA proceeds the auditing process and verifies whether the following equation holds or not:

$$e(\prod_{i=r_1}^{r_k} H(ct_{d[i]})^{b_i} \cdot u^{\mu}, g^k) = e(\phi, g) \quad (2)$$

That is to say,

$$\begin{aligned} & e(\prod_{i=r_1}^{r_k} H(ct_{d[i]})^{b_i} \cdot u^{\mu}, g^k) \\ =& e(\prod_{i=r_1}^{r_k} H(ct_{d[i]})^{b_i} \cdot u^{b_i ct_{d[i]}}, g^k) \\ =& e(\prod_{i=r_1}^{r_k} (H(ct_{d[i]}) \cdot u^{ct_{d[i]}})^{b_i}, g^k) \\ =& e(\prod_{i=r_1}^{r_k} ((H(ct_{d[i]}) \cdot u^{ct_{d[i]}})^k)^{b_i}, g^k) \\ =& e(\prod_{i=r_1}^{r_k} \phi_i^{b_i}, g) \end{aligned}$$

If the validation process passes, the file that the user stores in the cloud is complete. Otherwise the user's file is compromised.

6 Data Dynamic Procedures

Data dynamic operation [9] is very important in data auditing, which includes data modification procedure ($\mathcal{DMP}$), data insertion procedure ($\mathcal{DIP}$), data append procedure ($\mathcal{DAP}$) and lastly data deletion procedure($\mathcal{DDP}$). Data dynamic procedures which allow the user to update the selected file when a file block changes.

6.1 Data Modification Procedure

When the user wants to modify the ith file block, the user generates a new signature for this data block as $\phi^{'} = (H(ct_{d[i']}) \cdot u^{ct_{d[i']}})^k$, and produces a new file tag as $\tau^{'} = (g^r, g^{rh(F^{'})})$, and then the user sends $(M, i, ct(d[i^{'}]), H(ct_{d[i']})^{'}, \tau^{'})$ to CSP, where M is denoted as $\mathcal{DMP}$. Cloud storage server replaces $ct(d[i])$ with $ct(d[i^{'}])$, replaces ϕ with $\phi^{'}$, replaces τ with $\tau^{'}$, replaces $H(ct_{d[i']})$ with $H(ct_{d[i']})$, and then generates a new hash of the root node $H(R^{'})$ by reconstructing $\mathcal{MHT}$ with ith modified file block. Then the user authenticates the root by using $(H(ct_{d[i']}), AI(i))_i, \rho)$, produces $\rho^{'} = H(R^{'})^k$ with secret key k and sends it to the cloud for storage. In this way, the user completes the modification operation of the data block.

6.2 Data Insertion Procedure

When the user wants to insert the file block, the user first generates a signature for the inserted file block as $\phi^* = (H(ct_{d[i^*]}) \cdot u^{ct_{d[i^*]}})^k$ and computes the tag as $\tau^* = (g^r, g^{rh(F^*)})$. Assume that the insertion file block is $(I, i, ct(d[i^*]), \phi_i, \tau^*)$ and sends them to the CSP, where I is denoted as $\mathcal{DIP}$. When a new node is inserted, the hash value of the node at that location becomes $(H(ct(d[i])) \parallel H(ct(d[i^*])))$ and the index value of it will also change, too. Specific detail is shown in [9]. The user establishes $\mathcal{MHT}$ to authenticate the root node using $AI(I), H(ct(d[i]))$ in Equation (2), if the certification holds, it means that CSP performs the insert operation honestly.

6.3 Data Deletion Procedure

$\mathcal{DDP}$ is similar to $\mathcal{DIP}$. Assuming that we want to delete a data, then the hash value of the node is transferred, the corresponding index of the node changes, too.

6.4 Data Append Procedure

$\mathcal{DAP}$ is similar to the data insertion.

7 Security Analysis

In this part, we will analyze the security of our scheme. The Theorem 1 is reduced to that of Garg and Bawa's scheme [9], which has been proved to be secure in random oracle model. We show that our scheme is Path-PRV-CDA2 secure in Theorem 2. Finally, we give an analysis to show that the auditing is sound in Theorem 3.

Theorem 1. *As Garg and Bawa's scheme [9] is security, then an adversary $\mathcal{C}$ has an negligible advantage ϵ to generate a forgery for a data block $ct_{d[i']}$:*

$$\epsilon^{'} \geq (1/q_S + 1)e)\epsilon$$

Table 1: Functionalities and features comparison of deduplication and auditing

Schemes	Ciphertext deduplication	No additional key server	Auditing	Block dynamic operations
[1]	√	√	×	×
[9]	–	–	√	√
[13]	√	√	×	×
[15]	√	×	√	×
[23]	–	–	√	√
Ours	√	√	√	√

and in polynomial time:

$$t_c \geq t + t_{sm}(q_H + 2q_S)$$

where t_{sm} is time for one scalar multiplication in G and e is base of natural logarithm.

Proof. Assuming the attacker $\mathcal{A}$ has already known (g, g^a, g^b), our purpose is to solve the CDH problem by using a subroutine $\mathcal{B}$, $\mathcal{B}$ is maintained by $\mathcal{A}$.

Parameter Query: The adversary $\mathcal{C}$ makes queries to $\mathcal{B}$ about the relevant system parameters , and $\mathcal{B}$ responds it in the following, $\mathcal{B}$ chooses $r \in Z_p$ as its own private key, generates $g^r \in G$ as the public key, and sends (r, g^r, G) to the adversary, where r keeps secret.

Hash Query: The adversary $\mathcal{C}$ can make a Hash Query, $\mathcal{B}$ responds it as below. The adversary $\mathcal{C}$ also makes a list L_H: $\{ct_{d[i]}, w_i, k_i, c_l\}$, which is initially empty.

- If there has been a query on $ct_{d[i]}$ in the L_H, $\mathcal{B}$ responds with $H(ct_{d[i]}) = w_i$.
- Otherwise, $\mathcal{B}$ flips a coin $c \in \{0, 1\}$, when $c_l = 0$, the probability of it is δ. And when $c_l = 1$, the probability of it is $1 - \delta$.
- $\mathcal{B}$ chooses a element $k_i \in Z_p$ randomly, computes $w_i = (g^b)^{(1-c_l)}\phi(g)^{k_i}$ and puts $\{ct_{d[i]}, w_i, k_i, c_l\}$ to list L_H.

Sign Query: The adversary makes a signature inquiry about the data block $ct_{d[i]}$, and $\mathcal{B}$ replies to him as follows:

- If $c_l = 0$, $\mathcal{B}$ halts.
- Otherwise, if $c_l = 1$, then $\mathcal{B}$ responds with $\sigma_i = (\phi(g^a)^{k_i})(\phi(g)^{k_i r})$. Here $w_i = \phi(g)^{k_i}$, therefore $\sigma_i = w_i^{a+r}$.
- Assume that the adversary $\mathcal{C}$ has created a forged signature σ_k^* for the data block $ct_{d[k]}$, Then if $c_l = 1$, $\mathcal{B}$ halts. when $c_l = 0$, B replies to the adversary with $H(ct_{d[k]}) = g^b\phi(g)^k$ and σ_k^*.
  Then we can derive that:

$$g^{ab} = \sigma_k^*/(g^{rb}\phi(g^{ak})\phi(rk)).$$

Only $\mathcal{B}$ can calculate g^{ab} in the polynomial time.

Next, we show the probability that the CDH problem can be solved by $\mathcal{B}$. $\mathcal{B}$ wants to succeed mainly based on the following three cases:

- E_1: Any sign of an adversary $\mathcal{C}$ does not make $\mathcal{B}$ stop the game;
- E_2: The adversary $\mathcal{C}$ generates a genuine σ_k on data block $ct(d[k])$;
- E_3: The adversary $\mathcal{C}$ produces a forged signature on data block $ct(d[k])$ and $\mathcal{B}$ does not abort.

The probability of B succeed is

$$P[E_1 \cap E_2 \cap E_3] = P[E_1] \cdot P[E_2 \parallel E_1]P[E_3 \parallel E_1 \cap E_2]$$

From Garg and Bawas scheme in [9], we can calculate the probability of B succeed is $\epsilon^{'}$

$$\epsilon^{'} \geq (1/q_S + 1)e)\epsilon.$$

Since our scheme is based on the same difficult problem as Garg and Bawa's scheme, And the advantage of the attacker to break our scheme is the same as the attacker break the Garg and Bawa's scheme. So, our scheme is also secure in CDH problem. □

Theorem 2. *Our μR-MLE2 scheme is Path-PRV-CDA2 [1] secure.*

Proof. Given two sequences $v = (v_1, \cdots, v_n)$ and $v^{'} = (v_1^{'}, \cdots, v_n^{'})$, we consider the information that the adversary $\mathcal{C}$ can get through the two sequences. And if the tree path of two files is same, we recognize that they are the same one. We consider it in two cases.

One is when both of them have the same tree path, v is in the deduplication list, $v^{'}$ is also in the deduplication list. Then, the adversary $\mathcal{C}$ can not get any information from the two sequences.

The other is that v and $v^{'}$ have the same order relation. v is in the deduplication list, $v^{'}$ is not in the deduplication list. The user gives the path bit to the server. In both cases, the information obtained by the adversary is same, and the number of bits leaked does not exceed the height of the tree. So it is Path-PRV-CDA2 [1] secure. □

Table 2: Number of challenged blocks up to 90% of corrupted blocks

Number of corrupted blocks(x)	Number of challenged blocks(t)
6250	23
12500	12
18750	10
25000	7
31250	5
37500	4
43750	4
50000	3
56250	2

Theorem 3. *Assuming the hash function is collision-resistant, when clients and CSP follow the Modified Merkle tree-based protocol, a dishonest CSP cannot pass through the verification.*

Proof. Suppose that the user needs to verify the ith file block, the malicious CSP transfers part of the user's data and has two ways to cheat the user. One way is to return a forged message. The server may try to find an $ct_{d_j} \neq ct_{d_i}$ satisfying that $H(ct_{d_j}) = H(ct_{d_i})$. However, under the collision-resistant assumption, CSP cannot generate invalid data and the corresponding integrity path that the client can use to compute the correct metadata $H(R)$. The other way is that CSP may ignore the verification without giving the correct $P_f = \{\mu, \phi, (H(ct_{d_i}), AI(i)_{i\in Q}, \rho, SIB\}$, but to return another valid pair of data $P_{f^*} = \{\mu^*, \phi, (H(ct_{d_j}), AI(j)_{j\in Q}, \rho^*, SIB^*\}$ to the user.

In the phase of VerifyProof, TPA found that

$$e(\prod_{j=r_1}^{r_k} H(ct_{d[j]})^{b_j} \cdot u^{\mu^*}, g^k) \neq e(\phi, g)$$

In other words, any malpractice by CSP will be detected by a fully trusted TPA at the VerifyProof stage. Therefore, based on the Equation (2), CSP cannot use another data path pair to pass through the verification successfully. □

8 Performance Analysis

In this section, we will conduct our performance analysis including three aspects, the probability of malpractice at CSP, the computation cost, and communication overhead.

8.1 Probability of Detecting Malpractice at CSP

The solution [9] is to take the sampling method, that is, it divides the file F into n chunks and then randomly extracts t from n data blocks to detect the probability of detecting malpractice at CSP. Suppose that CSP changes x data block in n data blocks, then the probability of randomly sample a corrupted block is $\frac{x}{n}$. If the probability of detecting malpractice at least one block in challenge phase is P, then

$$\begin{aligned} P &= 1 - (1 - \frac{x}{n})(1 - \frac{x}{n-1}) \cdots (1 - \frac{x}{n-t+1}) \\ &= 1 - \prod_{i=0}^{t-1}(1 - \frac{x}{n-i}) \end{aligned} \tag{3}$$

In order to know more clearly the relationship among P, x, t, n, we simplify the Equation (3) and finally get

$$1 - (1 - \frac{x}{n - \frac{t-1}{2}})^t \leq P \leq (1 - \frac{x}{n-t+1})^t$$

Suppose the data owner divides the $1GB$ file into $62,500$ blocks, each one of which is $16kb$. We will show the number of blocks(t) required in challenge message to detect the number of blocks corrupted by considering the probability of malpractice detection ($P = 0.9$) in Table 2. Also with the number of corrupted data blocks increasing, the data blocks in the challenge decreasing. When CSP modifies 10% of total outsourced blocks(n), then CSP needs only 23 random blocks in the challenge set to detect a server malpractice with 0.9 probability.

8.2 Computation Cost

As is shown in Table 3. $Hash$ is represented as a hash function, which can map a message from any long bit string to a fixed length. Mul represents a multiplication on group G. Exp is expressed as a exponentiation operation. $Pair$ is represented as a pairing operation. m represents the total number of files in the cloud, each file is divided into n blocks. t is the number of challenged blocks.

In Table 3, Jiang *et al.* [13] and Abadi *et al.* [1] used deduplication to reduce the redundant data in the cloud. Although the computational cost of Jiang *et al.* [13] is $2Exp + Mul + Hash + 2(Hash + Exp) \cdot O(\log m)$, which is a litter higher than Abadi *et al.* [1], the time of deduplication reduced greatly from linear $O(m)$ to logarithmic $O(\log m)$. Wang *et al.* [23] and Garg *et al.* [9]

Table 3: Computation cost of deduplication and auditing

Schemes	Deduplication			Auditing		
	$User$	CSP	$Time$	CSP	TPA	$Time$
[1]	$2Exp + Mul$ $+Hash$	$2Pair \cdot O(m)$	$O(m)$	–	–	–
[9]	–	–	–	$tExp$ $+(t-1)Mul$	$2Pair + tExp$ $+tMul$	$O(\log(n))$
[13]	$2Exp + Mul + Hash$ $+2(Hash + Exp) \cdot O(\log m)$	$\emptyset$	$O(\log m)$	–	–	–
[15]	$Hash \cdot O(m)$	$\emptyset$	$O(m)$	$tExp$ $+(t-1)Mul$	$2Pair + tExp$ $+tMul + tHash$	$O(n)$
[23]	–	–	–	$tExp$ $+(t-1)Mul$	$2Pair + (t+2)Exp$ $+(t+1)Mul$	$O(n)$
Ours	$2Exp + Mul + Hash$ $+2(Hash + Exp) \cdot O(\log m)$	$\emptyset$	$O(\log m)$	$tExp$ $+(t-1)Mul$	$2Pair + tExp$ $+tMul$	$O(\log(n))$

Table 4: Communication cost of deduplication and auditing

Phases	Communication cost
Data deduplication	$User \leftrightarrow CSP : l + k$
Delegation of audit task	$User \rightarrow TPA : 2\|G\|$
Challenge phase	$TPA \rightarrow CSP : t\|Z_p\| + 283$
Responding proof	$CSP \rightarrow TPA : \|G\| + \|Z_p\| + (t+2) \times 256$

can detect the integrity of data in the cloud. Although Li *et al.* [15] can achieve both deduplication and audit, it makes the computation cost of auditor's become $2Pair + tExp + tMul + tHash$, which is much higher than Garg *et al.* [9]. And when the file is encrypted, a fully trusted key server is needed. Therefore, we implement both by adopting the method of Jiang *et al.* [13] and Garg *et al.* [9], which can not only reduce the time complexity from linear to logarithmic by using a decision tree, but also make the time of searching node vary from linear to sub-linear by using the Merkle Hash Tree with a relative index.

8.3 Communication Cost

As is showed in Table 4, $|Z_p|$ and $|G|$ are expressed as the size of element in Z_p and G, respectively. t is the number of blocks challenged. l represents as the size of file tag. k represents as the size of decision bit.

Communication costs are mainly divided into four phases. The first phase is to perform the data deduplication test between the user and CSP which includes that CSP sends the tag to user and user returns the decision bits to CSP. The second phase is to authorize the integrity of data to the third parties, therefore the communication costs equals the size of keys, root signature and which is one time for every audit. The third phase is that TPA sends the challenge message to the CSP, which needs to extract t element subset Q randomly and select random element $\{b_i\}_{i \in Q} \in Z_p$ to the CSP, and the fourth phase is the CSP response to the challenge phase. We can obtain that Q can be represented as 283 bits in [9], when the size of file $\leq 1024TB$ and $2 \leq err \leq 80$(err is error a probability).

9 Conclusions

In this paper, we have presented a novel approach to realize a secure and efficient data deduplication scheme supporting dynamic data public auditing. The proposed scheme can not only save the storage cost in the cloud, but also use the auditor to verify the integrity of data in the cloud. It is significant to reduce the time to detect the redundant data and the calculation cost of searching the block of file. In addition, our scheme also supports the dynamic data operations, such as data insertion, data deletion, data modification and data append.

Acknowledgments

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by the National Key R&D Program of China under Grant No.2017YFB0802000, the National Natural Science Foundation of China under Grants No.61472470 and 61572390, and the Scientific Research Plan Project of Education Department of Shaanxi Province under Grant No.17JK0362.

References

[1] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, "Message-locked encryption for lock-dependent messages," in *Advances in Cryptology (CRYPTO'13)*, pp. 374–391, 2013.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 12, 2011.

[3] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in *IACR International Workshop on Public Key Cryptography*, pp. 516–538, 2015.

[4] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," *IACR Cryptology ePrint Archive*, vol. 2013, pp. 429, 2013.

[5] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 296–312, 2013.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual International Cryptology Conference*, pp. 213–229, 2001.

[7] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 514–532, 2001.

[8] Z. J. Cao, L. H. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifiable outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.

[9] N. Garg and S. Bawa, "Rits-mht: Relative indexed and time stamped merkle hash tree based data auditing protocol for cloud computing," *Journal of Network and Computer Applications*, vol. 84, pp. 1–13, 2017.

[10] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[11] M. S. Hwang, C. C. Lee, and T. H. Sun, "Data error locations reported by public auditing in cloud storage service," *Automated Software Engineering*, vol. 21, no. 3, pp. 373–390, 2014.

[12] M. S. Hwang, T. H. Sun, and C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits, Systems and Computers*, vol. 26, no. 05, pp. 1750072, 2017.

[13] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, "Secure and efficient cloud data deduplication with randomized tag," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 532–543, 2017.

[14] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

[15] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2386–2396, 2016.

[16] H. Lima, R. Araujo, R. Viegas, and D. Rosario, "A secure collaborative network protocol," in *Proceedings of the 9th Latin America Networking Conference*, pp. 46–52, 2016.

[17] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *International Journal of Network Security*, vol. 19, no. 2, pp. 177–181, 2017.

[18] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[19] H. Shacham and B. Waters, "Compact proofs of retrievability," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 90–107, 2008.

[20] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data deduplication scheme for cloud storage," in *International Conference on Financial Cryptography and Data Security*, pp. 99–118, 2014.

[21] E. Stefanov, M. V. Dijk, A. Juels, and A. Oprea, "Iris: A scalable cloud file system with efficient integrity checks," in *Proceedings of the 28th Annual Computer Security Applications Conference*, pp. 229–238, 2012.

[22] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[23] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[24] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

[25] J. Xu and E. C. Chang, "Towards efficient proofs of retrievability," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 79–80, 2012.

[26] Z. Yan, M. Wang, Y. Li, and A. V. Vasilakos, "Encrypted data management with deduplication in cloud computing," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 28–35, 2016.

[27] M. Yang and Y. M. Wang, "On the security of three public auditing schemes in cloud computing," *Inter-*

national Journal of Network Security, vol. 17, no. 6, pp. 795–802, 2015.

[28] J. H. Zhang, P. Y. Li, and M. Xu, "On the security of an mutual verifiable provable data auditing in public cloud storage," *International Journal of Network Security*, vol. 19, no. 4, pp. 605–612, 2017.

Biography

Hua Ma received her B.S. and M.S. degrees in Mathematics from Xidian University, China, in 1985 and 1990, respectively. She is a professor of Mathematics and statistics, Her research includes security theory and technology in electronic commerce design and analysis of fast public key cryptography theory and technology of network security.

Xiaoyu Han received her B.S. degree in 2015 from College of Mathematics and Applied Mathematics, Lvliang University. Now, she is a master degree student in Mathematics at Xidian University. Her research focuses on network and information security.

Ting Peng received her B.S.degree in 2014 from College of Mathematics and Information Sciences, Xianyang Normal University. Now, she has graduated from Xidian University. Her research focuses on cryptography and network security.

Linchao Zhang received his B.S. degree in 2015 from College of Mathematics and Applied Mathematics, Hunan Institute of Science and Technology. Now, he is a master degree student in Mathematics at Xidian University. His research focuses on Proxy re-encryption and data security.

Probabilistic Framework for Assessing the Threat Level using Novel Decision Constructs in Mobile Adhoc Network

V. Sangeetha[1] and S. Swapna Kumar[2]

(Corresponding author: V. Sangeetha)

Department of Computer Science and Engineering, Kammavari Sangha Institute of Technology[1]
14, Kanakapura Main Road, Municipal Corporation Layout, Raghuvanahalli, Bengaluru, Karnataka 560062, India
(Email: sangeethares13@gmail.com)
Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology[2]
P.O. Thalakottukara, Kaipparambu, Thrissur, Kerala 680501, India

(Received June 19, 2017; revised and accepted Nov. 5, 2017)

Abstract

The existing secure routing protocol in Mobile Adhoc Network (MANET) lacks the capability of identifying the dubious communication behavior of a mobile node, which is essential in order to construct policy to resist them. This could happen when the malicious nodes choose to act like a regular node in order to bypass security. After reviewing the existing research approach, we found that existing studies are carried out in highly controlled research environment which is no more applicable if the environment changes. Therefore, we introduce a framework which is capable of assessing the level of legitimacy of the node in a network before confirming the route establishment with it. The study uses a novel decision making constructs for implementing its strategy of communication and it also incorporates strategic construction of assessing the security threat. The study outcome of proposed system is found to excel better communication performance when compared with existing security routing protocols in MANET.

Keywords: Intrusion Detection; Intrusion Prevention; Malicious; Mobile Adhoc Network

1 Introduction

Mobile Adhoc Network is one of the best way to provide seamless communication platform without any kind of fixed infrastructure. Hence, this communication feature allows it to perform adhoc based communication [9, 22]. Significant advantage of MANET system includes

1) Infrastructure independent;
2) Multi-hop routing;
3) Autonomous terminal;
4) Dynamic topology;
5) Fault tolerance;
6) Cost effective [1, 7].

It has its wide range of applicability in tactical network, emergency services, education applications, location-based services [12, 19, 20]. However, an interesting fact to observe that although MANET is being studied and investigated from more than two decades, but still date there are few application that is commercially available or known to the common people.

The communication in MANET is supported by three different routing protocols *i.e.* proactive, reactive, and hybrid [18]. At present, there are more than thousand numbers of research work on routing protocols till date, but majority of them suffers from one or other issues. For an example, proactive protocols suffers from slow convergence rate, tendency for loop creation, higher dependencies on resources, unexploited routing information *etc.* Reactive protocols suffers from out-date routing information, maximized delay, overhead cost, *etc.* Finally, hybrid protocol suffers from usage of random schemes (proactive) over the simulation area, latencies involved in inter-zones routing, routing over zones are highly resource dependent. Hence, it will be unwise to highlight any specific routing protocol in MANET to be highly efficient one. Although, these routing protocols are sufficient to form communication among mobile nodes but they are not enough powered to resist different forms of attacks *e.g.* active attack and passive attack in MANET. Some of the attacks in MANET are modification, Denial-of-Service, Spoofing, Impersonating, Masquerade, wormhole attack, Sybil attack, black-hole attack, rushing attack, replay attack, *etc.*

Some of the standard routing protocols in MANET are

1) Secured Efficient Distance vector (SEAD);
2) Secured Destination Sequence Distance Vector

(SDSDV);

3) Secure Line State routing protocol (SLSP);
4) Server Routing Protocol (SRP);
5) Byzantine Failure Resilient Protocol;
6) Authenticated Routing for Adhoc Networks (ARAN);
7) Secured Position-Aided Adhoc Routing (SPAAR);
8) Security Aware Routing (SAR), *etc.* [24, 28, 31].

However, all the existing secure routing protocols suffer from problems that really don't assist in proper identification [11].

At present there are also various techniques based on trust and reputation [27] meant for checking the security validity of the next node. Unfortunately, all these techniques have not offered any evidence that their outcome in the form of identification process is reliable or not. Hence, existing process doesn't offer any form of standardized validity that the outcome generated by security protocol should be believed as universal standard. This is a serious problem as it doesn't lead us to find the distinct difference between different types of mobile nodes in MANET. Therefore, if there is any malicious node pretending to be normal node existing within simulation that it may lead to collateral damage. Therefore, the proposed system offers a framework that applies the potential of decision making approach for strategy building in order to investigate the pattern of malicious communication behavior of mobile nodes.

The outcome of the study is meant to be used for both intrusion detection system as well as intrusion prevention system. The study uses multiple parameters of probability to find the level of authenticity of the mobile nodes present within the network. The proposed study is essentially meant for adopting a communication strategy based on the environmental condition. Section 1.1 discusses about the existing literatures where different techniques are discussed for secure routing protocols in MANET followed by discussion of research problems in Section 1.2 and proposed solution in Section 1.3. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

2 Background

This section presents the brief highlights of the existing research-based approaches towards securing the communication in MANET. Cao *et al.* [3] have presented a framework that evaluates the capacity of the secrecy along with the delay factor in MANET using empirical-based approach. Anand *et al.* [2] introduced a scheme that investigates the misbehavior of the node using dynamic approach of partially retaining the malicious information. Matam and Tripathy [17] have presented a multi-cast routing using digital signature in order to resist wormhole attack. Although this work is targeted for mesh network but it is equally applicable for MANET. Surendran and Prakash [26] have used bio-inspired algorithm for retaining maximum resiliency of routing process in MANET. Zhang *et al.* [33] have presented a technique that can offer mitigation from jamming-based intrusion in MANET.

Study towards investigating traffic behavior was carried out by Qin *et al.* [21] using statistical approach. Liu and Yu [14] have introduced a routing technique that offers both robust authentication as well as anonymity in MANET using digital signature. Sekaran and Parasuraman [23] have used conventional cryptographic approach in order to secure the routing protocol. Usage of network code for supporting a cryptographic scheme is seen in the work of Zhang *et al.* [18] for enhancing the confidentiality. Shakshuki *et al.* [10] have presented a unique mechanism of intrusion detection system on the basis of the acknowledge in the control message.

Liu *et al.* [15] have enhanced the reliability by presenting a clustering scheme for assisting in revocation of certificate in MANET. Lv and Li [16] have implemented a mechanism for securing group-based communication system in MANET. Study towards trust effectiveness is emphasized by Zhao *et al.* [34] considering the patterns of cyclic movements using stochastic approach and Bellmam-Ford algorithm. Zhao *et al.* [35] have presented a mechanism for identifying the extent of risk involved in capturing the response message in MANET. Chen and Wu [4] have designed a secure protocol for safeguarding the anonymity process during routing using hash function.

El-Defrawy and Tsudik [6] have also focused on privacy preservation using group signature for resisting suspicious node to take part in routing process. Dhurandhar *et al.* [5] have implemented a scheme for incorporating robust security while routing among the networks of friendly nodes. Study towards optimal secrecy was carried out by Liang *et al.* [13] towards ensuring enhanced throughput in communication process. Xu *et al.* [29] have presented a technique that performs execution of trust from kernel level. Shen and Zhao [25] have also emphasized on incorporating a technique to maintain anonymity towards positional information during the routing process in MANET.

Hence, it can be seen that there are various techniques that has been evolved since last decade for securing the routing process in MANET. All the techniques play different level of roles to address security problems as well as all of them are implemented towards routing security itself. Each one of the protocol has its own advantages in form of security strength. The next section briefly discusses about the problems explored from the existing system.

3 Research Problem

The significant research problems are: Existing solutions are specific to the routing adversaries and its applicability on different environment is yet to be proven. Studies

towards identifying malicious behavior have not been assessed deeply in existing system that is not capable of differentiating the characteristics feature of nodes. Influence of increasing level of attack (be it any) towards communicational performance is not yet tested in existing system. Existing studies also doesn't assure the effectiveness / reliability of outcome of intrusion detection system in case of complex attack scenario.

Therefore, the problem statement of the proposed study can be stated as *"It is technically a difficult task to assess the level of legitimacy of the neighborhood node if the malicious node chooses to either act as normal node or self node in order to achieve their aim of intrusion".*

4 Proposed Solution

The prime purpose of the proposed work is to present a novel framework that uses the strategic approach for constructing decision thereby assisting the node to perform legitimacy evaluation for secured routing in MANET. The adopted scheme of proposed system where the significant contribution lies in behavioral modeling of a mobile node into malicious and normal node as shown (see Figure 1).

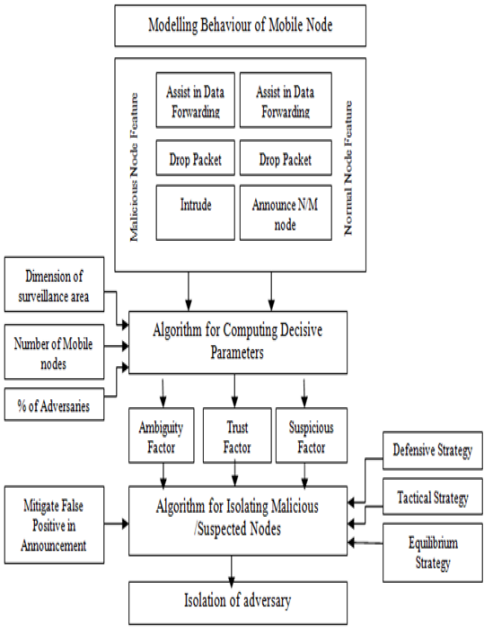


Figure 1: Adopted schema of proposed system

We formulate conditional feature stating that there are common and uncommon behavior for both the type of nodes. The common behavior is assisting the node in data forwarding and dropping packet. However, uncommon behavior is that actions of intrusion is only shown by adversary while announcing the node as malicious (M) or normal (N) is the feature of normal node.

The algorithm construction of proposed system takes the different form of inputs which after processing leads to evaluation of statistical information about ambiguity factor, trust factor, and suspicious factor using simple mathematical approach (discussed in the algorithm step in next section). The algorithm also considers using multiple form of strategies that either of the nodes could possibly consider for achieving their objectives. The possibility of false positive towards the announcement is also formulated in the proposed system. The notion is that for a given simulation scenario of unknown identities of node, the proposed system evaluates the communication behavior of the nodes and confirms a decision based on statistical evaluation. The decision is finally confirmed by filtering any form of false positive information in order to ensure proper isolation of malicious node from the further process of routing in MANET. The next section discusses about algorithm implementation of this concept.

5 Algorithm Implementation

The algorithm is mainly responsible for assessing the unpredictable behavior of the mobile nodes in MANET where it is assumed that confidentiality of any nodes is unknown. This assumption will mean that the proposed system does not have any kind of prior information about the legitimacy of the mobile nodes. The proposed system runs two different algorithms where one of them is responsible for computing the security attributes responsible for making decisions of legitimacy nodes and the other algorithm is responsible for isolating the malicious or suspected nodes to be participating in the routing process.

Algorithm for Computing Decisive Parameters

Input: s_a, n, a, b
Output: τ, T, S
Start
1. init s_a, n, a,b
2. [x . y]= s_a-(2*b).arb(n)
3. for i=1:n
4. τ = k .a_1.a_2
5. T=(1- τ).a.$(a+b)^{-1}$ and S=(1- τ).b.$(a+b)^{-1}$
6. end
End

The above mentioned algorithm is responsible for computing the decisive parameters for exploring the legitimacy of a node in MANET. The algorithm takes the input of s_a (dimension of surveillance area), n (number of mobile nodes), a (% of Adversaries), b (boundary of surveillance area) (Line-1), which after process yields the computed outcome of τ (Ambiguity factor), T (trust factor), S (Suspicious factor). A closer look into this formulation will show that the system just takes the input of proportion information of adversary node as input and it is never aware of any specific node to become adversary. The next part is to perform random distribution of the node according to Line-2, where the variable b represents boundary of node. For effective computation, the pro-

posed system uses probability theory for defining two different parameters a and b representing quantity of nodes assisting in data forwarding and occurrences of identified intrusion or packet drop respectively. It should be noted that process of packet drop is not only characteristic of malicious node but even a normal node can also drop the packet because of genuine technical reasons.

Hence, now the modeling imposes quite a challenging scenario to identify malicious or adversary node. In Line-4, the variable a_1 and a_1 will represents (a.b) and (a+b)2. (a+b+1) respectively that is used for computing ambiguity factor. The variable k represent network coefficient. Similarly, the empirical representation of computation of trust T and suspicious factor S is as shown in Line-5. This computation is an iterative process and is carried out by the transmitting node while choosing its neighborhood nodes by evaluating their legitimacy first. The next part of the algorithm will further assist the node to confirm its decision by taking necessary security measures.

Algorithm for Isolating Malicious/Suspected Nodes

Input: $\mu 1$, $\mu 2$, $\mu 3$
Output: isolation of adversary
Start
1. [n] = [$\mu 1$, $\mu 2$, $\mu 3$]
2. if $\lambda * (1\text{-}\tau) <$ Threshold
3. if $\lambda <$ h
4. return strategy $\rightarrow v_1$
5. else
6. return strategy $\rightarrow v_2$
7. end
8. end
9. Compute τ, T, S
10. $\Omega = s_i$ *((c- v_1)/φ)
11. Flag n (max(card(τ))) $\rightarrow$ adversary
End

The above algorithm confirms the level of threat for its monitored nodes and isolates them from participating in the routing process. The algorithm takes the input of three different strategies i.e. $\mu 1$ (Defensive Strategy), $\mu 2$ (Tactical Strategy), $\mu 3$ (Equilibrium Strategy), which after processing leads to isolation of adversaries (Line-1). By defensive strategy, it will mean that normal node will always assist in data forwarding while malicious node will always intrude. Hence, defensive strategy is the easier one that can be adopted by node straightly. Tactical strategy will mean that malicious node may even forward data packet without harming anyone and normal node may drop the packet without having any intention of disrupting the ongoing communication. Therefore, the tactical strategy is the most challenging one where there are chances of misidentification of legitimacy of either of the nodes. However, we believed that a malicious node will never continue to forward a data packet for a longer duration of time as it may significantly drain their resources which will lower the success rate of their execution of harmful intention. Hence, at certain point of time, it will definitely intrude.

In order to solve this problem, the proposed system introduces a probability parameter λ that represents the probability that the identified mobile node is possibly an adversary. A statistical threshold is used which is compared with the probability of confirming that a node is malicious ($\lambda * (1 - \tau)$) (Line-2). A new temporary parameter h is used for computing the gain obtained by a mobile node for forwarding a data packet (Line-4). It should be noted that if the malicious node is forwarding the data packet that it will not have gain as it is only meant for initiating attacks. Similarly, if the regular node forwards data then its gain will increase. Therefore, the condition stated in Line3-Line7 is that, if the threat probability parameter λ is found to be minimal to h than it is only the possibility that a data forwarding event v_1 is taking place (Line-4) otherwise it will mean that data packet is dropped (Line-6). Although, this condition gives information about the state of data packet forwarding or dropping, but it doesnt give much clarity that if this information obtained from the node is normal node or malicious node. Hence, the decision cannot be confirmed although the nature of communication being regular or threatful is confirmed.

The solution to this problem is consideration of the third strategy called as $\mu 3$ (Equilibrium Strategy) that is also one of the possible characteristics of any node (Line-1). According to this characteristics, it will mean that a malicious node will obtain maximum gain if it achieves its intention of intrusion/attack as faster as possible without much resource consumption. Similarly, equilibrium strategy also states that a normal node has all the right to compute the legitimacy of its neighbor node and can declare them to be normal or malicious nodes depending upon the level of threats in communication as seen till Line-6.

Hence, we formulate a condition that if the normal node flags incorrect information about its neighborhood node than its gain value will reduce. Interestingly, we don't model any such characteristics of computing legitimacy for the adversary. It is because we believed that performing such computation is completely unnecessary for the adversary node as it will only result in draining its own resources, which should be used only for invoking attacks. After this, the algorithm recomputes the value of trust factor T, suspicious factor S, and ambiguity factor τ (Line-9). We define a parameter τ which is representation of false positive information about the neighborhood node computed by a normal node (Line-10). The variable s represents selected strategy of action by the node (Line-10) whereas the variable c represents computation of the probability of the threat level to higher intensity. The variable Ω represents probability of identifying a mobile node to be malicious, which will mean that higher value of Ω will provoke the normal mobile node to confirm that the identified mobile node is malicious node. At the same

time, the malicious node will ensure that it doesn't take such step so that value of Ω for itself comes to be higher as per the principle of equilibrium strategy.

Therefore, according to the equilibrium strategy, a regular node will be be continuing more number of packet dropping event as in that case its gain obtained will be exponentially reduced which will affect its i) trust value and ii) its resources too. At the same time, a malicious node will only keep on forwarding data as long as their gain of invoking an attack is more than the resource expenditure inorder to carry out an attack. Hence, it is eventual that an attacker node will not continue to be in the mode of forwarding the data packet as in that way it will minimize its gain, which is only meant for attack purpose. Therefore, an indication of the attack scenario is that consistent frequencies of packet dropping by a same node is a direct indication of the malicious node (Line-11).

Even if such characteristics is carried out by a normal node than we assume that involvement of such node is highly detrimental for routing performance and therefore, we choose to remove the identity of the compromised / malicious node from the routing table. Also, we find that there is a strong relationship between the ambiguity factor and Ω whereas we find that if the first one increases than the later one also increases. Hence, the cardinality of the ambiguity factor is consistently assessed. Our observation says that a normal node will never exhibit more occurrences of relayed information more close to ambiguity factor, which is the definite identification of the malicious node. Therefore, the proposed system can successfully offer better behavioral analysis of the mobile nodes and performs secure routing only after ascertaining that its link with neighborhood nodes are stable and not yet compromised. The algorithm incorporates more decision making capabilities to the mobile node by using three different strategies to select from. The next section discusses about the result being accomplished after implementing the proposed algorithm.

6 Result Analysis

The implementation of the algorithm discussed in prior section has been designed by MATLAB considering simulation area of $1200 * 1500m^2$. The analysis was carried out considering 100 mobile nodes where 10% of the nodes are considered to be an adversary. The proportion of adversaries can be varied to understand the impact. The implementation is also analyzed considering all the three different forms of strategies (defensive, tactical, and equilibrium). For better assessment of the study outcome, we consider comparative performance analysis with the most standard secured protocol in MANET i.e. Secured AODV [30] and ARIADNE [8].

As shown (see Figure 2) the proposed system offers better throughput performance as compared to that of existing system of SAODV and ARIADNE. The prime reasons behind this are many. One of the advantages of

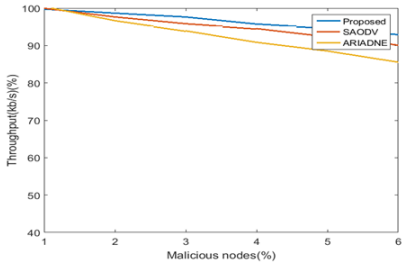


Figure 2: Comparative analysis of throughput

SAODV is its capability to detect and prevent misbehavior of node and it does so by using digital signature. Usage of digital signature offers significant resistance to the entry towards falsifying the legitimacy of the identity of the requester node. Although, SAODV schemes offers higher degree of resiliency towards authentication but it doesn't have capability to identify the selfish node like our system does. Therefore, if a regular node is found to drop packet for any good reason, SAODV still considers that node as malicious node. This causes the complete communication process to slow down causing lowering of the throughput with an increased level of authentication being demanded for with an increase in malicious node.

On the other hand, ARIADNE protocol is believed to offer resiliency against denial-of-service attacks in adhoc network, where the lightweights of the secured routing is confirmed by the usage of symmetric encryption. Usage of secret shares makes this protocol highly resistive towards authentication failures using digital signatures. ARIADNE also uses MAC protocol to perform robust authentication among each other. A closer look into both SAODV and ARIADNE protocol shows that it offers maximum resiliency when there is an attacker present in the network. However, none of these protocols are found capable of identifying any selfish node or compromised node, which is the main pitfall of existing system. Therefore, when SAODV and ARIADNE is allowed to be executed in our environment where the adversaries acts as a normal node and assists in forwarding data packet, both the protocol has failed to identify it.

Moreover, the existing protocol also found to be failing in understanding the motive that malicious node assist in data packet forwarding only because they want to increase trust level which lowers down the resource expenditure to greater degree. This causes the malicious node to meet an appropriate situation where it is not possible for any of the existing system to identify the degree of threat for the existing system. From the perspective of throughput as shown (see Figure 2), routing overhead as shown (see Figure 3), and routing latency as shown (see Figure 4), the trend is nearly similar. ARIADNE offers significant routing overhead along with increased delay because of its combined usage of MAC authentication with digital signature. Hence, existing on-demand routing schemes may offer good security against certain types of attacks but

doesn't excel optimal performance when it comes to communication performance in MANET where the identity of the attacker is not immediately disclosed.

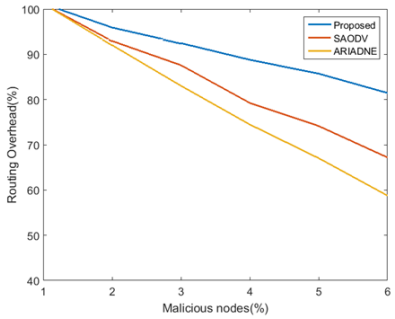


Figure 3: Comparative analysis of routing overhead

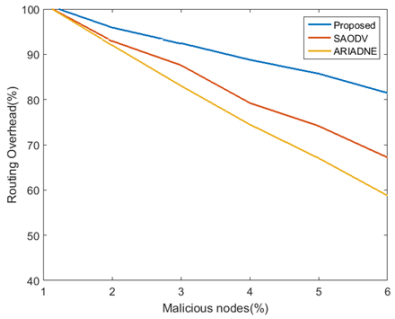


Figure 4: Comparative analysis of routing latency

Apart from this, we also find that proposed system takes approximately 0.31176 seconds in order to identify the malicious node while the existing system are found to consume 0.9762 seconds and 2.7669 seconds for SAODV and ARIADNE routing protocol tested on core i3 machine on windows platform. Moreover, the proposed system doesn't store any information during the run-time of the algorithm, all the information regarding the ambiguity factor, trust factor, suspicious factor are computed on run time. The advantage of this mechanism is that the system forcibly introduces lots of updated information about the legitimacy which assists the normal node to take a final decision with high true positive about the identity of the intruder by observing the communication behavior of them. The proposed system doesn't act directly as intrusion prevention system but rather it offers more insights on the typical behavior of a mobile node whose identity is suspected to be malicious. The framework is free from any form of encryption and therefore it is highly light weighted compared to any form of security protocol in existing system. The applicability of proposed framework is more on intrusion detection and prevention system for any form of malicious activity in MANET.

7 Conclusion

A robust and full proof security incorporation is one of the open-end challenging problems in MANET system primarily due to its effect of decentralization. The existing studies towards secure communication only offers resiliency from particular form of attack. This will mean that if the adversary launches two different form of attacks at same time than it is nearly impossible for the normal node even to identify the threat level and definitely will not possess enough time even to take a decision for adopting a precise mitigation. It may also be the case that mitigation policy doesn't even exists in the node being about to be victimized. Therefore, the proposed study presents such a technique that could compute the level of threat and takes necessary action in order to resist it. The outcome of the study was assessed to find that proposed system offers better throughput and minimal overhead and latency as compared to existing secured routing system in MANET.

References

[1] A. Abdullah, Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study" *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116-123, 2017.

[2] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 18, no. 6, pp. 938-947, 2016.

[3] X. Cao, J. Zhang, L. Fu, W. Wu and X. Wang, "Optimal secrecy capacity-delay tradeoff in large-scale mobile Ad Hoc networks," in *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, PP. 1139-1152, 2016.

[4] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 3, pp. 519-527, June 2011.

[5] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, "FACES: Friend-based Ad Hoc routing using challenges to establish security in MANETs systems," *IEEE Systems Journal*, vol. 5, no. 2, pp. 176-188, 2011.

[6] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," *IEEE Transactions on Mobile Computing*, vol. 10, no. 9, pp. 1345-1358, 2011.

[7] B. S. Gouda, D. Patro and R. K. Shial, "Scenario-based performance evaluation of proactive, Reactive and hybrid routing protocols in MANET using random waypoint model," in *International Conference on Information Technology (ICoIT'14)*, pp. 47-52, 2014.

[8] Y. Hu, A. Perrig and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", *Wireless networks*, vol. 11, no. 2, pp. 21-38, 2005.

[9] A. Jamalipour, S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto, "Detecting blackhole attack on AODV-based mobile Ad Hoc networks by dynamic learning method," *International Journal of Network Security*, vol. 5, no. 3, pp. 338-346, 2007.

[10] P. Joshi, P. Nande, A. Pawar, P. Shinde and R. Umbare, "EAACK - A secure intrusion detection and prevention system for MANETs," in *International Conference on Pervasive Computing (ICPC'16)*, pp. 1-6, 2016.

[11] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[12] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[13] Y. Liang, H. V. Poor and L. Ying, "Secrecy throughput of MANETs under passive and active attacks," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6692-6702, 2011.

[14] W. Liu and M. Yu, "AASR: Authenticated anonymous secure routing for MANETs in adversarial environments," in *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585-4593, 2014.

[15] W. Liu, H. Nishiyama, N. Ansari, J. Yang and N. Kato, "Cluster-based certificate revocation with vindication capability for mobile Ad Hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 2, pp. 239-249, 2013.

[16] X. Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," *IET Information Security Technology*, vol. 7, no. 2, pp. 61-66, 2013.

[17] R. Matam and S. Tripathy, "Secure multicast routing algorithm for wireless mesh networks," *Journal of Computer Networks and Communications*, pp. 11-17, 2016.

[18] H. Moudni, M. Er-Rouidi, H. Mouncif and B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks," in *International Conference on Information Technology for Organizations Development (ITOD'16)*, pp. 1-7, 2016.

[19] A. Negi, K. Ammayappan, V. N. Sastry, "A new secure route discovery protocol for MANETs to prevent hidden channel attacks," *International Journal of Network Security*, vol. 14, no. 3, pp. 121-141, 2012.

[20] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile Ad-hoc wireless networks," *International Journal of Network Security*, vol. 3, no. 2, pp. 191-202, 2006.

[21] Y. Qin, D. Huang and B. Li, "STARS: A statistical traffic pattern discovery system for MANETs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 2, pp. 181-192, 2014.

[22] A. Rana, D. Sharma, "Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 1-8, 2018.

[23] R. Sekaran and G.K. Parasuraman, "A secure 3-way routing protocols for intermittently connected mobile Ad Hoc networks," *The Scientific World Journal*, vol. 2014, pp. 13, 2014.

[24] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," in *International Conference on Computing, Communication and Automation (ICCCA'16)*, pp. 637-640, 2016.

[25] H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1079-1093, 2013.

[26] S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault - tolerant routing in MANETs," in *China Communications*, vol. 12, no. 8, pp. 93-110, 2015.

[27] Z. Ullah, M. H. Islam and A. A. Khan, "Issues with trust management and trust based secure routing in MANET," in *13th International Bhurban Conference on Applied Sciences and Technology (IBCAST'16)*, pp. 402-408, 2016.

[28] M. K. Verma, S. Joshi and N. V. Doohan, "A survey on: An analysis of secure routing of volatile nodes in MANET," in *CSI Sixth International Conference on Software Engineering (CONSEG'12)*, pp. 1-3, 2012.

[29] G. Xu, C. Borcea and L. Iftode, "A policy enforcing mechanism for trusted Ad Hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp.321-336, 2011.

[30] M. G. Zapata, "Secure Ad Hoc on-demand distance vector routing", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106-107, 2002.

[31] L. Zhang, X. Song, Y. Wu, *Theory, Methodology, Tools and Applications for Modeling and Simulation of Complex Systems*, Springer, 2016.

[32] P. Zhang, C. Lin, Y. Jiang, Y. Fan and X. Shen, "A lightweight encryption scheme for network-coded mobile Ad Hoc networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2211-2221, 2014.

[33] R. Zhang, J. Sun, Y. Zhang and X. Huang, "Jamming-resilient secure neighbor discovery in mobile Ad Hoc networks," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5588-5601, 2015.

[34] H. Zhao, X. Yang and X. Li, "cTrust: Trust management in cyclic mobile Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2792-2806, 2013.

[35] Z. Zhao, H. Hu, G. J. Ahn and R. Wu, "Risk-aware mitigation for MANET routing attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 250-260, 2012.

Biography

V. Sangeetha is working as Associate Professor at Department of Computer Science and Engineering, K.S.Institute of Technology, Bengaluru, Karnataka, India. She received the B.E degree in Computer Science and Engineering from Acharya Institute of Technology, from Visvesvaraya Technological University (VTU), Bengaluru, Karnataka, India in 2004, and M.Tech in Computer Science and Engineering from R.V.College of Engineering, VTU, Bengaluru, Karnataka, India in 2011. Currently pursuing Ph.D in Computer Science & Engineering from VTU, Karnataka, India. Her current research interests include Network security, Wireless network, Embedded System. She has also a life membership of several professional bodies including Indian Society for Technical Education (ISTE); Institution of Engineers (IEI) and International Association of Engineers (IAENG).

S. Swapna Kumar, Ph.D., is Professor and Head, of Department of Electronics and Communication Engineering, in Vidya Academy of Science and Technology, Thrissur, Kerala, India. Presently, he is a Supervisor for the Ph.D. scholars under Visvesvaraya Technological University (VTU) and also an external examiner for Thesis evaluation/ Public Viva-voce of Ph.D. students. He has been in the teaching for profession courses under UG/PG level for nearly decade, and has worked for various national and international industries. He is a reviewer of several National and International journals. Besides, he has also authored a books on "A Guide to Wireless Sensor Networks" and "MATLAB easy way of learning". Dr. Swapna Kumar is a Fellow Member and Chartered Engineer of the Institution of Engineers (INDIA). He has also a life membership of several professional bodies, including Indian Society for Technical Education (ISTE) and IEEE. His area of interest include Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, LaTeX, MATLAB modeling and simulation.

A Review on DNA Based Cryptographic Techniques

Animesh Hazra[1], Soumya Ghosh[2], and Sampad Jash[2]
(Corresponding author: Animesh Hazra)
Department of Computer Science and Engineering, Jalpaiguri Government Engineering College[1]
Jalpaiguri, West Bengal 735102, India
(Email: hazraanimesh53@gmail.com)
Department of Information Technology, Jalpaiguri Government Engineering College[2]
(Received May 12, 2017; revised and accepted Oct. 28, 2017)

Abstract

Today, data security has become a great concern. The increase in digitalization and e-commerce has encouraged more and more people to use the Internet. As a result, the web has become a part of our life. Hence the need of data security is evident. In order to enhance the data security, researchers have come up with new concepts. The use of DNA cryptography along with various encryption techniques is one of the major trends used in modern data security. Experimental results show that several biological operations and encoding techniques can be applied on DNA. This paper gives a brief review of the methods used in DNA cryptography and real time implementation of those techniques. Computational advantages along with the limitations regarding DNA cryptography is also addressed.

Keywords: Data Security; Decryption; DNA Cryptography; E-Commerce

1 Introduction

Cryptography [38] can be defined as the art of achieving security with the help of encoding messages in order to make them non-readable. The technique of decoding the non-readable messages into readable one is known as cryptanalysis and it can be said that cryptology is defined as the combination of cryptography and cryptanalysis. Before the age of computers, the art of cryptography was performed my manual techniques. Some of the techniques involved are substitution technique and transposition technique. Caesar cipher, modified version of Caesar cipher, mono alphabetic cipher, polygram substitution cipher, Vigenere cipher are different examples of substitution technique. Some transposition techniques include rail-fence technique, simple columnar transposition technique, vermin cipher *etc.* The introduction of computer made it possible to use more complex cryptographic algorithms. Technical terms like encryption and decryption came into existence. Encryption is defined as the process involved in the encoding of plain text to cipher text and decryption is the reverse process of encryption [13].

There are two aspects in respect to this encryption and decryption process. One is the algorithm that is involved in the encryption process and another one is the key used in the algorithm. Key is the most important attribute on which the security of the encryption technique depends. It can be classified into two categories. If the same key is used for both encryption and decryption procedure then the key is known as symmetric key whereas in asymmetric key different keys are used for both encryption and decryption algorithm. There are various methods to implement these techniques like data encryption standard (DES), International data encryption algorithm (IDEA) [29, 31], RC4, RC5, blowfish, advanced encryption standard (AES) [30, 45], RSA [14, 33], ElGamal [18, 19, 42, 43], and ECC cryptography [36, 54] *etc.*

There are some challenges involved in traditional cryptography. One such problem is the sharing of key because it may fall prey to attacks like eavesdropping or man in the middle. It has been found out that the ultimate power of a cipher depends on three important factors *i.e.* the size of the key, the infrastructure on which the key is running and last one is the algorithm on which it is designed. Today the most secure key length is 2028 bits. A famous symmetric key algorithm known as DES which uses a 5-bit key size is no more considered as safe. The increase in computational power has compromised the safety of the traditional cryptographic techniques. This problem is solved with the use of DNA cryptography.

1.1 Operations on DNA

Many biological operations [5, 6, 46] can be done on DNA molecules which will aid us in solving mathematical and computational problems. Some of the arithmetic and logical operations performed on DNA are as follows.

The basic arithmetic operations which can be imposed on DNA nucleotides are addition and subtraction. They are described in the following section.

1) Addition Operation: The addition operation on DNA nucleotides are performed according to the traditional binary addition rules. For example, if two binary numbers 10 and 11 are added then it will result the value 01. Now, suppose the four DNA nucleotide bases A, T, C and G are encoded as 00, 01, 10 and 11 respectively. Then it can be concluded that when C is added with G, it results into T.

2) Subtraction Operation: The subtraction operation on DNA sequences are performed according to the traditional binary subtraction rules. For example, if 01 is subtracted from 11 then the result is 10. Now, suppose the four DNA nucleotide bases A, T, C and G are encoded as 00, 01, 10 and 11 respectively. Then it can be concluded that when T is subtracted from G, it results into C.

The logical operations which can be implemented on DNA sequences are NOT, OR, AND, XOR, NOR, NAND and XNOR. They are described below in details.

Deoxyribonucleic acid (DNA) has a number of characteristics that enables us to mimic the traditional logical operations. DNA prefers to be in double stranded form, so single stranded DNA sequences naturally migrate towards complementary sequences to form double stranded complexes. Complementary sequences pair the bases adenine (A) with thymine (T) and cytosine (C) with guanine (G). DNA sequences pair in an anti-parallel manner.

In each DNA-based logic operation, the input is represented by a single stranded DNA sequence with the requirement that the sequence representing a true evaluation is complementary to the sequence representing a false evaluation for a single gate. For example, ACCTAG can be represented as true whereas CTAGGT is represented as false, since CTAGGT is the reverse complement of ACCTAG. This enables sequence assignment to be dynamic in nature. A user could arbitrarily assign a new set of representative sequences for each gate in a circuit.

DNA's preference to be in double stranded form enables the implementation of traditional logic operations in a very convenient way. For each respective DNA-based gate design, a predetermined mixture is supplied containing a specific single stranded sequence to induce the appropriate chemical reaction which is known as the base mixture. If the gate input sequence provided is complementary to the base sequence then the corresponding double stranded DNA sequence will form. Thus, the presence or absence of a double stranded sequence is used to evaluate the gate output whereas the presence of a double stranded sequence represents a true evaluation and it's absence represents a false evaluation.

Fluorescent labels can be used to detect the presence or absence of the double stranded sequence. In this process fluorescent molecules are attached to the nucleotide sequence, which absorbs and emits light at a particular wavelength. Thus, by attaching the fluorescent molecule to one of the strands of the double stranded sequence, the double stranded sequence can be detected. It's presence can be identified by examining the sequence solution at the fluorescent probe's characteristic wavelength.

The presence of a fluorescently labelled double stranded sequence only works if the single stranded labelled sequences are removed. Deoxyribonuclease (DNase) is an enzyme that breaks down the single stranded DNA sequences by degrading the sugar bonds connecting adjacent to nucleic acids.

The final step of the DNA-based logic gates is to use the output observed at the previous gate as the input into the next logic gate in the circuit.

The representative sequences can be dynamically assigned and a new set of complementary sequences can be substituted between evaluation of the previous gate and the insertion of the representative sequence in the next proceeding gate. Each DNA-based logic gate design is built on the preceding set of procedures. Individual gate logic is achieved through the introduction of a specific complementary sequence in the base mixture provided to each gate. Specific gate construction for the traditional DNA-based Boolean logic gates for NOT, OR, AND, XOR, XNOR, NAND and NOR are discussed in the following section. All Boolean logic gates can be easily derived from the three fundamental logic gates AND, OR and NOT.

1) NOT Gate: The NOT gate often referred to as an inverter, is one of the simplest DNA-based logic gate. Only one input is supplied to the gate and the output is the corresponding complementary sequence. Because the output should evaluate true only in the presence of a false input and the base mixture provided to the gate contains the representative true sequence. DNase is supplied to destroy any single stranded sequences. If a double stranded sequence is observed then the result is true otherwise the result is false.

2) OR Gate: The OR gate evaluates true if at least one of the gate input is true. DNase is supplied to destroy any single stranded sequences. If a double stranded sequence is observed then the result is true otherwise the result is false.

3) AND Gate: The AND gate evaluates true if both inputs are true. DNase will destroy any single stranded sequence in the mixture. If a double stranded sequence is observed then the result is true otherwise the result is false.

4) XOR Gate: The XOR gate evaluates true only if exactly one of the input sequences evaluate true. With binary inputs, XOR is defined as evaluating true if input values are opposite. In DNA-based logic gates the XOR gate has the most simplistic design since no

base sequence needs to be supplied to the gate. Opposite input sequences are complementary and will bind together to form a double stranded sequence. If the inputs are not opposite then the sequences will not be able to bind with each other and DNase will destroy both input sequences.

5) XNOR Gate: The XNOR gate which evaluates true when both inputs are the same, is created by applying the NOT gate to one of the inputs then applying the XOR gate to the result and the other input. Like the preceding gate designs, the presence of a double stranded sequence indicates a true evaluation of the gate while the absence of a double stranded sequence indicates a false evaluation of the gate.

6) NAND Gate: The NAND gate evaluates true if both inputs are not true. The DNA-based NAND logic gate is similar to the OR gate presented previously except the base sequence contains the sequence representing value true rather than false. Thus, at least one of the inputs must be false in order to form a double stranded sequence. DNase will destroy any single stranded sequence in the mixture. If a double stranded sequence is observed then the result is true otherwise the result is false.

7) NOR Gate: Finally, the NOR gate which evaluates true when both inputs are false, is implemented by applying the NOT gate to the output of the OR gate.

2 DNA Cryptography

DNA computing can be defined as a new technique for securing information with the help of biological structures. Leonard Max Adleman [2] can be considered as the pioneer of the DNA computing. He used this in 1994 for solving complex algorithmic problems. Now it is discovered that DNA can be used to store and transmit data. There are several advantages of DNA computing out of which a few of them are discussed as follows.

1) Minimum storage requirement: In a compact volume large amount of data can be stored. Calculations suggest that 1 gram of DNA contains 10^8 terabytes of data.

2) Speed: DNA computing techniques are almost 100 times faster than the modern-day fastest computer.

3) Minimum power requirements: DNA computing needs very less or no power at all compared to modern day computers.

DNA cryptography is defined as a process of hiding data in terms of DNA sequence. At present, the work in the field of DNA cryptography is focused on the use of DNA sequences to encrypt binary data in some form or other. In the near future, DNA computing will become as one of the leading techniques for securing information. Some of the DNA cryptographic techniques are discussed as follows.

2.1 DNA Complement Operation

In DNA complement operation the four nucleotide bases adenine(A), cytosine(C), thymine(T) and guanine(G) are substiuted according to the complementary rule and antiparallel manner where A is substituted with T and vice-versa. Similarly C is substituted with G and vice-versa. For example, if the input DNA sequence is ACTGACTG, then it's complemented DNA sequence will be TGACTGAC.

2.2 DNA Digital Coding

It is a technique of mapping the 4 different bases of DNA that are A, C, T and G with 0 and 1. Plain text messages can be easily encoded using this scheme. There are 24 such patterns possible but only 8 unique combinations are considered which fit the complimentary rule. This will be clear with the following example. Suppose someone wants to send the number 97 using DNA encoding. He or she can convert 97 to binary, by breaking 9 to 4 bit binary form 1001 and 7 is converted into 0111. Then both the binary forms of 9 and 7 are joined together. The resulting binary number will be 10010111.

Table 1: Conversion scheme for binary form to DNA nucleotide

Binary Form	DNA Nucleotide
00	A
01	T
10	C
11	G

Starting from the left most bit, two consecutive binary digits are taken and converted to corresponding DNA nucleotide bases following the scheme described in Table 1. In this way finally, the number "97" will be encoded as "CTTG". Now the encrypted message "CTTG" will be sent through a channel to the receiver. The receiver then decodes it and extracts the original message.

2.3 Hao's Permutation and Fractal Sequence Representation

Hao *et al.* [32] designed and proposed a DNA fractal sequence representation approach. A complete genome of length N is given which may be circular or a linear DNA sequence composed of N letters from the alphabets A, C, G and T. The authors designed a mapping technique that maps the four letters A, C, G and T to the base 4 number

system. α: {G,C,A,T}→{0,1,2,3}.

$$x = \Sigma_{i=1}^{k} 2^{k-i}[\alpha(s_i) >> 1] \quad (1)$$

$$y = \Sigma_{i=1}^{k} 2^{k-i}[\alpha(s_i) \& E] \quad (2)$$

In Equations (1) and (2) E means a binary number 1, ">> 1" indicates the right shift by one bit, symbol "&" is bitwise AND operator and s stands for the chosen DNA sequence. Here is a mapping function which converts the selected sequence into its corresponding base 4 number system.

This permutation approach is robust and provides high security, particularly in image encryption. Using this approach authors have proposed a new key generation process for image encryption [56].

2.4 Polymerase Chain Reaction (PCR)

It is a technique using molecular biology which amplifies the DNA. The steps followed in PCR operation is denaturation, primer annealing and primer extension. In denaturation, a two single stranded DNA is formed from a double-stranded molecule. This is done by heating the sample at a very high temperature of about 94 to 96 degree Celsius. Then primer annealing is done at about 50 to 65 degree Celsius where the primers which are designed to amplify the DNA regions are attached to the complimentary sequences. Finally, primer extension is performed. In this step, the temperature is again raised to about 72 degree Celsius. Here, nucleotides are added to the strand of a short primer on the base of original DNA strand using polymerase enzyme.

Apart from traditional methods some of the hybrid DNA cryptographic techniques which are evolving in this era are discussed as follows.

2.5 Elliptic Curve Cryptography Using DNA Encoding

It is one of the most efficient public key cryptography methods [34,35] . There are several benefits and facilities of this technique such as reduced key size. The security provided by this algorithm is similar to the security provided by RSA algorithm but the key used is much smaller compared to the RSA algorithm. Elliptic curve arithmetic is used for this technique. The security is increased by encoding the message with a DNA encryption technique. Elliptic curve cryptography is implemented over this DNA encoded message, thereby making the method more robust and a hybrid one.

2.6 Quantum Cryptography Using DNA Encoding

Quantum cryptography can be explained as emerging security technique in which the receiver and the sender communicate through a quantum channel. Quantum cryptography is based on Heisenberg's uncertainty principle and no-cloning theorem. This is purely based on the laws of applied physics. DNA encoding can be applied in the encryption technique of the plain text that is being sent through the quantum channel. The process is tough to crack and has given birth to a new hybrid technique.

3 DNA Encryption Techniques

The technique of converting the plain text to cipher text with involvement of DNA is known as DNA encryption. In the following section four DNA encryption techniques are discussed.

3.1 DNA Random One-Time Pad Based

This encryption technique is implemented using a set of randomly organized non-repeating characters. These act as the input ciphertext. It is named as one-time pad because if an input ciphertext is used once it is not used again. This helps in increasing the security. In this scheme the length of the one-time pad should be equal to the length of the plain text. In order to convert the short segments of plain text messages to cipher text, DNA one-time pad process is used. A random and unique codebook is taken into account for replacing the plain text. The problem in this method is that it is applicable only on short messages. For large messages the current hardware is not suitable enough for one-time pad. The increase in size of the message escalates the complexity of DNA mapping.

3.2 DNA Chip Based

The introduction of DNA chip technology has been a great progress in the field of DNA cryptography. It is helpful for the manipulation of a huge amount of genome sequences along with storing and handling of biological information. The DNA chip is commonly known as microarray. The microarray is made of nucleic acid and its electronic circuit is composed of semiconductors. Encryption and decryption occur using biochemical processes and it can be applied in encryption of plain text messages and images. Since the DNA chip is a biological element, its properties may change due to other physical factors. This sudden change will have a negative impact on encrypted messages.

3.3 DNA Steganography

The technique of hiding messages inside another message is known as steganography. When DNA is used in steganography it is known as DNA steganography. The scheme allows the message to be hidden in an image, audio or even a video file. It is a new emerging technique in the field of DNA cryptography. This is ideal for hiding a large amount of data. The process involves biological strands hence the data can get corrupted due to the sudden change of environment.

3.4 DNA Fragmentation

This method is used for library construction in DNA sequence. It is used to split the DNA sequence into small pieces. Many encryption algorithms use this as a second layer of security. It is also implemented in encryption of the key.

4 Literature Survey

There are several research papers which explore the DNA based cryptographic techniques. In this section the summaries of some of them are presented in a nutshell.

These papers are further categorized into five classes. They are DNA-based symmetric cryptography technique, DNA-based asymmetric cryptography technique, DNA-based elliptic curve cryptography technique, DNA-based quantum cryptography technique and DNA-based cloud cryptography technique respectively. It is described below in details.

Zhang *et al.* [25] proposed a DNA cryptographic algorithm. The method is based on DNA fragment assembly. Authors have implemented the features of DNA digital coding, DNA molecular key and some software techniques in their algorithm. This technique follows the concept of symmetric key cryptography. The encryption mechanism is done here using DNA digital coding. The main disadvantage of this algorithm is the implementation of the DNA molecular key.

In [24] the authors have mentioned a new encryption scheme on data security and cryptography, based on DNA sequencing. In the proposed system the message is converted into its binary form. Prior to communication establishment, the session key is shared through a secure channel between sender and receiver. Two rounds of encryption are used in this technique. The security is increased by breaking the sequence into blocks which is followed by hexadecimal addition and subtraction. The encoding method used here is based on symmetric key cryptography. This concept can be implemented in real-time security of distributed network systems. The sharing of key during distribution is a real difficulty in this algorithm.

Ibrahim *et al.* [1] proposed a technique to enhance the security of data hiding using double DNA sequences. The main idea behind the designed scheme is the encryption of secret message to ensure security and robustness. The encryption is done in two phases. The encrypted message is hidden into another DNA reference sequence. Overall a new data hiding algorithm based on DNA sequences has been recommended. In this scheme hiding of data in repeated characters minimizes the modification rate. On analysing the security aspect of this algorithm, it can be concluded that it would be difficult for the attacker to identify the secret message. But, if somehow the attacker manages to obtain the secret message then the method can be broken down easily.

In [39] the authors have proposed a method to encrypt information with DNA-based cryptography which is performed on five main stages. The first stage is data preprocessing where binary data is converted into a DNA string. The second step is the key generation followed by the encryption process. The fourth step is the decryption process where the DNA strand cipher text acts as the input and the output is DNA plaintext. The secret key is used to decrypt the cipher text. The last step is data post-processing where the obtained DNA sequence plain text is converted into binary plaintext. This algorithm is very much secured since it has a double layer of security and is based on vigenere cipher. The time complexity involved in this algorithm is huge.

Anwar *et al.* [4] proposed a new DNA cryptographic algorithm. This encryption technique is a combination of XOR operation and symmetric key exchange. It is very simple but powerful algorithm. The scheme encrypts plain text message into DNA cipher text. In order to increase security, the message is checked at the receiver end. Sender uses the symmetric key technique and encrypts the plain text into DNA sequence. The message is then sent to the receiver through various insecure channels like the Internet. At the receiver end, the receiver decrypts the cipher text into plain text using the DNA sequence. The concept of DNA hybridization and matrix calculations are done here to minimize the time complexity. DNA sequences can store large messages in very compact form which is one of the major advantage of this algorithm. Implementation of this method in real life is very cost effective.

Bama *et al.* [49] provided an interesting algorithm for secure data transmission using various properties of DNA sequencing and substitution techniques. The encryption technique is mainly dependent on a substitution scheme and a selected DNA sequence. The DNA sequence is selected out of 55 million possibilities which make the algorithm very much secured. Some intelligent binary logic and reverse substitution techniques are used to recover the message during the decryption phase. This method is very simple, efficient and reliable. The proposed algorithm is already implemented in an Electronic Medical Record System. The substitution scheme used here needs to be protected because if the scheme is compromised then the whole method will be vulnerable.

In [52] the authors proposed a cryptographic algorithm based on DNA, random key generation scheme and matrix multiplications. This generated key is XOR-ed with the outcome of the scrambled matrix. As a result even though the same key and same message is used, each and every time this technique will generate a different cipher text. Here, a total of three keys are used *i.e.* the initial key, primer key and the generated key. The performance and security of the DNA-based algorithm is suitable for multilevel security. This DNA cryptographic algorithm can resist exhaustive attack, statistical attack and differential attack. For single level security this method unnecessarily increases the time complexity.

Raj *et al.* proposed a technique on DNA-based cryptography using random key generation and permutation [51] . The above algorithm uses the concept of DNA pattern generation in a random manner. The method is very simple where the encryption starts by first converting the plain text into ASCII code and then into binary form. Table 2 is used here to convert the binary data into DNA sequences.

Table 2: Conversion formula for binary code to DNA nucleotide

Binary Form	DNA Nucleotide
00	A
01	T
10	C
11	G

A DNA sequence is selected as a key and grouped in blocks where each block consists of four characters. A table is created on the basis of how the characters occupy the block positions. Finally, from this table the randomly selected DNA sequence gets converted into encrypted form. The cipher sequence along with the key is sent to the receiver. The DNA sequences are decoded by following Table 2. The reverse steps are applied to get back the original message. This algorithm is somehow different from others, since traditional mathematical operations or data manipulation techniques are not used. Hence this method cannot be applied for multilevel security.

In [44] the authors presented a method which gives a secure data transfer mechanism using symmetric algorithm through DNA cryptography. Initially, the input data, text or image is converted to ASCII value and then it is again converted into its binary equivalent. Now, the binary value is converted to DNA code. The DNA code is randomly assigned on the basis of a private key and is converted to the extended ASCII code. Finally, the message is encrypted using DNA code and clinical permutation is done with the private key. The proposed system is implemented using Java and falls in the category of modern symmetric key encryption technique. DNA chromosome need to be used during the data transmission. On deep analysis of the algorithm, we can conclude that this method uses a much faster and better encoding scheme than conventional cryptographic techniques. This scheme can be used to increase the security mechanism of wireless networks. However, the use of DNA chromosome increases the overall implementation cost of the algorithm.

Researchers in [28] came up with a new technique for secure data transmission using the process of XOR operation, one-time pad (OTP) scheme and DNA cryptography. OTP scheme is applied here by a suitable method which has some preconditions. XOR operation is applied between the OTP and binary form. The binary digits are converted into DNA sequence by the following scheme: 00=A, 01=T, 10=C and 11=G. After complementing DNA bases, the DNA sequence is reversed from right to left. Then resulting encrypted data is sent to the recipient. This algorithm provides three levels of security *i.e.* arithmetic operation or XOR operation, one-time pad and DNA complementary rule. Overall the process is very simple to understand but highly secured as the randomly generated OTP is very much hard to guess for an attacker. Since there are some preconditions applied, therefore the method is not so user friendly as the user always has to take care of the preconditions while choosing the OTP.

Sravanan *et al.* [50] proposed an algorithm based on the modified Shamir's secret algorithm as well as DNA-based encryption and decryption technique. In the receiver end, a group is involved instead of a single user. Some added security is incorporated in the algorithm. When all the clients in the group are involved in the decryption process, only then the secret message can be decoded. Mathematical calculations are performed to convert the message into ASCII values. It is then altered into DNA bases. The message is transmitted to the group of clients and then the message is decrypted using DNA encoding to increase the security of message transmission for multicast applications. The proposed protocols can be implemented in Python and Java. This process can be used in trust-based image encryption system in future. The method is suitable only for a group and if someone is missing then the message cannot be decrypted.

Kamaraj *et al.* [11] proposed a new cryptography algorithm based on DNA computing. The algorithm is divided into two stages namely encryption and decryption. The first step converts the data into the corresponding cipher text and then it is sent to the receiver. At the receiver end, the encrypted code is decoded into original data. Here, the input message is in the form of normal text which is given to the FPGA(Field-Programmable Gate Array) through PS 2 keyboard. The message is read by the FPGA as ASCII value codes. Then it is converted to the codon by a codon table provided by the authors. Vigenere cipher is used for the encryption of the codon. This algorithm gives an idea of double layer security with a symmetric key. The distribution of key is not discussed here hence it can be a hectic problem for the algorithm.

In [22] the authors proposed a new structure for distributed system security with the help of DNA cryptography and trust-based approach. A rule-based approach for evaluating the trust-management has been designed. It is processed using the reputation approach. The reputation approach contains three phases *i.e.* proof collection, reputation factor approximation and reputation confidence. In the rule-based approach, the authors have used a DNA-based cryptographic method where detailed rules for encryption and decryption are laid out. The trust-based distributed systems used here are extremely robust in dealing with the security aspects. The introduction of DNA-

based cryptography in this type of system will make the system highly secured. Data post-processing approach is integrated into this method to deal with various cyber-attacks. This method cannot have wide applications and is applicable to only trust-based distributed systems.

Roy *et al.* [17] designed a method to improve the key generation based on DNA synthesis. This system optimizes the encryption and decryption process. The plain text is converted to the primary cipher text by a first level key (PK1) along with an encryption algorithm. The concept of second level key is introduced which increases the security of this technique. The second level private key add primers and positions of introns which strengthen the cipher text. On analysing the proposed method against brute force attack, excellent results are achieved. It would take more than half a year for the hacker to decrypt the cipher text with the help of modern day computer. Time and space complexity associated with this method is very high.

In [3] the authors have introduced a complimentary pair approach instead of traditional DNA encryption method. Initially, the DNA bases are complemented in the following manner: A-T, C-A, G-C and T-G. Then a DNA reference sequence is selected and named as S. This S will be known to both sender and receiver. S is then complemented and named as S'. This S' is then sent to the receiver by using any steganographic technique. The receiver will decrypt cipher text S' with the help of S. Application of steganography enhances the security of the proposed method. The algorithm is implemented in Java. In order to decrypt the message, an attacker has to guess the randomly generated sequence S. There are roughly 55 million publicly DNA sequences are available, hence it will be very hard to crack S. This makes the algorithm a robust and reliable one. The distribution of S is not discussed properly and if the receiver does not know S from before then the algorithm cannot be applied in that case.

Rani *et al.* [37] developed a DNA-based encryption technique using XOR operations. Initially, the plain text is selected and a random key is generated. A Randomized codon list is created and XOR-ed with the key. Swap complement operation is applied to create the encrypted message. The key is generated on the basis of DNA properties and biotechnology. The XOR operation is very fast hence it is implemented in O (log N) time. In future, more work can be done on decreasing the space complexity of the algorithm.

Zhang *et al.* [53] designed a method on index-based encryption algorithm which follows the concept of symmetric key cryptography. The proposed technique is based on the index of string and block cipher. The plaintext is encrypted twice with the help of the key. First, the plain text is converted to ASCII code and then it is expressed in 8-bit binary value. DNA encoding technique is performed to convert the binary form into DNA sequences using the scheme described in Table 3.

Table 3: Conversion scheme from binary form to DNA nucleotide

Binary Form	DNA Nucleotide
00	C
01	T
10	A
11	G

In the next step, the key is selected and it is divided into two parts. Finally, the encryption process takes place. The uniqueness of this algorithm is that it gives a huge key space and an extremely complex encryption algorithm. The chaos mapping added in this algorithm increases the mathematical security. Key generation ensures that the huge key space is fully optimized and can prevent extensive attacks. The space complexity associated with this method is huge.

Borda *et al.* [12] proposed a method on secret writing with the help of DNA hybridization. The algorithm hides the data in artificial or real DNA digital form. It is based on the one-time pad (OTP) scheme. In the designed method the receiver and transmitter will have a set of such non-repeating strands. Each ssDNA from the set will be used once and then destroyed. The concept of OTP is applied with ssDNA key in order to encrypt the message. This message is hidden with the help of Viviana Risea's idea. The actual message is changed to ASCII value and then in binary form. One time pad is applied and finally the encrypted message is a set of segments which is complementary to the ssDNA. The encoded message will be transmitted in a compact form and is hidden using DNA steganography technique. The message recovery is possible for someone who has the knowledge of the medium containing the message, the one-time pad and the primer sequences which are used for the encryption process. This algorithm has the advantage of parallel computing. It's implementation is done using Bioinformatics Toolbox present in Matlab software. The use of this method requires high tech laboratories.

In [7], the authors proposed a new concept on DNA cryptography. It is based on Yet Another Encryption Algorithm (YAEA). YAEA was first proposed by Saeb and Baith. Symmetric key cryptography is used here. This method uses sequential search algorithm. Then it locates and returns one of the many positions of quadruple DNA nucleotides. These nucleotides represent the binary octet of each plain text characters. The decryption process is done with the help of pointer file and random binary file. This binary file is available to both sender and receiver from beforehand. In order to get a higher order of security, larger genome sequence is used. The technique can be used in large digital information products. If the receiver does not have the binary file from beforehand then he or she cannot apply this algorithm.

In networking and data communication the main con-

cern is security. Mobile networks are becoming vulnerable day by day. In [20] the authors have proposed a method to secure mobile networks through DNA-based cryptography. The message to be sent is initially converted into 8 bit extended ASCII code and then to binary form. DNA encoding, mRNA sequence, amino acid and some mathematical concepts are used for encryption procedure. The algorithm is implemented using C++ environment in Windows Vista machine. The proposed technique is secured enough to endure the brute force method as the permutations used in this methodology are very strong. This process can be applied as a hardware solution. The method can only be used in wireless communications.

Shinde *et al.* [26] proposed a new DNA-based cryptography technique. The method comprises of traditional cryptographic technique along with new approaches for enhancing the data security. Initially, the plaintext is converted into ASCII value then consequent binary strings. Further, the binary strings are converted into hexadecimal values and simultaneously using MD5 algorithm a 128 bit key is generated. This key is converted into the hexadecimal string of length 32 characters which are mapped to 16 dynamic values. The binary values are encoded with the help of mapping table. Some mathematical and logical operations are performed after encoding. An insecure transmission channel is used for data transfer. Here decryption is not exactly the reverse process of encryption. Some extra parameters are required for decryption procedure. This technique is very fast and efficient one. The algorithm is implemented on Java platform. The security provided in this algorithm is not suitable for multilevel applications.

Chavan designed a new DNA cryptographic technique based on DNA hybridization and one-time pad (OTP) scheme [15] . Here, same keys are used in encryption and decryption process, hence making the algorithm symmetric. One of the keys is a randomly chosen string of nucleotides forming a ssDNA sequence. The second key is a binary sequence that is used for the OTP. The length of the ssDNA sequence key should be half of the length of binary key. XOR technique, OTP, ssDNA sequence and oligonucleotides are used for encryption method. DNA hybridization is implemented in decryption procedure. Experiment results show that the security of this algorithm is very high. About 1 in 1.94 X 10^{84} combinations can be right while guessing the key. The main advantage of this technique is scalability and reusability. Nevertheless, as the data for encryption increases, the computational complexity also increases. However, in future with the increase in processing power of computers, this problem may be solved.

Verma *et al.* [23] have proposed an index based DNA encryption algorithm. The plain text messages are encrypted into DNA sequences with the help of index of strings and block cipher. The DNA sequence is then sent to the receiver through a secure communication channel. Initially, the plain text or message is converted into ASCII code and then converted into binary code. This binary code is further encoded into DNA sequence. An algorithm is designed to search the key sequence among the encoded DNA sequences. Finally, the sequences are given an index number which acts as the cipher text. It is very hard for any attacker to guess the real message. The main difficulty of this algorithm is to find a secure communication channel in order to send the DNA sequence.

Paspula *et al.* [16] proposed a unique cipher text generation procedure as well as a new key generation method. The key generation method has two rounds. A conventional cryptographic technique generates an intermediate form of cipher text and in the second round the intermediate form of cipher text is converted into final cipher text. The method generates a fake DNA sequence inorder to confuse an intruder. If the application requires a single layer of security then this algorithm unnecessarily increases the time and space complexity.

In [8] biotic pseudo DNA cryptography method has been proposed. The methodology uses splicing system to improve the security. The key is generated in a random fashion, due to this reason the degree and confusion of the algorithm increases and makes the resulting cipher text difficult to de-cipher. Robustness analysis of the method shows that the method is very much secured from common cipher attacks. The implementation of this algorithm requires high tech bio-computational laboratories.

Tanaka *et al.* [47] proposed a DNA cryptographic algorithm which is based on one-way public key. The keys are generated using ODN mixture for Pk_B and solid mixture for Pk_A where Pk_A and Pk_B are public keys A and public key B respectively. The plain text or message is encoded in a DNA sequence with the help of one of the public key. It is furthermore synthesized and ligated both with DNA synthesizer and the remaining public key. In order to decode the DNA sequence, PCR amplification with the help of a secret sequence is done. This is an asymmetric method which has a high level of security but very costly to implement.

Lai *et al.* [41] designed a method which is based on the asymmetric key algorithm. The proposed method uses DNA chip technology where the DNA chip is fabricated with probes. The probes are used for encryption and decryption purpose. This algorithm uses the National Engineering Centre for Biochip at Shanghai as the bank for generating the keys. On the basis of intensity of probes, the value of probes are assigned. If intensity is greater than some threshold, then the value is fixed to 1 else it is 0. The process uses two keys for encryption, one by the sender and another one by the receiver. In first step, the plaintext is converted to ASCII value and then to its equivalent binary code. These binary codes are arranged in the form of a matrix. For 0 and 1 in the matrix, probe 0 and probe 1 are selected respectively. These probes are spotted on the DNA chip and then fabricated. This fabricated chip now becomes the cipher text. The receiver uses hybridization technique and the decryption key to decrypt the cipher text. A light spot in the key indicates

high intensity that means 1 and dark spots correspond to 0. The use of two keys in the encryption process increases the complexity of the algorithm.

In [21] the authors have implemented a method which is based on the asymmetric key. The algorithm uses PCR amplification along with DNA digital coding and digital synthesis for encryption of the plain text. PCR amplification is added here to provide security and safeguard during the communication phase. This encryption scheme has high confidential strength and at the same time is very cost effective.

Vijayakumar *et al.* [55] have proposed a technique using DNA cryptography and hyper elliptic curve cryptography to enhance the level of security. In DNA-based elliptic curve cryptographic technique the key size used is quite large hence the message encryption and decryption time increases. The concept of DNA strands is used in order to remove the above limitation. In this method converting the original text message into DNA nucleotide is the first level of security. Koblitz method provides the second level of security. The encoded nucleotide is converted into numbers and then the numbers are mapped into points. These points act as plaintext for encryption using hyper elliptic curve cryptography. This method can be implemented using MATLAB simulation tool. Real time implementation of the algorithm will be a challenging one.

Barman *et al.* [9] have proposed a new method to develop a DNA cryptography technique through a hybrid approach. The technique is composed of traditional DNA cryptography and elliptic curve cryptography (ECC). In this method, the plain text is converted first to ASCII value and then to binary form. A DNA nucleotide is taken from publicly available sequences which will be known to both sender and receiver. These nucleotide bases are converted to binary form using DNA encoding scheme. Several pairs of binary numbers are produced and all these pairs are concatenated to generate a long binary number. Encoding is done here by following some tables. The Koblitz method is used to convert the decimal numbers into elliptic curve points. These points are again encrypted to another elliptic curve point with the help of ECC encryption expression. The encrypted points are in the form of cipher text points which are sent to the receiver. This DNA-ECC hybrid method is more efficient in terms of security than the present DNA cryptography techniques. It uses a small key size and at the same time has two levels of security. The proposed method can be implemented on FPGA-based embedded system. Since the key size is small, so this method is not very much secured from the brute force attack.

Gogte *et al.* [27] presented a new type of DNA cryptography system based on quantum cryptography for secure communication. Quantum cryptography can be explained as an emerging security technique in which two parties communicate through a quantum channel. It is based on Heisenberg's uncertainty principle and no-cloning theorem. Initially, a simulation of quantum key exchange along with authentication is done. This step is followed by an application of a DNA-based algorithm. The proposed system consists of the following steps. The first step is authentication, which is based on both the traditional and quantum cryptographic methods. Secure key exchange using the BB84 protocol is done in the second step. This protocol is purely a quantum cryptography based method. The designed algorithm follows this protocol as it is except for the method through which random bits and basis are generated. The DNA encryption algorithm uses a symmetric block cipher where the input is a 128 bit key. The method is perfectly secured from the man in the middle attack, eavesdropping, replay-attack, packet sniffing and spoofing. The technique is very expensive to implement in real life.

Cloud computing has become very popular. It has many features like cost effectiveness, resource-ness, sharing and easy to use. Nevertheless, the security provided in the cloud data is one of the main concerns. In [40], the authors have proposed a new DNA-based cryptography method to increase the security of cloud data. The proposed algorithm uses a symmetric key for the encryption process. Initially, the original text is encrypted using a key and then converted to binary text. DNA sequences are selected and converted to the corresponding DNA base pair cipher. Though the algorithm looks simple yet it is very much secured.

As the field of cloud computing started emerging, many companies are embracing this technique. Eventually, there are many risks involved in this technique like theft of data, data leakage *etc.* The concept of multi-cloud has evolved in order to cope up with the problems of cloud computing. In multi-cloud technique, the users' data are split into different parts and uploaded into multiple clouds. In [48] the authors have described a DNA-based cryptographic technique which can be used in multi-cloud computing environment to enhance the security. The proposed strategy is divided into two phases, namely data embedding and data extracting. Initially, the data is converted into binary form and then into DNA sequence. The base pairing rule is applied to the message. The index of nucleotides is searched and matched from the reference. The data is then sent over the cloud. Data extracting phase follows the reverse steps of data embedding phase. The cipher text is converted back to the original text. This step takes place at the receiver side. The security of this algorithm is very strong. The probability for the attacker to guess the message correctly is less than 1 in million chances. This algorithm is implemented using Microsoft Visual Studio 2010 and Microsoft SQL 2008 on Windows 8 platform. This strategy is proved to provide the cloud user with more secured storage. The method has huge time complexity.

In [10] the authors have proposed a DNA-based encryption method using BIG data. The idea is very innovative and tough to crack. If a third party or any unauthorized person tries to retrieve the message, then he or she will only be able to get the DNA sequences, without the

key nobody can break the encryption algorithm. When a large amount of data is to be stored using BIG data then the use of this encryption technique is suggested. The designed method uses PHP language and a DNA encoding table for the encryption process. So far BIG data analysis is facing many challenges. Therefore this encryption process can be used to solve some of the problems in BIG data analysis.

5 Discussion

The use of cutting edge technologies and the computational properties of DNA are bringing several cryptographic methods into existence. The key used in these techniques is one of the main factors. It helps to determine the strength of the algorithm. Most of these methods are designed using a symmetric key. These algorithms are efficient, fast and reliable. Nevertheless, if the key is known to the attacker then the method will be cracked in few minutes. The use of an asymmetric key is one solution to this problem. Even if one of the keys is known, without the private key it is impossible to break the algorithm. But asymmetric key increases the computational complexity and making the process slow down. If the data to be encrypted is huge then an asymmetric key is not at all preferred. These disadvantages have paved the way for hybrid cryptographic methods. The use of DNA encryption techniques with quantum cryptography and hyper elliptic curve cryptography methods have become the new area of research. But implementation of these methods will be very costly as well as a challenge to the computer engineers.

6 Conclusion

DNA cryptography provides a medium of ultra-compact information storage. A few grams of DNA can hold about 10^8 terabytes of data. Effective and efficient algorithms are implemented in order to bring DNA computing on a digital level and use it on large scale. In future, DNA encryption will replace the need of digital signature, authorization and digital timestamps as DNA itself is a unique signature. It is fast, reliable and can work in a parallel manner. DNA cryptography has a wide range of applications and can be implemented in various fields like mobile networks, cloud computing, multi-cloud computing, plain-text messages, images, videos, servers *etc.* Exploring the various characteristics of DNA molecule and using it in the field of cryptography is one of the main concerns among the researchers. In order to increase more security, work can be done on developing asymmetric keys which will make the system more secure. The encryption schemes used in the four cryptography techniques *i.e.* traditional cryptography, DNA cryptography, elliptic curve cryptography and quantum cryptography is being interchanged with each other and as a result new hybrid techniques are being invented. DNA has the potential to explore the further biological molecule based computation methods. The invention of energy efficient DNA computer chip by IBM has opened up new gates for a bright future in this field. DNA cryptography is in its primary phase and hence it's implementation will need bio-molecular labs and costly instruments which are major constraints for the smooth progress in this field.

References

[1] H. M. Abdelkader, F. E. Ibrahim, M. I. Moussa, "Enhancing the security of data hiding using double DNA sequences," in *Industry Academia Collaboration Conference (IAC'15)*, 2015. (`https://www.researchgate.net/publication/278028006_Enhancing_the_Security_of_Data_Hiding_Using_Double_DNA_Sequences`)

[2] L. M. Adleman,"Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021-1025, 1994.

[3] A. Aggarwal, P. Kanth, "Secure data transmission using DNA encryption," *International Journal of Advanced Research in Computer Science*, vol. 5, no. 6, pp. 57-61, 2014.

[4] T. Anwar, A. Kumar, S. Paul, "DNA cryptography based on symmetric key exchange," *International Journal of Engineering and Technology (IJET'15)*, vol. 7, no. 3, pp. 938-950, 2015.

[5] B. Arazi, C. M. Gearheart, E. C. Rouchka, "DNA-based active logic design and its implications," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 3, pp. 756-766, 2012.

[6] M. A. Athitha, M. A. Akshatha, B. Vandana, "A review on DNA based cryptographic techniques," *International Journal of Science and Research*, vol. 3, no. 11, pp. 2819-2824, 2015.

[7] S. T. Amin, S. E. Gindi, M. Saeb, "A DNA-base implementation of YAEA encryption algorithm," in *International Conference on Computational Intelligence*, pp. 120-125, 2006.

[8] E. S. Babu, M. H. M. K. Prasad, C. N. Raju, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," *International Journal of Network Security*, vol. 18, no. 2, pp. 291-303, 2016.

[9] P. Barman, B. Saha, "An efficient hybrid elliptic curve cryptology system with DNA encoding," *International Research Journal of Computer Science*, vol. 2, no. 2, pp. 33-39, 2015.

[10] M. S. S. Basha, I. A. Emerson, R. Kannadasan, "Survey on molecular cryptographic network DNA (MCND) using big data," in *Procedia Computer Science of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*, vol. 50, pp. 3-9, 2015.

[11] M. Bhavithara, A. P. Bhrintha, A. Kamaraj, "DNA-based encryption and decryption using FPGA," *International Journal of Current Research and Modern Education (IJCRME'16)*, pp. 89-94, 2016.

[12] M. E. Borda, T. Hodorogea, O. Tornea, "Secret writing by DNA hybridization," *ACTA TECHNICA NAPOCENSIS*, vol. 50, pp. 21-24, 2009.

[13] Z. Cao, L. Liu, Z. Guo, "Ruminations on attribute-based encryption," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 9–19, 2018.

[14] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[15] S. Chavan, "DNA cryptography based on DNA hybridization and one time pad scheme," *International Journal of Engineering Research and Technology (IJERT'13)*, vol. 2, no. 10, pp. 2679-2682, 2013.

[16] K. Chiranjeevi, S. L. Kumar, R. Paspula, "Hidden data transmission with variable DNA technology," *International Journal of Electronics and Information Engineering*, vol. 7, pp. 41-52, 2017.

[17] R. Chakraborty, G. Rakshit, B. Roy, "Enhanced key generation scheme based on cryptography with DNA logic," *International Journal of Information and Communication Technology Research*, vol. 1, no. 8, pp. 370-374, 2011.

[18] T. Y. Chang, M. S. Hwang, J. W. Li, C. C. Yang, "Simple generalized group-oriented cryptosystems using ElGamal cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111-120, 2003.

[19] C. C. Chang, M. S. Hwang, K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445-446, 2002.

[20] K. Chugh, H. Dhaka, H. Singh, A. K. Verma, "DNA based cryptography: An approach to secure mobile networks," *International Journal of Computer Applications*, vol. 1, no. 19, pp. 77-80, 2010.

[21] G. Cui, L. Qin, Y. Wang, X. Zhang, "An encryption scheme using DNA technology," in *IEEE International Conference of Bio Inspired Computing: Theories and applications*, pp. 37-42, 2008.

[22] M. Darbari, V. Prakash, "A new framework of distributed system security using DNA cryptography and trust based approach," *International Journal of Advancements in Research and Technology*, vol. 3, no. 3, pp. 1-4.

[23] M. Dave, R. C. Joshi, A. K. Verma, "Securing Ad hoc networks using DNA cryptography," in *IEEE International Conference on Computers and Devices for Communication*, pp. 781-786, 2006.

[24] S. Deb, N. Kar, A. Majumder, M. C. Pal, A. Saha, "Data security and cryptography based on DNA sequencing," *International Journal of Information Technology and Computer Science (IJITCS'13)*, vol. 10, no. 3, pp. 24-32, 2013.

[25] B. Fu, Y. Zhang, X. Zhang, "DNA cryptography based on DNA fragment assembly," in *IEEE International Conference Information Science and Digital Content Technology (ICICDT'12)*, vol. 1, pp. 179-182, 2012.

[26] L. Gehlot, R. Shinde, "A survey on DNA-based cryptography," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET'16)*, vol. 5, no. 1, pp. 107-110, 2016.

[27] S. Gogte, T. Nemade, P. Nalawade, S. Pawar, "Simulation of quantum cryptography and use of DNA-based algorithm for secure communication," *IOSR Journal of Computer Engineering*, vol. 11, no. 2, pp. 64-71, 2013.

[28] N. Gulati, S. Kalyani, "Pseudo DNA cryptography technique using OTP key for secure data transfer," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 5657-5663, 2016.

[29] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 59-71, 2017.

[30] T. Gulom, "The encryption algorithm AES-PES16-1 and AES-RFWKPES16-1 based on network PES16-1 and RFWKPES16-1," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 53–66, 2015.

[31] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 20–31, 2018.

[32] B. L. Hao, H. C. Lee, S. Y. Zhang, "Fractals related to long DNA sequences and complete genomes," *Chaos Solitons Fractals*, vol. 11, pp. 825-836, 2000.

[33] M. S. Hwang, K. F. Hwang, I. C. Lin, "Cryptanalysis of the batch verifying multiple RSA digital signatures", *Informatica*, vol. 11, no. 1, pp. 15-18, Jan. 2000.

[34] M. S. Hwang, P. C. Sung, C. S. Tsai, "Blind signature scheme based on elliptic curve cryptography," *Journal of Computer Society of India*, vol. 34, no. 3, pp. 58-60, July 2004.

[35] M. S. Hwang, C. S. Tsai, S. F. Tzeng, "Generalization of proxy signature based on elliptic curves," *Computer Standards and Interfaces*, vol. 26, no. 2, pp. 73-84, Mar. 2004.

[36] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of Proxy Signature Based on Elliptic Curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[37] S. Jain, M. Rani, Asha, "Enhancing asymmetric encryption using DNA-based cryptography," *International Journal of Computer Science Trends and Technology (IJCST'14)*, vol. 2, no. 3, pp. 7-11, 2014.

[38] A. Kahate, *Cryptography and Network Security*, Third Edition, Mc Graw HIll, 2016.

[39] N. S. Kazazi, M. R. N. Torkaman, "A method to encrypt information with DNA-based cryptography,"

International Journal of Cyber Security and Digital Forensics (IJCSDF'15), vol. 4, no. 3, pp. 417-426, 2015.

[40] A. Kumar, V. K. Pant, "DNA cryptography a new approach to secure cloud data," *International Journal of Scientific and Engineering Research*, vol. 7, no. 6, pp. 890-895, 2016.

[41] X. Lai, "Asymmetric encryption and signature method with DNA technology," *Science China Information Sciences*, vol. 53, no. 3, pp. 506-514, 2010.

[42] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[43] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[44] T. Mahalaxmi, B. B. Raj, J. F. Vijay, "Secure data transfer through DNA cryptography using symmetric algorithm," *International Journal of Computer Applications*, vol. 133, no. 2, pp. 19-23, 2016.

[45] A. Mersaid, T. Gulom, "The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1–11, 2016.

[46] R. Nag, A. Nath, D. Roy, "Image encryption using DNA encoding techniques: A brief overview," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 4, pp. 112-119, 2016.

[47] A. Okamoto, I. Saito, K. Tanaka, "Public key system using DNA as a one way function for distribution," *Biosystem*, vol. 81, no. 1, pp. 25-29, 2015.

[48] B. D. Phulpagar, R. H. Ranalkar, "DNA based cryptography in multi cloud security strategy and analysis," *International Journal of Emerging Trends and Technology in Computer Science (IJETICS'14)*, vol. 3, no. 2, pp. 189-192, 2014.

[49] K. Priyadarshani, R. Bama, S. Deivanai, "Secure data transmission using DNA sequencing," *IOSR Journal of Computer Engineering (IOSRJCE'14)*, vol. 16, no. 2, pp. 19-22, 2014.

[50] T. Purusothaman, K. Saravanan, "DNA-based secret sharing algorithm for multicast group," *Asian Journal of Information Technology*, vol. 15, no. 15, pp. 2699-2701, 2016.

[51] B. B. Raj, V. Panchami, "DNA-based cryptography using permutation and random key generation method," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 5, pp. 263-267, 2015.

[52] K. G. Raju, P. S. Varma, "Cryptography based on DNA using random key generation scheme," *International Journal of Science Engineering and Advance Technology*, vol. 2, no. 7, pp. 168-175, 2014.

[53] R. O. Sinnot, Z. Yupeng, Z. Yu, W. Zhong, "Index based symmetric DNA encryption algorithm," in *IEEE 4th International Congress on Image and Signal Processing*, pp. 2290-2294, 2011.

[54] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[55] P. Vijayakumar, V. Vijayalakshmi, G. Zayaraj, "Enhanced level of security using DNA computing technique with hyper elliptic curve cryptography," *ACEEE International Journal on Network Security*, vol. 4, no. 1, pp. 1-5, 2013.

[56] X. Wei, Q. Zhang, S. Zhou, "An efficient approach for DNA fractal based image encryption," *Applied Mathematics and Information Sciences*, vol. 5, no. 3, pp. 445-459, 2011.

Biography

Animesh Hazra is working as Assistant Professor in Jalpaiguri Government Engineering College, India. He has received master degree in Computer Science and Engineering from Jadavpur University in 2005. His area of expertise includes network security, cryptography, data mining, computer graphics and image processing. He has published several papers in international journals and conferences.

Soumya Ghosh is pursuing B.Tech. in Information Technology from Jalpaiguri Government Engineering College, India. His area of interest includes network security, cryptography and data mining.

Sampad Jash is pursuing B.Tech. in Information Technology from Jalpaiguri Government Engineering College, India. His area of interest includes network security and cryptography.

A Novel Scheme for the Preview of the Image Encryption Based on Chaotic Ikeda Map

Chunhu Li, Guangchun Luo, and Chunbao Li
(Corresponding author: Chunhu Li)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
Chengdu, Sichuan, 610054, China
(Email: lchh-tiger@163.com)

(Received June 01, 2017; revised and accepted Sept. 12, 2017)

Abstract

Image encryption has been a popular research field in recent decades. This paper presents a novel scheme for the preview of the encrypted image. Using the scheme can preview the encrypted-image before decryption. So we can get to know that this image is really needed before decryption. Using the scheme can save a lot of unnecessary decryption time. To the best of our knowledge, this work is the first attempt to present such a scheme in the field of image encryption. We present the design and implementation of the scheme. The design of the proposed scheme is efficient. The experiments results show that the suggested scheme satisfies the requirement. It provides the necessary properties for a secure image encryption scheme. These characteristics make it a suitable candidate for using in cryptographic applications.

Keywords: Chaotic Ikeda Map; Image Encryption; Image Encryption Preview

1 Introduction

Recently, with the rapid development of network technology and their increasing popularity, the roles of images in the exchange of information among people become more frequent, image data protection has become more and more important. To meet the needs of the image authentication, image encryption algorithms were proposed [21, 22, 45]. In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on. The first description of a chaotic process was made in 1963 by Lorenz [30], who developed a system called the Lorenz attractor that coupled nonlinear differential equations. The complex behavior of chaotic systems in nonlinear deterministic was described. The implementation of chaotic maps in the development of cryptography systems lies in the fact that a chaotic map is characterized by:

1) The initial conditions and control parameters with high sensitivity;

2) Unpredictability of the orbital evolution;

3) The simplicity of the hardware and software implementation leads to a high encryption rate [16].

These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [39].

Over the past two decades, the image encryption based on Chaos theory has become a hot research topic. A large number of digital image encryption schemes have been proposed with demonstrated success. The classic encryption architecture based on chaotic map has been investigated. Researchers have proposed many chaos-based digital image encryption schemes [2, 8, 9, 12, 20, 28, 29, 34, 38, 43, 49], which utilize chaotic maps. Jawad and his research group promoted a chaotic map-embedded Blowfish algorithm for security enhancement of color image encryption [25]. Mao and his research group proposed a new color image encryption scheme based on chaotic nonlinear adaptive filter [19]. Mirzaei and his research group designed a parallel encryption algorithm based on hyper chaos [31]. Haroun's real-time image encryption used a low-complexity discrete 3D dual chaotic cipher [18]. Xiao-Jun Tong and his partner proposed an image encryption algorithm based on cross chaotic map [40]. Guodong Ye's chaotic image encryption algorithm using wave-line permutation and block diffusion [47].

The average decryption time of images with different sizes is different. The larger the encrypted image is, the longer it takes to decrypt. Decrypting a 2048×2048 image takes about 50 times as much time as a 256×256 image [6, 7, 13, 33]. So how do we get to know that this image is really what we need before decryption? In order to solve this problem, this paper gives a novel solution. Before decryption, we can decrypt the key region that has been set up in advance, so as to find out if it is the image we are interested in. We can manually or automatically

select one or more key regions of the image that will be encrypted. We encrypt the key region image and the entire image separately. The two encrypted images are combined into an encrypted image. The image segmentation and recognition algorithm will be employed.

The organization of this paper is as follows: Section 2 presents the related works. In Section 3, the details of our scheme are proposed. The experimental results are introduced in Section 4. The security discussion is shown in Section 5. Finally, the conclusions are drawn in Section 6.

2 Related Works

We categorize the related work into three topics, and each topic is summarized separately.

2.1 Image Encryption

There are many image encryption algorithms. They have some common characteristics, which are some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties. In [28], we proposed an encryption algorithm based on chaotic tent map. In [26], Manish and his team presented a new algorithm for image security using ECC (Elliptic Curve Cryptography) diversified with DNA encoding. Zang *et al.* suggested a novel optical image encryption algorithm, which based on spatially incoherent illumination [48]. Akhavan and his partners proposed a novel parallel hash function based on 3D chaotic map [4]. Choosing a suitable image encryption algorithm is not difficult.

In this paper, we presents an image encryption algorithm, which is based on the chaotic Ikeda map. The design of the proposed algorithm is simple and efficient. It provides the necessary properties for a secure image encryption algorithm including the confusion and diffusion properties. We use well-known ways to perform the security and performance analysis of the proposed image encryption algorithm. Simulation results show that the suggested algorithm satisfies the required performance tests such as large key space, high level security, and acceptable encryption speed. The fail-safe analysis is inspiring and it can be concluded that the proposed algorithm is efficient and secure. These characteristics make it a suitable candidate for using in cryptographic applications.

In physics and mathematics, the Ikeda map is a discrete-time dynamical system given by the complex map [23]. The original map was proposed first by Ikeda as a model of light going around across a nonlinear optical resonator in a more general form. In 1979, Kensuke Ikeda did an experiment on brain simulation [24]. The result confirms that the Ikeda model with its multiple extrema nonlinear function is a good candidate for chaos generation dedicated to encryption [27].

$$z_{n+1} = A + Bz_n e^{i(|z_n|^2+C)}. \quad (1)$$

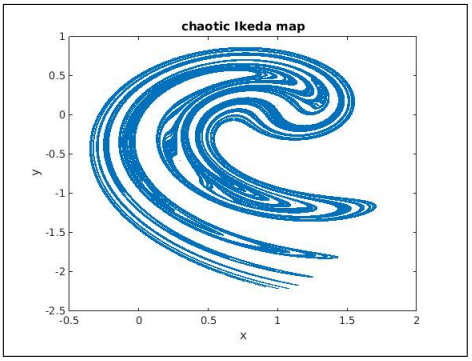


Figure 1: The image of the chaotic Ikeda map

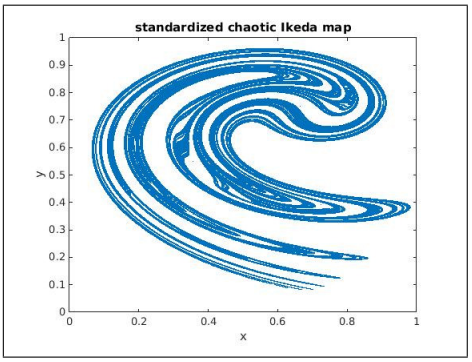


Figure 2: The image of the standardized chaotic Ikeda map

The complex Ikeda map is reduced to the above simplified form by Ikeda, Daido and Akimoto. Where z_n stands for the electric field inside the resonator at the n-th step of rotation in the resonator, A, B and C are parameters which indicate laser light applied from the outside, and linear phase across the resonator, respectively. In particular the parameter $B \leq 1$ is called dissipation parameter characterizing the loss of resonator, and in the limit of $B = 1$ the Ikeda map becomes a conservative map.

A 2D real example of the complex map is:

$$x_{n+1} = 1 + \mu(x_n cost_n - y_n sint_n) \quad (2)$$

$$y_{n+1} = \mu(x_n sint_n - y_n cost_n) \quad (3)$$

where μ is a parameter and $t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}$.

For $\mu \geq 0.6$, this system has a chaotic attractor. The Ikeda map has the dynamical behavior of nonlinear systems.

Using MATLAB in the experiments, the Ikeda equation parameter μ was selected as $\mu = 0.9$, in this case the system has a chaotic behavior. Figure 1 shows trajectories of 10000 random points for various values.

In order to apply the chaotic Ikeda map to image encryption, we made the transformation, let all $x_n \in (0,1)$ and $y_n \in (0,1)$, $n \in$ [0,1,2,$\cdots$], showing in Figure 2.

2.1.1 The Image Encryption Algorithm

In this section, we use the chaotic Ikeda map Equation (2) and Equation (3) to implement encryption process. This

paper proposes an image encryption algorithm includes the following main steps:

1) Read plain-images (original-image) ($P_{a\times b\times c}$), get size of P, *e.g.* using $[a, b, c]$ save size of P, let $N = a*b*c$, let $x(0) = 0.100001$, $y(0) = 0.100003$;

2) Input the secret (encryption) key μ into the chaotic ikeda map equation. Iterate the chaotic ikeda map N times using system Equation (2) and Equation (3), obtain an array $X_{(N)}$ and $Y_{(N)}$;

3) Confusion: Change $X_{(N)}$ into $[0, 255]$ using $X_{(N)} * 1000 \ mod \ 256$, we can get $C_{X_{(P)}} = X_{(N)} \ XOR \ P_{a\times b\times c}$;

4) Diffusion: $C_{Y_{(P)}} = Y_{(N)} * C_{X_{(P)}}$;

5) Change $C_{Y_{(P)}}$ into $C_{a\times b\times c}$, which is encrypt each element of matrix ($P_{a\times b\times c}$) using the key array $X_{(N)}$ and $Y_{(N)}$, namely, mix the confusion of the original image ($P_{a\times b\times c}$) ($C_{X_{(P)}}$) components with the diffusion of the original image ($P_{a\times b\times c}$) ($C_{Y_{(P)}}$), get the resulting image is the ciphered image $C_{a\times b\times c}$.

2.1.2 The Image Decryption Algorithm

In this section, we use the chaotic Ikeda map Equation (2) and Equation (3) to implement decryption process. This paper proposes an image decryption algorithm includes the following main steps:

1) Read ciphered-images (encrypted-image) ($C_{a\times b\times c}$), get size of C, *e.g.* using $[a, b, c]$ save size of C, let $N = a * b * c$, let $x(0) = 0.100001$, $y(0) = 0.100003$, here $x(0)$ and $y(0)$ must be same as encryption process;

2) Input the secret (encryption) key μ into the chaotic ikeda map equation. Iterate the chaotic ikeda map N times using system Equation (2) and Equation (3), obtain an array $X_{(N)}$ and $Y_{(N)}$;

3) Inverse confusion: Change $X_{(N)}$ into $[0, 255]$ using $X_{(N)} * 1000 \ mod \ 256$, we can get $P_{X_{(C)}} = X_{(N)} \ XOR \ C_{a\times b\times c}$;

4) Inverse diffusion: $P_{Y_{(C)}} = P_{X_{(C)}} * Y_{(N)}^{-1}$;

5) Change $P_{Y_{(C)}}$ into $P_{a\times b\times c}$, decrypt each element of matrix ($C_{a\times b\times c}$) using the key array $X_{(N)}$ and $Y_{(N)}$, namely, mix the confusion of the ciphered image ($C_{a\times b\times c}$) ($X_{(C)}$) components with the diffusion of the ciphered image ($C_{a\times b\times c}$) ($Y_{(C)}$), get the resulting image is the original image $P_{a\times b\times c}$.

2.2 Image Segmentation

Many image segmentation techniques are available in the articles [1, 11]. They proposed a number of related algorithms and schemes. In [17], a novel method is proposed for performing multi-label, interactive image. In [10], Boykov and his partners focused on possibly the simplest application of graph-cuts: segmentation of objects in image data. Vese and his research group proposed a new multiphase level set framework for image segmentation using the Mumford and Shah model, for piecewise constant and piecewise smooth optimal approximations [42]. We can choose an image segmentation algorithm for image segmentation.

2.3 Image Recognition

Image recognition technology has been studied by many scholars in recent years. In [37], Shi and his research group proposed a novel approach for learning coupled mappings to improve the performance of low-resolution (LR) face image recognition. In [46], Wu and his research partners presented a state-of-the-art image recognition system, Deep Image, developed using end-to-end deep learning. In [41], a neural network model, the hyper-column model (HCM), which is applicable to general image recognition, was proposed by Tsuruta and his partners. We can choose an image recognition algorithm to automatically select the feature regions from the image.

3 Proposed Scheme

Before introducing the preview scheme, we first introduce a definition that is the Preview-Region-Image. The Preview-Region-Image is the key region which is a part of the original image. Then we can find out if the original image is the image we are interested in.

We can manually or automatically select one or more Preview-Region-Image from the original image that will be encrypted. The Preview-Region-Image and the original image are encrypted separately. The two encrypted images are combined into an encrypted image. The decryption process is exactly the opposite of the encryption process. In order to preview the image, we extract and decrypt the encrypted Preview-Region-Image from the encrypted image. Details are given in the following encryption and decryption schemes.

3.1 The Image Encryption Preview Scheme

In this section, we give the processing flow of the image encryption scheme. The flowchart of the image encryption scheme is shown in Figure 3. This paper proposes an image encryption scheme which includes the following main steps:

1) Select the Preview-Region-Image. Two methods of selection can be used. Get the original image I[$a \times b \times c$], $c = 2$ or 3.

   - Using the mouse click spot as the center manually selects a region.
     a. $a > 256$ and $b > 256$, selects a region ($256 \times 256 \times c$), save to an array K[$256 \times 256 \times c$];

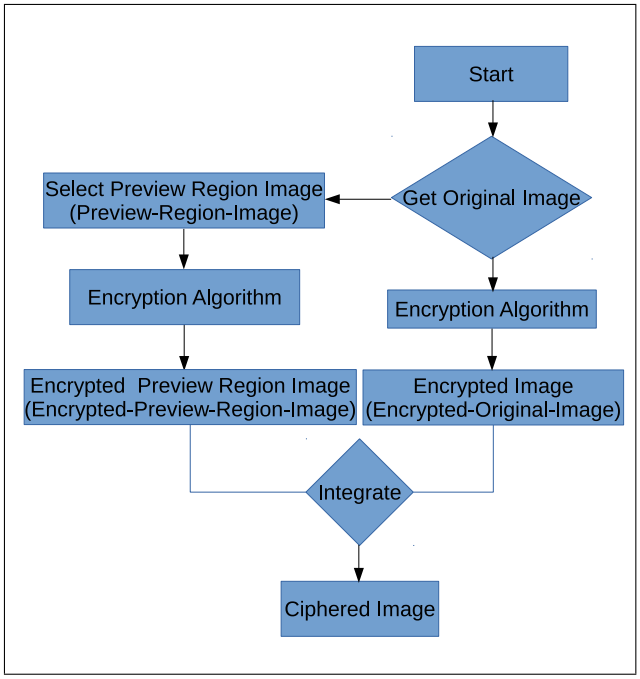


Figure 3: The flowchart of the image encryption scheme

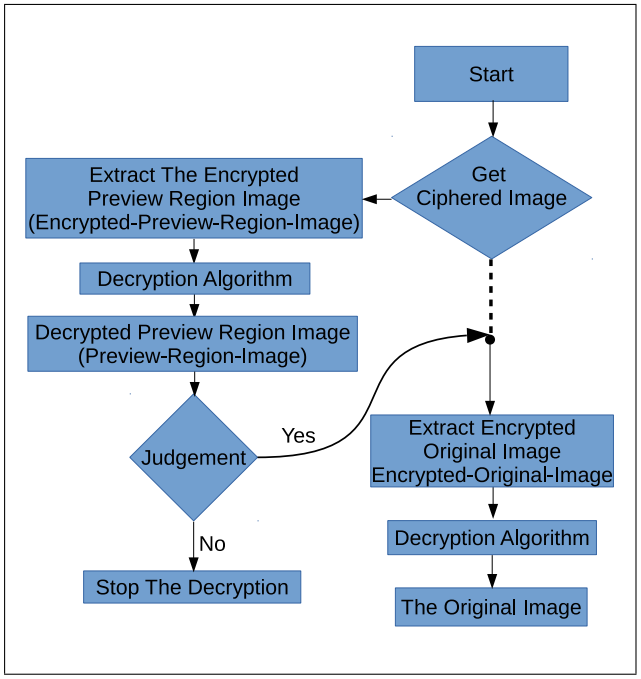


Figure 4: The flowchart of the image decryption scheme

b. $a > 256$ and $b < 256$, selects a region $(256 \times b \times c)$, save to an array K$[256 \times b \times c]$;

c. $a < 256$ and $b < 256$, selects a region $(a \times b \times c)$, save to an array $K[a \times b \times c]$;

d. standardize the array K to $SK[256 \times 256 \times c]$, insufficient 0 fill. the array $SK[256 \times 256 \times c]$ is named as Preview-Region-Image, before we encrypt the original image.

- Before encrypting the original image ($I[a \times b \times c]$), we can use image recognition technology to automatically select a Preview-Region-Image from the original image, and standardize to $SK[256 \times 256 \times c]$, insufficient 0 fill.

2) Encryption. Using the image encryption algorithm. We encrypt the Preview-Region-Image ($SK[256 \times 256 \times c]$) that is selected in step (1), named as Encrypted-Preview-Region-Image ($CSK[256 \times 256 \times c]$). Encrypt the original image, named as Encrypted-Original-Image ($CI[a \times b \times c]$).

3) Integration. In this step, we integrate two encrypted images (Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$ and Encrypted-Original-Image $CI[a \times b \times c]$) save to the array $C[(a + (256 \times 256/b)) \times b \times c]$. We place Encrypted-Preview-Region-Image (the encrypted preview region image) in front of Encrypted-Original-Image (the encrypted original image).

3.2 The Image Decryption Preview Scheme

In this section, we give the processing flow of the image decryption scheme. Before decryption, we first decrypt Encrypted-Preview-Region-Image to preview the original image. The flowchart of the image decryption scheme is shown in Figure 4. This paper proposes an image decryption scheme which includes the following main steps:

1) Extract the encrypted preview image. Extract the Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$ from the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$, Get the image region (its size is $256 \times 256 \times 3$), namely, the Encrypted-Preview-Region-Image $CSK[256 \times 256 \times c]$, from the beginning of the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$;

2) Decrypt the encrypted preview image. Decrypt the Encrypted-Preview-Region-Image (the encrypted preview image) $CSK[256 \times 256 \times c]$, get the Preview-Region-Image (the preview region image) $SK[256 \times 256 \times c]$, and show it;

3) Decrypt the encrypted original image. In Step 2, if we find that this image is the image we need. Extract the Encrypted-Original-Image (the entire encrypted original image) $CI[a \times b \times c]$) from the encrypted image $C[(a + (256 \times 256/b)) \times b \times c]$, and decrypt it. In Step 2, if we find that this image is not the image we need, stop the decryption.

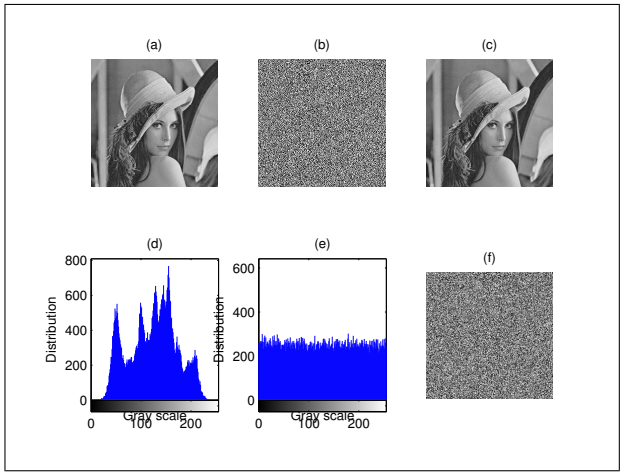


Figure 5: (a) The original image; (b) The encrypted image; (c) The decrypted image; (d) The histogram of original image; (e) The histogram of ciphered image; (f) The decrypted image with wrong key.

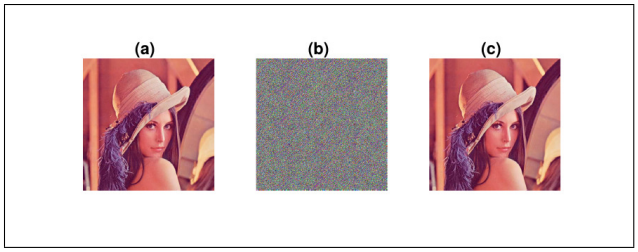


Figure 6: (a) The original image; (b) The encrypted image; (c) The decrypted image.

4 Experimental Results

4.1 Experimental Results of The Image Encryption

The efficiency of the proposed image encryption algorithm is shown in the following experimental results. The standard gray scale image Lenna (Figure 5(a)) with the size 256×256 pixels is used for this experiment.

The results of the encryption are presented in Figure 5(b). As can be seen from the encrypted image Figure 5(b), there are no patterns or shadows visible in the corresponding cipher image. The result of the decryption is presented in Figure 5(c). As can be seen from the decrypted image Figure 5(c), it is not different from the original image.

The color image Lenna with the size $512 \times 512 \times 3$ pixels is used for this experiment. The Figure 6(a) is the color image of Lenna, Figure 6(b) is the encrypted color image of Lenna, and Figure 6(c) shows the decrypted color image of Lenna from Figure 6(b).

The result of the decryption using wrong key is presented in Figure 5(f). As can be seen from the Figure 5(f), there are no patterns or shadows visible in the corresponding ciphered image.

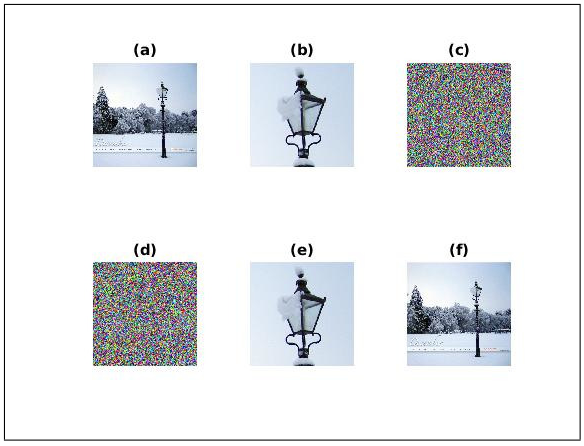


Figure 7: (a) The original image ($1024 \times 1024 \times 3$); (b) The preview region image ($256 \times 256 \times 3$); (c) The encrypted preview region image; (d) The integrated encrypted image; (e) The decrypted preview region image; (f) The decrypted original image.

4.2 Experimental Results of The Image Encryption Preview Scheme

The efficiency of the proposed image encryption preview scheme is shown in the following experimental results. The color images with different sizes are used in this experiment.

The color image with the size $1024 \times 1024 \times 3$ is used in this experiment. The Figure 7(a) is the color image of street lamp in snow ($1024 \times 1024 \times 3$), Figure 7(b) is the preview region image ($256 \times 256 \times 3$), which is a party selected from Figure 7(a), Figure 7(c) shows the encryption of Figure 7(b), Figure 7(d) shows the integrated encrypted image (include the encryption of the preview region image and the entire encrypted original image), Figure 7(e) shows the preview of the encryption image, Figure 7(f) shows the decrypted color image of street lamp in snow.

We have also done another experiments using the color image with the size $2048 \times 2048 \times 3$, as shown in Figure 8.

5 Security Analysis

Security is a major issue of a cryptosystem. When a new cryptosystem is proposed, it should always be accompanied by some security analyses. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analyses have been performed on the proposed scheme like key space analysis, distribution of the cipher-text, correlation analysis of two adjacent pixels, information entropy, plain-text sensitivity analysis, etc. The security analysis demonstrates a high security level of the new scheme.

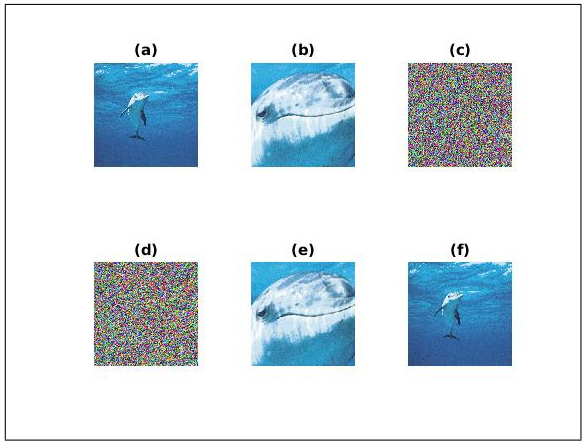


Figure 8: (a) The original image ($2048 \times 2048 \times 3$); (b) The preview region image ($256 \times 256 \times 3$); (c) The encrypted preview region image; (d) The integrated encrypted image; (e) The decrypted preview region image; (f) The decrypted original image.

5.1 Key Space

For every cryptosystem, the key space is very important. The key space of an encryption algorithm should be large enough to resist brute-force attacks. In our proposed scheme, the key space of the image decryption is computed by:

$$T(\mu, x_0, y_0) = \theta(\mu \times x_0 \times y_0),$$

where $x_0 \in [0, 1]$, $y_0 \in [0, 1]$, $\mu \geq 0.6$, the each precision of x_0, y_0 and μ is 10^{-16}, namely, the size of key space is 2^{160} $(((10^{16})^3))$. This key space is big enough for brute-force attacks [32]. In this scheme, we take the key to the original as follows: $x_0 = 0.100001$, $y_0 = 0.100003$, $\mu = 0.9000000001$. When taking the wrong key: the difference between wrong and right key is 10^{-16}. For example, using $\mu = 0.9000000001000001$ as the wrong key to decrypt the encryption image, we get a wrong decrypted image shown in Figure 5(f).

5.2 Distribution of The Ciphertext

An image histogram displays that how pixels in an image are distributed by plotting the number of pixels. Here we take a Lenna image (its size is 256×256) as the original image. Histogram of the original Lenna image and the corresponding ciphered Lenna image are shown in Figures 5(d) and 5(e). As is shown, the histograms of the ciphered image is uniform and do not provide any clues to the use of any statistical analysis attack on the encrypted image [7] .

5.3 Correlation Analysis of Two Adjacent Pixels

The superior confusion and diffusion properties are shown in the correlations of adjacent pixels from the ciphered image [44]. We analyze the correlation between adjacent pixels in original and ciphered Lenna image. We calculate the correlation coefficient in the horizontal, vertical and diagonally, the following relation is used [5]:

$$C_r = \frac{(N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j)}{(N\sum_{j=1}^{N}(x_j)^2 - (\sum_{j=1}^{N} x_j)^2)(N\sum_{j=1}^{N}(y_j)^2 - (\sum_{j=1}^{N} y_j)^2)}$$

where x_j and y_j are the values of the adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We choose randomly 3000 image pixels from the original image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in horizontal, vertical and diagonally direction. It demonstrates that the encryption algorithm covers up all the characters of the original image showing a good performance of balanced 0 1 ratio. The correlation of the original image and the encrypted image are shown in Figures 9 and 10.

Table 1: Correlation coefficient of two adjacent pixels in simulated original and ciphered image

Direction	Original image	Ciphered image
Horizontal	0.9302	0.0057
Vertical	0.8367	0.0041
Diagonal	0.8623	0.0032

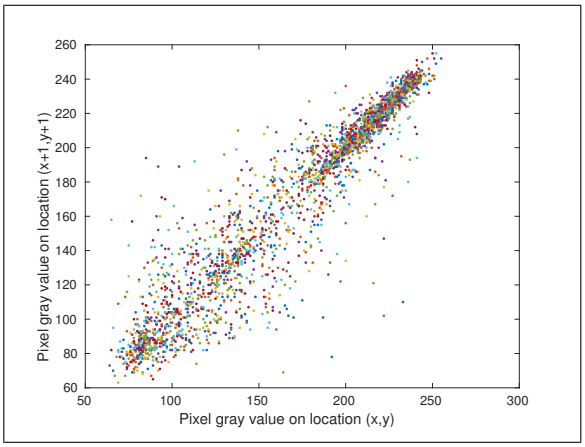


Figure 9: Correlation analysis of original image

5.4 Information Entropy

Information theory is a mathematical theory founded in 1949 by Shannon [36]. Modern information theory is concerned on data compression, error-correction, communications systems, cryptography, and related topics. There is a universal formula for calculating information entropy:

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \log_2 \frac{1}{P(s_i)}$$

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. The ideal entropy value

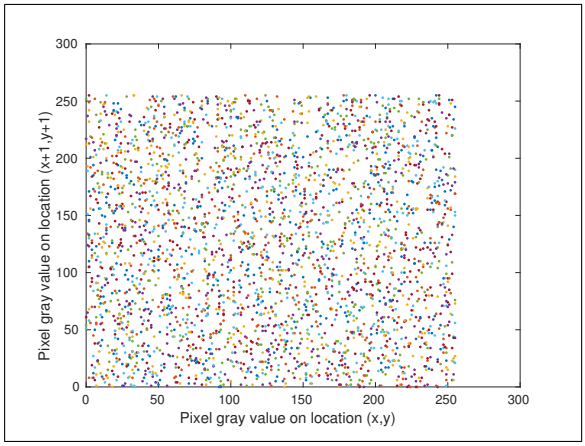


Figure 10: Correlation analysis of encrypted image

for an encrypted image should be 8. The calculation of entropy for the ciphered image (Figure 5(b)) is presented below:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} = 7.9986387.$$

The result shows that the entropy of the encrypted image is very close to the ideal entropy value, higher than most of other existing algorithms. This indicates that the rate of information leakage from the proposed image encryption algorithm is close to zero.

5.5 Plain-text Sensitivity Analysis (Differential Attacks)

Attackers often make a slight change for the original image, use the proposed scheme to encrypt the original image before and after changing, and through comparing two encrypted images to find out the relationship between the original image and the encrypted image. This kind of attack is called differential attack [44]. In order to resist differential attack, a minor alternation in the plain-image should cause a substantial change in the ciphered image. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: $NPCR$ and $UACI$ [14]. $NPCR$ represents the change rate of the ciphered image provided that only one pixel of plain-image changed. $UACI$ which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image. For calculation of $NPCR$ and $UACI$, let us assume two ciphered images C_1 and C_2 whose corresponding plain images have only one-pixel difference. Label the gray-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$; otherwise, $D(i, j) = 1$. $NPCR$ and $UACI$ are defined by the following formulas [35]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_i(i,j) - C_2(i,j)|}{255} \right] \times 100\%$$

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme by considering the one-pixel change influence on a 256-gray scale image of size 256×256. Also in order to clarify the effect of small change in the secret key such as initial condition ($x_0 = 0.100001$ to $x_0 = 0.1000010000000001$,$y_0 = 0.100003$ to $y_0 = 0.1000030000000001$) $NPCR$ is calculated. We obtained $NPCR = 0.00351$ ($1 - NPCR = 0.99649$) and $UACI = 0.367$. The percentage of pixel changed in encrypted image is over 99% even with one-bit difference in plain-image. $UACI$ is near to 1/3 as security required [3]. Moreover, in order to analyze the effect of the control parameter μ in the cipher image, the $NPCR$ test is conducted on the algorithm over this parameter. The process of the analysis is almost the same as the one for a single bit change in the plain-text, but this time we keep plain-image as original, and analyze the number of bit changes between two different cipher texts achieved from encryption with two different parameters with very small change ($\mu = 0.9000000001$ versus $\mu = 0.9000000000000001$). The calculated value of $NPCR$ for the proposed algorithm is 0.003169 which is very close to the ideal value. Also, compared with other chaos based algorithms such as $NPCR$ and $UACI$ of the proposed algorithm has a good ability to anti differential attack [15].

5.6 Analysis of Speed

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. We measure the encryption/decryption rate of several color images of different-size by using the proposed image encryption scheme. The time analysis is done on a core 2 duo 2.26Gz CPU with 4GB RAM notebook running on Debian 8.0 and using Matlab 2014b glnxa64. The average encryption/decryption time taken by the algorithm for different-sized images is shown in the Table 2. The average time of the image encryption preview scheme taken by the algorithm for different-sized images is shown in the Table 3.

6 Conclusion

In this paper we concentrate on the field of image encryption. The image encryption and decryption preview schemes have been given. In this scheme, we presented a method to preview the encrypted image before entire decryption. Using the scheme can save a lot of unnecessary decryption time. Experimental results show that

Table 2: Average ciphering time taking of a few different size images

Images size(pixels)	Bits/pixels	Ciphered time(s)
$256 \times 256 \times 3$	24	0.53-0.68
$512 \times 512 \times 3$	24	2.92-3.06
$1024 \times 1024 \times 3$	24	10.57-13.23
$2048 \times 2048 \times 3$	24	33.80-39.75

Table 3: Average ciphering preview time taking of a few different size images

Images size(pixels)	Bits/pixels	Ciphered time(s)
$256 \times 256 \times 3$	24	0.53-0.68
$512 \times 512 \times 3$	24	0.55-0.71
$1024 \times 1024 \times 3$	24	0.63-0.76
$2048 \times 2048 \times 3$	24	0.67-0.82

the scheme is efficient and usable for the preview of the image encryption. To the best of our knowledge, this is the first attempt to present such a scheme in the field of image encryption. The advantage of this scheme is that it is possible to know whether the encrypted image is the image we need. The disadvantage is that the encrypted preview image also takes up more storage spaces. Following up, we will try to solve this defect. One possible solution is that we use the encrypted preview image to replace the corresponding part of the original encrypted image.

Acknowledgments

This work is supported by the foundation of science and technology department of Sichuan province NO.2016GZ0077 and NO.2017JY0007.

References

[1] E. Aghajari and G. D. Chandrashekhar, "Self-organizing map based extended fuzzy c-means (seefc) algorithm for image segmentation," *Applied Soft Computing*, vol. 54, pp. 347–363, 2017.

[2] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbullu, "Chaos-based engineering applications with a 3d chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2015.

[3] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *Journal of the Franklin Institute*, vol. 348, no. 8, pp. 1797–1813, 2011.

[4] A. Akhavan, A. Samsudin, and A. Akhshani, "A novel parallel hash function based on 3d chaotic map," *EURASIP Journal on Advances in Signal Processing*, vol. 2013, no. 1, pp. 126, 2013.

[5] A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel block cipher based on hierarchy of one-dimensional composition chaotic maps," in *IEEE International Conference on Image Processing*, pp. 1993–1996, 2006.

[6] M. Amin, O. S. Faragallah, and A. A. A. El-Latif, "A chaotic block cipher algorithm for image cryptosystems," *Communications in Nonlinear Science & Numerical Simulation*, vol. 15, no. 11, pp. 3484–3497, 2010.

[7] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A*, vol. 366, no. 4, pp. 391–396, 2007.

[8] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[9] S. Bouchkaren and S. Lazaar, "A new iterative secret key cryptosystem based on reversible and irreversible cellular automata," *International Journal of Network Security*, vol. 18, no. 2, pp. 345–353, 2016.

[10] Y. Boykov and G. Funkalea, "Graph cuts and efficient n-d image segmentation," *International Journal of Computer Vision*, vol. 70, no. 2, pp. 109–131, 2006.

[11] L. Caponetti and G. Castellano, *Image Segmentation*, Springer International Publishing, 2017.

[12] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems & Software*, vol. 58, no. 2, pp. 83–91, 2001.

[13] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[14] N. D. Deckard, "Book review: Elementary statistics: A step by step approach, 9thed," *Teaching Sociology*, vol. 44, 2016.

[15] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.

[16] J. Gleick, "Chaos: Making a new science," *The Quarterly Review of Biology*, vol. 56, no. 64, pp. 1053–1054, 1989.

[17] L. Grady, "Random walks for image segmentation," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 28, no. 11, pp. 1768, 2006.

[18] M. F. Haroun and T. A. Gulliver, "Real-time image encryption using a low-complexity discrete 3d dual chaotic cipher," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1–13, 2015.

[19] H. I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Processing*, vol. 117, no. C, pp. 281–309, 2015.

[20] H. I. Hsiao and J. Lee, "Fingerprint image cryptography based on multiple chaotic systems," *Signal Processing*, vol. 113, pp. 169–181, 2015.

[21] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[22] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–556, Jan. 2000.

[23] K. Ikeda, H. Daido, and O. Akimoto, "Optical turbulence: Chaotic behavior of transmitted light from a ring cavity," *Physical Review Letters*, vol. 45, no. 9, pp. 709–712, 1980.

[24] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Optics Communications*, vol. 30, no. 2, pp. 257–261, 1979.

[25] L. M. Jawad and G. Sulong, "Chaotic map-embedded blowfish algorithm for security enhancement of colour image encryption," *Nonlinear Dynamics*, pp. 1–15, 2015.

[26] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on dna encoding and elliptic curve diffieVhellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[27] L. Larger, J. P. Goedgebuer, and V. Udaltsov, "Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos," *Comptes rendus - Physique*, vol. 5, no. 6, pp. 669–681, 2004.

[28] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[29] L. H. Liu and Z. J. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics & Information Engineering*, vol. 5, 2016.

[30] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[31] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 67, pp. 557–566, 2012.

[32] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[33] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitutionVdiffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science & Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[34] P. Praveenkumar, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Mojette (d) secret image "SEDIH" in an encrypted double image - a histo approach," *International Journal of Network Security*, vol. 19, no. 1, pp. 47-59, 2016.

[35] P. Schneier, Bruce/Sutherland, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1995.

[36] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[37] J. Shi and C. Qi, "From local geometry to global structure: Learning latent subspace for low-resolution face image recognition," *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 554–558, 2015.

[38] S. Sowmya and S. V. Sathyanarayana, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points over GF(p)," *International Journal of Network Security*, vol. 12, no. 3, pp. 137–150, 2011.

[39] J. C. Sprott, *Chaos and Time-Series Analysis*, Oxford University Press, 2003.

[40] X. J. Tong, Z. Wang, M. Zhang, and Y. Liu, "A new algorithm of the combination of image compression and encryption technology based on cross chaotic map," *Nonlinear Dynamics*, vol. 72, no. 1-2, pp. 229–241, 2013.

[41] N. Tsuruta, R. I. Taniguchi, and M. Amamiya, "Hypercolumn model: A combination model of hierarchical self?organizing maps and neocognitron for image recognition," *Systems and Computers in Japan*, vol. 31, no. 2, pp. 49–61, 2015.

[42] L. A. Vese and T. F. Chan, "A multiphase level set framework for image segmentation using the mumford and shah model," *International Journal of Computer Vision*, vol. 50, no. 3, pp. 271–293, 2002.

[43] X. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[44] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[45] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", *Journal of Systems and Software*, vol. 84, no. 12, pp. 2196–2207, 2011.

[46] R. Wu, S. Yan, Y. Shan, Q. Dang, and Gang Sun, "Deep image: Scaling up image recognition," *Computer Science*, 2015. DOI: 10.1038/nature0693.

[47] G. Ye, H. Zhao, and H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 1–11, 2015.

[48] J. Zang, Z. Xie, and Y. Zhang, "Optical image encryption with spatially incoherent illumination," *Optics Letters*, vol. 38, no. 8, pp. 1289, 2013.

[49] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, pp. 1–19, 2017.

Biography

Chunhu Li received his B.S. (2008) in computer science from Qingdao Agricultural University and M.S. (2011) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include cloud computing, network security, image encryption and artificial intelligence.

Guangchun Luo received his Ph.D. degree in computer science from UESTC in 2004. He is currently a professor of computer science at UESTC. His research interests include computer networks, mobile networks and network security.

Chunbao Li received his B.S. (2011) in computer science from China West Normal University and M.S. (2014) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include artificial intelligence, machine learning.

ZBMRP: Zone Based MANET Routing Protocol with Genetic Algorithm and Security Enhancement Using Neural Network Learning

V. Preetha[1] and K. Chitra[2]
(Corresponding author: V. Preetha)
Research Scholar, Department of Computer Science, Bharathiar University[1]
Coimbatore, Tamil Nadu 641046, India
(Email: preetha_mca2005@yahoo.com)
Department of Computer Science, Government Arts College[2]
Melur, Madurai, Tamil Nadu, India
(Received July 2, 2017; revised and accepted Dec. 3, 2017)

Abstract

Due to the rapid technological development all the inexpensive hand held devices can be quickly set up as a Mobile adhoc network (MANET). This makes it possible for efficient communication in disaster scenarios where instant communication is necessary. Our initial phase of research focuses on the two important protocols: Cluster Based Routing Protocol and Zone based Routing Protocol. Cluster based routing protocol, one of the methodology of hierarchical routing have been developed by researchers for easier routing of large scale networks. By aggregating nodes into clusters controlled by cluster heads, many cluster based routing protocols have been developed. The main challenging task is the Cluster head election in cluster based Protocols. Zone based Routing protocol, one of the Hybrid schemes in protocol classification, have been designed for large scale networks by focussing on Zone radius, InterZone and IntraZone routing. The main challenging task is the security Enhancement in Zone based routing Protocols. By considering the two important factors such as Cluster Head selection and security Enhancement, we designed the Zone based MANET Routing Protocol (ZBMRP) protocol. In this protocol,cluster or Zone based routing is performed with efficient Zone head. The Zone head is elected based on our proposed MANETIC algorithm which is based on the Metaheuristic Genetic Algorithm. In order to enhance the security of the protocol the registration of all the nodes and the authentication is carried out using our Registration & authentication algorithm which effectively uses the Neural Network learning approach. GACA and EWCA are the traditional important clustering algorithms with cluster head Election schemes. In order to analyse our Protocol based on the Zone head,the comparison is made with GACA and EWCA in terms of Load balancing factor,average number of clusters,Packet delivery ratio and throughput.

Keywords: Genetic Algorithm; Neural Network Learning; Zone Based Routing; Zone Head

1 Introduction

MANET as an emerging technology has a rapid growth from 1990s. The dynamic nature of the mobile adhoc networks demanded many challenges and issues and the network strategies have to be refined to achieve the better performance. Despite the fact that MANET has dynamic topology, limited channel bandwidth and limited battery power, Mobile adhoc networks is popular for group communication due to its robust ness and instant usage. MANETs as divergent to Infrastructure wireless networks gaining attention due to world wide mobile connectivity. Mobile Adhoc networks though started its technology from IEEE 802.11b, gained rapid importance due to its emerging trends in IOTs and pervasive pervasive computing. The vibrant wireless research DARPA Packet radio Network to military rescue and radio technologies. Though the research started from 1972, due to the advancement in MANET in recent IOT, Ubiquitous and Pervasive computing the research in MANET will never end up. Routing is the major challenging issue in a MANET. The depending on the different applications as Education, Disaster recovery, Commercial as vehicular adhoc network and so on. Some Systems demand a multi cluster environment to adapt dynamically for changing environments. A responsible and efficient node will be the leader. Also MANETs in very sensitive areas will face the problem of privacy and security. Many clustering algorithms have been proposed by researchers. Several Key Management schemes and Cryptographic functions were implemented

to ensure security. But till now a secured effective communication is a challenging task in MANETs.

1.1 Motivation

MANETS due to their low cost and easier deployment is widely used in all the fields especially in disaster recovery from natural disasters. Due to the tremendous increase in the number of users, different protocols are emerging depending on the applications and the need of the users. Every protocol is having its own advantages and lacks in some performance. Due to the varying mobility and link conditions it is often a challenging task to provide the required performance. The network resources, diversity of networks, load balancing routes, and efficient routing has to be considered as important factors while designing a Routing Protocol. Hierarchical routing is one of the approaches in MANET. It performs the the Intra routing within the Zone or cluster and Interrouting outside the cluster or Zone efficiently. The concept of dividing the networks into n-number of clusters will help for easier maintenance but the leader node should be very effective in communications. Traditional algorithms will not be sufficient to overcome all the hindrances in finding the specific route or for electing the leader. Hence we concentrate our work on the hierarchical routing which divides the network into zones and the zone leader is elected using Metaheuristic Genetic algorithm.Only the best fit node will be elected as a leader in our approach. Another promising factor is the lack of security which in technical words termed as malicious, Intrusion detections,Attacks in MANETs and so on. Cryptography will provide several solutions to the aspects of security in terms of confidentially, authentication, integrity and non repudiation. Many hash functions will solve the problem of security to some extent but we have designed the security framework by Neural network learning methodology in which only the authenticated nodes will enter into the network. Due to the Neural Network learning, the authentication process will be faster. The input to the Neural Network will be the cryptographic hash function. The Key sharing for secured username and password registration combined with Reed Solomon coding will provide security for the protocol.

1.2 Our Contribution

In prior we analysed the parameters for effective zones using fuzzy [11]. In our work we have chosen Genetic Algorithm, one of the soft computing techniques for Zone head selection. As the entire network falls on the efficiency of the zone head, the Zone head is efficiently chosen by the proposed MANET Algorithm based on Genetic Algorithm.Only the best fit nodes alone will participate in the ranking procedure. The fitness path is determined for specific route which reduces the latency in route determination and congestion and avoids unnecessary broadcasting and flooding messages. The leader will be responsible for all the further communication because the communication will be processed from zone head to another zone head. The main contributions of our proposed protocol are

1) MANET Algorithm based on Genetic approach is proposed for Zone head election.
2) Effective routing with prior link estimation knowledge.(fitness path).
3) Ranking of the nodes is performed which ensures the performance of the nodes and to identify the weak nodes.
4) Registration Procedure is carried out in the Entry point using encrypted username and password in which the Zone head will act as a administrator.
5) Packet verification for secure transmission of data through the supervised Neural Network learning and cryptographic hash function.

The remaining sections of the paper are systematized as follows: Section 2 gives a brief overview about the existing methodologies for Hierarchical Routing, Genetic Approach in MANET, Neural Network learning in MANET. Section 3 explains the proposed protocol including network model, Analysis of parameters using fuzzy, Neighbor discovery and zone forming, Zone head election using MANET algorithm, member Registration procedure with user id and password, Reed Solomon coding,Key sharing and Node learning using Neural Network and Node authentication. Section 4 illustrates the performance evaluation results of the proposed protocol. Section 5 presents the conclusion and future scope of the proposed protocol.

2 Related Work

This section provides an overview about the existing research works related to Hierarchial routing, Genetic Approach in MANET, Neural network approach in MANET.

2.1 Hierarchical Routing

The Investigation of the Research is conducted from the analysis of Routing protocols. No fixed infrastructure for MANET, Energy Constraint, Mobility factors and other factors are challenging when considering the routing protocols. Each node in a MANET will not have the same properties. Any two neighboring nodes will even differ in their signal strength, reliability, power and so on. Basically, the Routing Protocols are categorized as: Global/Proactive, On Demand/Reactive, Hybrid. Another Classification of Routing Protocols are: Flat Routing, Hierarchical and Geographic position assisted Routing. Hierarchical Routing is further classified as the following categories as: HSR, CGSR, ZRP and LANMAR. Every routing protocol has its own advantages and disadvantages. While Considering the Hierarchical Routing,

the Internet Hierarchy is a traditional Hierarchical Routing in the wired network. The most popular way of Hierarchical approach is the cluster based approach. In general, Cluster based routing protocol (CBRP) falls under the reactive category but due to its level-oriented administration and governance by cluster head it has the hierarchical component. CBRP has many advantages such as energy consumption and network performance. Thus a typical hierarchical structure can be implemented by partitioning the network into clusters depending on the geographic region, transmission range, and communication reliability irrespective of the sparse and dense regions. Hierarchical routing greatly increases the scalability of routing in ad hoc networks by increasing the robustness of routes. Jin *et al.'* [8] classified the clustering schemes under six categories as Dsbased, Low Maintenance, Mobility-aware, Energy Efficient, Load balancing and combined metrics based clustering. Cost comparison of the six clustering schemes and communication complexity are analyzed based on the ripple effect of re-clustering, stationary assumptions for cluster formation etc. Many researchers have focused the clustering schemes based on different metrics. Correa, Ospina, Hincapie (2007) [3] classified the Clustering Techniques for Mobile Adhoc Networks into eight categories as Lowest ID heuristic, Highest degree heuristic, k-CONID, Max-min heuristic (α, t) cluster framework, MobDhop DMAC and WCA and explained their advantages and disadvantages. In [10], Mehta and Rajput classified the clustering approaches based on its objectives and tabulated the advantages and drawbacks of the algorithms. From the related works, it is observed that WCA gained importance due to its consideration of its four factors and its objective function as $Wv = w_1\Delta v + w_2 Dv + w_3 Mv + w_4 Pv$.

Where w_1, w_2, w_3 and w_4 refers to the corresponding systems weighing parameters [2]. Hussein *et al.* [7] extended the weighted clustering algorithm (EWCA) for load balancing and stability of the network. In [8], Wang *et al.* proposed a new clustering strategy using Genetic Annealing based clustering Algorithm in weighted clustering algorithm for energy aware and topology management.

2.2 Genetic Approach in MANET

Genetic Algorithm, one of the soft computing techniques has been used by many researchers to solve optimization problems. Genetic Algorithm is widely used in all the areas of Engineering but the applications in MANET is very limited. The main advantage of genetic algorithm is its robustness in its performance which can be applied for previous learning. The objective function (or the desired outcome) for a given application would be to achieve improvements to an existing solution already in hand or simply finding a solution to a complex problem. Table 1 lists out the Authors and their work on Genetic Algorithm in MANET.

Table 1: The genetic approach in MANET

S. No	Authors	Genetic Approach
1.	Alba *et al.* [1]	For Optimum Broadcasting strategy
2.	Sahin *et al.* [14]	For Uniform distribution of mobile agents
3.	Sahin *et al.* [15]	For Topology control
4.	Preetha [13]	To Predict the stability of clusters in MANET

2.3 Neural Network Learning in MANET

Artificial Neural Network is one of the very powerful tool for solving complex problems. Neural Network is widely used in all the applications involving forecasting problems. In MANETs, Neural Network is used in Intrusion detection systems, Mobility prediction and delay prediction. Neural network based algorithms works superior to traditional algorithms. Because of its robust and self adaptive methods, even with minimal datasets and relationships, Neural networks can predict approximate values with high accuracy. Self organizing neural networks are used in behavior modeling in games [4]. For power systems static security assessment [6] multi-layer feed forward artificial neural network is used to implement the online module for power system static security assessment. In MANETs some of the usage of Neural network learning is tabulated as in Table 2.

Table 2: Neural networks approach in MANET

S.No	Authors	NN approach in MANET
1.	Kaaniche *et al.* [9]	For Mobility Prediction
2.	Singha *et al.* [16]	For Delay Prediction
3.	Gangwar *et al.* [5]	For Cluster Head Selection

Since Neural Network and Genetic Algorithm is very efficient, it is used in our ZBMRP protocol and the Performance is analysed and it emerges that under many circumstances it performs well.

3 Proposed ZBMRP Protocol

This section explains the proposed protocol in detail. ZBMRP focuses on the zone based clustering by analysing the efficient parameters using fuzzy logic. The best fit zone head is elected using MANET algorithm and a novel security method is imparted in the proposed protocol with highly secured node registration and authentication pro-

cedure using cryptographic hash functions and neural network learning.

The main stages of our proposed work are

- Network model;
- Analysis of Parameters using Fuzzy;
- Neighbor Discovery and Zone Forming;
- Link Estimation and Zone Selection;
- Zone Head Election using MANET Algorithm;
- Member Registration with user id and password;
- Reed Solomon coding;
- Key sharing and Node learning using Neural Network;
- Node authentication.

3.1 Network Model

The proposed scheme is deployed by a Network model by assuming as an undirected graph $G(V, E)$ where $V = \{v_1, v_2, \cdots, v_n\}$ represents the number of nodes and $E = \{e_1, e_2, \cdots, e_q\}$ is the set of edges connecting two nodes, only if they are located within the transmission range of each other. The proposed Zone based Routing protocol is based on the Radius R.

3.2 Analysis of Parameters Using Fuzzy

The parameters such as connectivity Index, Transmission range, Battery power, density of the nodes and mobility factors are analysed (see Table 3). In our previous work [12] we defined the parameters as:

$$connectivity = \frac{|largest\ connected\ component|}{N}$$

where N represents the total number of nodes participating in the network. Transmission range is defined as

$$\sum_{u \in V, u \neq v} \{D_{uv} < T_x, Transmission\ range.\}$$

Where D is the distance. Mobility may vary depending on the application. The energy states of node during a network may have sleep, idle, transmit and receive mode.

The fuzzy rule for the defined parameters is IF x_1 is A_{i_1} and ... and x_n is A_{i_n} **THEN** y is C_i, $i = 1, 2, \ldots L$. In our previous work we conclude using the fuzzy membership functions that the chance of effective clustering will be high,if the connectivity index is high and if the mobility and density are medium. This condition may exist particularly in applications such as disaster recovery model using MANETs.

Table 3: Parameters chosen for clustering and its range

Parameters chosen for clustering	**Range**
Connectivity Index of Particular zone	High connectivity
	Medium connectivity
	Low connectivity
Transmission Range (distance covered)	Long distance
	Short distance
	Medium distance
Mobility	High speed
	Medium speed
	Less speed
Density	Large denser area
	Medium denser area
	Lesser denser area

3.3 Neighbor Discovery and Zone Forming

The Zone radius is defined in ZBMRP. That is Zone radius is the minimum distance from the Zone head. A local Routing table is maintained in which every node will thus broadcast its own routing information to all the other nodes. Inter-Zone routes are established dynamically using the node membership information kept at each Zone head. Instead of flooding,Inter Zone routing protocol will help to find the route as a reactive component. It uses the Global reactive component. All the interior members will have the minimum distance less than R. All the Peripheral nodes will have the node distance exactly equal to R. For Intra Zone routing performance the Link state list, Peripheral node list, Inner Route list, Update Detect list, Periodic Update timer, Expiration of Link state routes and the IntraZone Agent are maintained. If the path to the destination is not within the Zone the InterZone routing is performed.

3.4 Link Estimation

The link phase is estimated based on connectivity index, transmission range. The energy of the node's bandwidth and queue congestion are analysed for the effective link phase determination. The values are normalized between 0 to 1.

3.5 Zone Head Election Using MANET Algorithm

Our proposed MANET algorithm for Zone head election is based on the Genetic algorithm.Genetic algorithm is used to find a better solution goal by using generations and survival of the fittest logic. But there will be randomization in exchange of data. But repeatedly performing different trials with different operations such as crossover,

mutation a new set of possible feasible solution can be obtained. The steps in the genetic algorithm are:

- Encoding of the data;
- Creating initial population;
- Selection;
- Crossover;
- Mutation;
- Elitism;
- Fitness value for chromosome.

Encoding of the Data: The number of nodes can be randomly selected and can be assigned unique IDs. Encoding can be binary encoding, Real valued encoding or Integer encoding. Binary encoding is represented as in Figure 1.

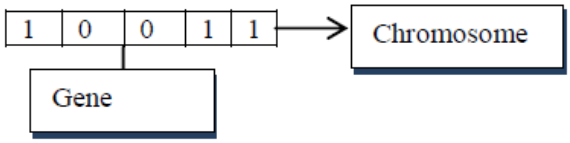


Figure 1: Binary encoding

Creating Initial Population: The initial population can be created with the pool size that is equal to the number of nodes in the network.

Selection: After the initial population is generated, selection of the best fit data is calculated based on the objective function with the weighing parameters. The selection can be based on roulette wheel selection, linear rank selection or tournament selection. The best fit individual is selected based on the weighing parameters such as mobility, distance, energy, transmission range, speed limit and the geographic location. The probability P that a string is selected which contains the bit pattern H is [17]:

$$P = \frac{f(H_1)}{Nf_\mu} + \frac{f(H_2)}{Nf_\mu} + \cdots + \frac{f(H_k)}{Nf_\mu}$$

where $H_1, H_2, \ldots, H_k$ represent all strings of the generation which contain the bit pattern H. If there are no such strings, then P is zero.

Crossover: Crossover techniques can be used to produce new offsprings. Single-point, multi-point, N-point crossover, uniform crossover, shuffle crossover, precedence preservative crossover are some of the types of crossover techniques.Precedance preservative crossover can be used for routing in nodes. This crossover operation has deletion-append scheme.

Mutation: The mutation technique involves inverting the value of each gene with a small probability. Flipping, interchanging, reversing can be chosen for mutation. The splitting and merging operations in mutation may move objects from one zone to another zone. If mutation probability is 100% whole chromosome is changed. Mutation interchanging may help to manage the Zone head with its neighbors. According to the mutation probability, one random gene of a chromosome is replaced by a better node if available, otherwise replaced by a random node.

Elitism: The idea behind Elitism is to update the current solution with the new solution if and only if the new solution is better than previous one.

Fitness Value for Chromosome: In our proposed protocol the initial population is randomly generated and fitness of the path is calculated using the following equation:

$$FitnessF : (Path) = \frac{1}{\sum_{i=1}^{N-1} C(P_i, P_{i+1})}$$

$$\text{F}= \begin{cases} 1 & F \geq Threshold \\ 0 & otherwise \end{cases}$$

The fitness of the path is calculated and the best guess value is calculated. If the Path P is from $s \rightarrow i \rightarrow j \cdots \rightarrow t \cdots \rightarrow d$ then path $= \{(s,i),(i,j),(j,k),\ldots(t,d)\}$.

Since the Link metric is discovered in Neighbor discovery the corresponding Node id will be registered. The population is ranked based on the fitness value and the best individual is being found for Zone head. The best node will be guessed randomly using MANETIC Algorithm and from the best guess the population is carried out for further optimizing. The fitness value is calculated and the population is ranked using the fitness values. The generations are created using best fit values. The fitness values are evaluated using the minimum and maximum threshold (see Algorithm 1).

3.6 Member Registration with User ID and Password

The Zone members will have already participated in the MANET Algorithm and their ranking is evaluated. In Intra routing the zone head will have the knowledge of all the members in its zone. Every member will be registered with user ID and password. The User ID and Password is a secured technique in cryptographic point of view. The generated username and password are encrypted and converted. It is then trained using Neural Network learning technique and assigning a weight function. The algorithm is as follows (Table 4 shows the symbols of the algorithm).

1) User selects ID (ID_r) and password (PW_r);
2) Compute the encrypted password $E(PW_r)$;

Algorithm 1 Zone Head Election Using MANET Algorithm

Begin
Initialize: The Source and Destination points
Generate: Randomly the initial population using via nodes in each path
while NOT (convergence condition) **do**
{
Evaluate the fitness for each path in current Population using following equation:

$$FitnessF : (Path) = \frac{1}{\sum_{i=1}^{N-1} C(P_i, P_{i+1})}$$

if (F(Path) > 0) **then**
Feasible path
else
not Feasible path.
end if
Rank the population using the fitness values
Eliminate the lowest fitness path
Duplicate the highest fitness path
Apply randomly validation process between current Parents using the given probability, while keeping the start and end nodes without change in the population
if (failure in path detected) **then**
Apply the mutation process with the given probability
Generate the new population
else
Continue in Same Path
end if
end while
Output the best individual found
End

3) Convert the ID (ID_r) and encrypted password $E(PW_r)$ to p-bit binary number B_r;

4) Apply Reed-Solomon coding algorithm to convert the (B_r) to N-bit binary number $U_r(n \geq 2p)$;

5) Train the nodes in NN by using the computed N- bit binary number U_r by weight update as follows.
$y_j(t+1) = H[\sum_{i=1}^{n} W_{ij} y_j(t)](1 \leq j \leq N)$

6) Update NN NN_{output};

7) If $(NN_output = U_r)$
Accept the new password
Else
Go to Step 8

8) User provide the ID (ID_k) and password (PW_k)

9) Perform encryption, conversion and NN training (U_k)

10) Retrieve the weights from the Step 5

11) Input the (U_k) to NN with retrieved weight
//Log-in Authentication

12) If $(HNN_{output}) = U_k$
Authorize the user with new password
Else
Reject the user

13) Recall the pairs (ID_r, PW_r) and repeat from Step 1

Table 4: Symbols and descriptions

Symbols	Descriptions
(ID_r)	Registration ID
(PW_r)	Registration Password
$E(PW_r)$	Encrypted Password
(B_r)	p-bit Binary Number
U_r	N-bit binary number
H	Hash function
NN	Neural Network
NN_{output}	Neural Network output
(ID_k)	Registration ID with key
(PW_k)	Password with key

3.7 Reed Solomon Coding

Reed Solomon coding will help to reduce the probability of occurrence of the error. Since it is also known as BCH code, possible number of bit errors can be detected. The (PW_r) is converted to $E(PW_r)$ and concatenated as $(ID_r) + E(PW_r)$ to (B_r).

3.8 Key Sharing and Node Learning Using Neural Network

HMAC, a type of MAC which involves the combination of a cryptographic hash function and a secret key is used. It is used for checking the integrity and certification of the data packet. The HMAC is dependent on the cryptographic potential value of the hash function, key size we have determined and the quality and output of the hash function. The HMAC is defined as

$$HMAC(U_r, pac) = H(k \oplus out \;||\; H((k \oplus IN))|| \; pac).$$

In the above equation 'H' represents the cryptographic hash function, 'pac' represents the packet in queue to be verified, 'K' is the secret key, $\oplus$ represents the operator exclusive OR (XOR), and || symbol denotes the concatenation, 'Out'represents the outer padding and 'IN' refers to the inner padding. The packet is received and encryption is invoked. Packet encryption is performed using the HMAC function. Neural Network uses dynamic memory cycles for learning the patterns. The Converted output is

trained using neural network with the weight function to determine the patterns. If the Neural Network output is equal to the new pass word is accepted. Every user is thus allotted with a (ID_k) and (PW_k) Using the Neural Network the training is performed and the weight function is retrieved.

Node Authentication

If the Neural Network output is equal, the user is authorized or else rejected. The Id and password pairs are recalled and the function is repeated for all the nodes authentication.Only the authenticated nodes will participate in the transmission. Thus the cryptographic hash with Hmac and Neural Network training will yield only the authenticated secured Nodes in the transmission.

4 Performance Analysis

This section illustrates the performance Analysis and evaluations of the proposed ZBMRP protocol by comparing it with the existing techniques such as GACA and EWCA techniques based on Clustering.

GACA: It uses the Genetic Annealing method for Energy aware and topology management in Weighted Clustering Algorithm.

EWCA: This method extends the Weighted clustering Algorithm for load balancing and stability of the network.

Cluster Reaffiliation: Cluster reaffiliation factor (CRF) is defined in [2] as follows:

$$CRF = \frac{1}{2}\sum |N_{i_1} - N_{i_2}|$$

where i represents the average cluster numbers and N_{i_1} and N_{i_2} represents the degree of nodes. If the Zone Head is 8 and it has 6 neighbors, then N=6 and so on. As the nodes are moving the degrees may vary. If CRF is equal to one, then it is assumed that if one node in a particular Zone moves into another Zone, then one reaffiliation occurs. So we can conclude that only if the speed of the nodes increases the reaffiliation occurs often. If we consider a disaster recovery model, we expect that within the specific radius the nodes mobility will not increase too much and minimizes the reaffiliation.

Transmission Range: If the transmission range is high, the average members in a zone will decrease. The number of nodes N will depend on the short range and long range and is defined as

$$N = \sum_{u \in V, u \neq v \{D_{uv} < T_x, TR\}}$$

where D represents the Distance, TR represents the Transmission range. Since we have specified the radius, if it is a disaster scenario we can predict the incident location's transmission range priorly.

Load Balancing Factor: The definition for Load Balancing factor is given as:

$$LBF = \frac{n_c}{\sum (x_i - \mu)^2} \quad \text{where} \quad \mu = \frac{N - n_c}{n_c}$$

Where N represents the Number of Nodes. n_c is the average number of clusters. If N= 50 and $n_c = 7$ then $\mu = (50-7)/7 = 6$. We can conclude that the load is more or less equally balanced as the Load balancing factor is approximately equal to the average number of clusters.

Packet Delivery Ratio: The number of packets actually delivered to the destination to the total number of packets originated is defined as Packet delivery ratio. The location information of the nodes will yield high packet delivery ratio (see Figure 2 and Table 5).

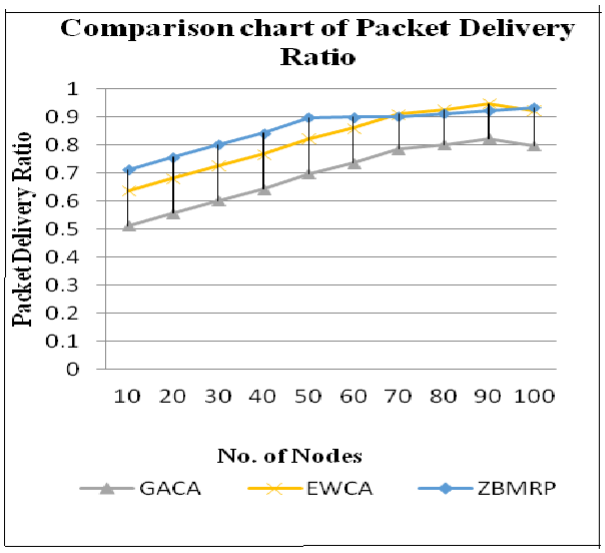


Figure 2: Packet delivery ratio plot of the proposed ZBMRP with the existing GACA and EWCA

Table 5: Comparative analysis of packet delivery ratio of ZBMRP protocol with existing GACA and EWCA

No of Nodes	GACA	EWCA	ZBMRP
10	0.512	0.637	0.712
20	0.556	0.681	0.756
30	0.601	0.726	0.801
40	0.642	0.767	0.842
50	0.698	0.823	0.898
60	0.735	0.86	0.899
70	0.785	0.91	0.901
80	0.801	0.926	0.911
90	0.822	0.947	0.922
100	0.798	0.923	0.932

Average number of cluster members (M): M is defined as $M = \odot(1)$ because all clusters should have

a maximum size constrain to avoid overburdening cluster heads [7]. In this proposed protocol the average number of clusters did not exceed the average highest value depending on the number of nodes (see Figure 3 and Table 6).

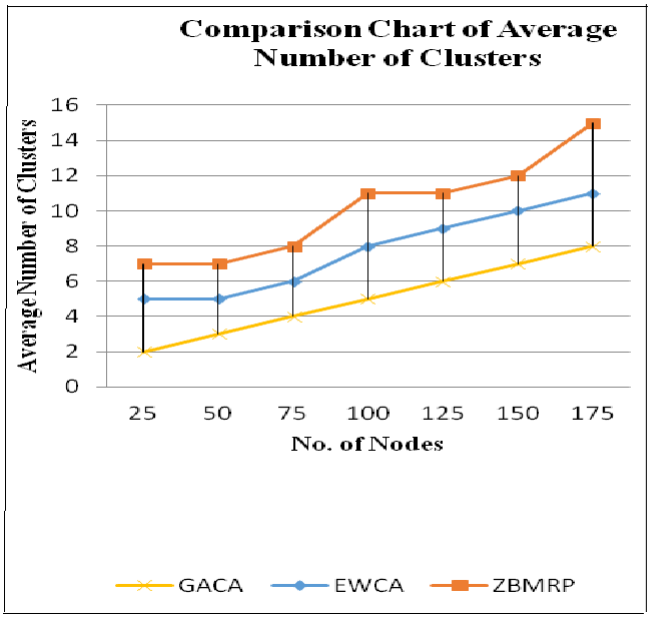


Figure 3: Average number of clusters plot of the proposed ZBMRP with the existing GACA and EWCA

Table 6: Comparative analysis of average number of clusters of ZBMRP protocol with GACA and EWCA

No of Nodes	GACA	EWCA	ZBMRP
25	2	5	7
50	3	5	7
75	4	6	8
100	5	8	11
125	6	9	11
150	7	10	12
175	8	11	15

End to End delay: It is determined by the time lapse between the source and destination nodes and it increases if the location information of all the nodes are obtained (see Figure 4 and Table 7).

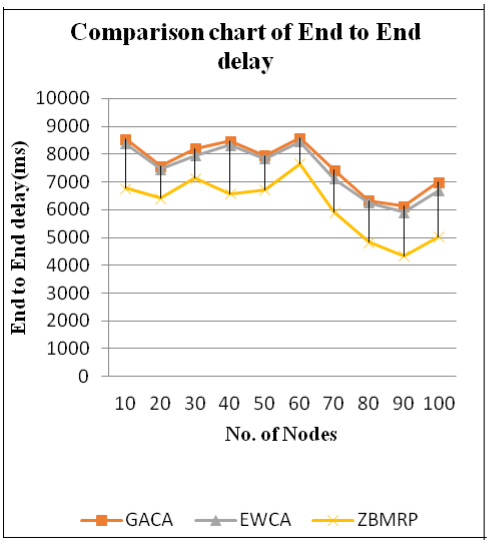


Figure 4: End to end delay plot of the proposed ZBMRP with the existing GACA and EWCA

Table 7: Comparative analysis of end to end delay of ZBMRP protocol with GACA and EWCA

No of Nodes	GACA	EWCA	ZBMRP
10	8546	8373	6776
20	7562	7464	6423
30	8201	7954	7145
40	8475	8328	6574
50	7954	7834	6715
60	8582	8449	7659
70	7421	7121	5904
80	6325	6258	4827
90	6124	5916	4340
100	6985	6693	5021

Throughput: Throughput is measured in megabytes per second. Throughput is defined as the amount of successful transmission of data over the network (see Figure 5 and Table 8).

5 Conclusion

This section presents the conclusion and future scope of the proposed work. A novel ZBMRP protocol with effective leader election based on fitness path and secured architecture using Neural Network is presented in this paper. Initially, the parameters are analysed and Zone radius is determined. The fitness path is calculated. The nodes are ranked and the best leader is elected Node authentication is verified effectively and the proposed protocol will be adaptable for all the situations. The proposed ZBMRP protocol is compared with existing clus-

tering techniques GACA and EWCA and the results are analysed and ensures that the performance yields better results. In future, the security performance of the protocol based on different types of attacks will be analysed.

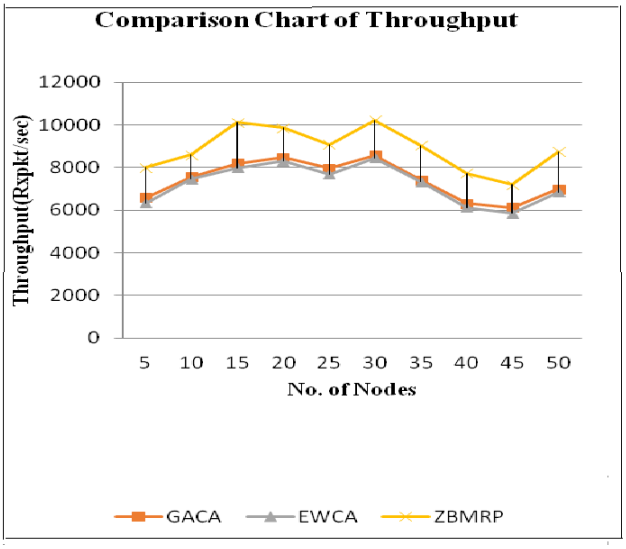


Figure 5: Throughput plot of the proposed ZBMRP with the existing GACA and EWCA

Table 8: Comparative analysis of throughput of ZBMRP protocol with existing GACA and EWCA

Simulation times(ms)	GACA	EWCA	ZBMRP
5	6582	6348	8004
10	7562	7450	8594
15	8201	7977	10126
20	8475	8305	9864
25	7954	7683	9074
30	8582	8459	10232
35	7421	7323	9048
40	6325	6129	7738
45	6124	5842	7203
50	6985	6836	8755

References

[1] E. Alba, B. Dorronsoro, F. Luna, A. J. Nebro, P. Bouvry, L. Hogie, "A cellular multi-objective genetic algorithm for optimal broadcasting strategy in metropolitan MANETs," *Computer Communications*, vol. 30, no. 4, pp. 685–697, 2007.

[2] M. Chatterjee, S. K. Das and D. Turgut, "WCA: Weighted clustering algorithm for mobile adhoc networks," *Cluster Computing*, vol. 5, no. 2, pp. 193–204, 2002.

[3] B. A. Correa, L. Ospina, R. C. Hincapie, "Survey of clustering techniques for mobile ad hoc networks," *Revista Facultad de Ingenieria Universidad de Antioquia*, no. 41, pp. 145–161, 2007.

[4] S. Feng and A. H. Tan, "Self-organizing neural networks for behavior modeling in games," in *IEEE World Congress on Computational Intelligence*, pp. 1–8, 2010.

[5] S. Gangwar, K. Kumar, M. Mittal, "Cluster head selection in mobile adhoc network using ART1 neural network," *African Journal of Computing & ICT*, vol. 8, no. 1, pp. 191–204, 2015.

[6] M. H. Gavgani, M. Abedi, F. Karimi, M. Reza, "Demand response-based voltage security improvement using artificial neural networks and sensitivity analysis," in *IEEE Smart Grid Conference (SGC'14)*, pp. 1–6, 2014.

[7] A. Hussein, S. Yousef, and O. Arabiyat, "A load-balancing and weighted clustering algorithm in mobile ad-hoc networks," in *The 3-rd IT Student Conference for the Next Generation*, University of East London, UK, vol. 8, pp. 21–22, 2009.

[8] W. Jin, S. Lei, J. Cho, Y. Lee, "A load-balancing and energy-aware clustering algorithm in wireless ad-hoc networks," in *IFIP International Federation for Information Processing*, pp. 1108–1117, 2005.

[9] H. Kaaniche and F. Kamoun, "Mobility prediction in wireless ad hoc networks using neural networks," *Journal of Telecommunications*, vol. 2, no. 1, pp. 95–101, 2010.

[10] M. Mehta, I. Rajput, "A survey of clustering approaches for mobile adhoc network," *Compusoft*, vol. 3, no. 2, pp. 507–512, 2014.

[11] V. Preetha, K. Chitra, "Clustering and cluster head selection techniques in mobile adhoc networks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 7, pp. 5151–5157, 2014.

[12] V. Preetha, K. Chitra, "Parameter analysis for clustering in MANET in disaster scenarios," in *7th International Conference on Information Technology (ICIT'15)*, pp. 241–251, 2015.

[13] V. Preetha, K. Chitra, "Prediction of stability of the clusters in MANET using genetic algorithm," in *IEEE International Conference on Advances in Computer Applications (ICACA'16)*, pp. 338–341, 2016.

[14] C. S. Sahin, S. Gundry, E. Urrea, M. UmitUyar, M. Conner, G. Bertoli, C. Pizzo, "Uniform distribution of mobile agents using genetic algorithms for military applications in MANET," in *IEEE Military Communications Conference (MILCOM'08)*, pp. 1–7, 2008.

[15] C. S. Sahin, S. Gundry, E. Urrea, M. UmitUyar, M. Conner, G. Bertoli, C. Pizzo, "Convergence analysis of genetic algorithms for topology control in MANETS," in *IEEE Sarnoff Symposium*, pp. 1–5, 2010.

[16] J. Singha, P. Duttab, A. Palc, "Delay prediction in mobile ad hoc network using artificial neural network," *Procedia Technology*, vol. 4, pp. 201–206, 2012.

[17] D. Turgut, S. K. Das, R. Elmasri and B. Turgut, "Optimizing clustering algorithm in mobile adhoc networks using genetic algorithm approach," in *IEEE Global Telecommunications Conference (GLOBECOM'02)*, vol. 1, pp. 62–66, 2002.

[18] J. Y. Yu, P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Communications and Surveys*, vol. 7, no. 1, pp. 32–47, 2005.

Biography

V. Preetha M. C. A., M. Phil, (Ph,D), Assistant Professor is having 12 years of teaching Experience. She has published many research papers in reputed International Journals and International Conferences. Her research papers have good citation metrics and H-index factor. Her area of Interest is Mobile adhoc Network and Soft computing. She has also obtained best paper award for her research paper in the National level conference.

K. Chitra M. C. A., M. Phil., Ph.D, Assistant Professor is having 16 years of academic experience and 10 years of research experience. She has published more than 60 research papers in reputed International Journals. She is guiding research scholars in the area of Cloud Computing and Mobile Computing. She is ORACLE and IBM certified academician.

Formal Analysis of SDN Authentication Protocol with Mechanized Protocol Verifier in the Symbolic Model

Lili Yao, Jiabing Liu, Dejun Wang, Jing Li and Bo Meng
(Corresponding author: Bo Meng)

School of Computer Science, South-Central University for Nationalities
708 Minzu Ave, Hongshan Qu, Wuhan, Hubei Sheng 430074, China
(Email: mengscuec@gmail.com)
(Received Aug. 21, 2017; revised and accepted Nov. 1 & Oct. 21, 2017)

Abstract

With the wide development and applications of SDN, its security has attracted the attention of the people. In this study, in the beginning we apply applied PI calculus in symbolic model to formalize Mynah authentication protocol and mechanized analyze it with ProVerif. We find that there are two security vulnerabilities. And then, we propose an improved Mynah authentication protocol to address the vulnerabilities found by us. At the same time, the improved Mynah protocol is modeled by applied PI calculus and analyzed with ProVerif. Finally, we develop and deploy the improved Mynah authentication protocol to open source controller ONOS and switch Open vSwitch to validate its securities.

Keywords: Authentication; Formal Method; ProVerif; Security Protocol

1 Introduction

The purpose of introducing SDN is to establish a flexible data access and forwarding method in network and then to deal with the barriers for deploying the new technologies of the network protocols and to decrease cost and to overcome the difficulty of network management, especially provide a good environment for large-scale implementation of cloud computing and virtualization. With the wide development and applications of SDN [15, 16, 18], people have paid a special attention to its security [2, 25]. Owning to that the design and development of most SDN controllers that are the key component in SDN network at first focuses on the schedule and control of network resources and ignoring the security considerations of the controller itself [27]. SDN network is facing enormous security challenges, for example, the lack of trust mechanisms [25, 28]. Kloti and Kotronis [13] use STRIDE tool and Attack Tree to provide a security analysis of OpenFlow-based SDN and find that there are security risks such as information disclosure, denial of service and intervention vulnerabilities in a controller or a channel between the controller and the switch. In order to address the authentication [29], Shin *et al.* [26] present the FRESCO security application development framework in OpenFlow-based SDN. Based on Nox [9] and FRESCO, Porras *et al.* [23] introduce the FortNOX, a software add-on that applies a digital signature to implement the authentication of users. Mattos and Duarte [17] present AuthFlow which is a mechanism for authentication and access control based on host credentials. Dangovas and Kuliesius [7] introduce a SDN-based authentication and access control system to provide strong AAA (authentication, authorization and accounting) schemes.

Recently in order to address the vulnerability of DatapathID (DPID) duplication and provide the authentication between the controller and the switch, Kang *et al.* [12] propose Mynah authentication protocol and claim that it can address the two vulnerabilities. However, security analysis of Mynah protocol is not only not clear, but also DPID duplication problem has not fully been solved found by us. Hence in the study, we present formal analysis and an improved Mynah authentication protocol.

The main contributions of this study are summarized as follows:

1) The state-of-art of security research of SDN network is introduced in detail.

2) Apply applied PI calculus in the symbolic model to formalize Mynah authentication protocol and mechanized analyze it with mechanized tool ProVerif. The result shows that it cannot provide mutual authentication between the controller and the switch and is unable to deal with DPID duplication.

3) Propose an improved Mynah authentication protocol to address the security vulnerabilities found by

us. At the same time, the improved Mynah authentication protocol is modeled by applied PI calculus and mechanized analyzed with ProVerif. The result shows that the improved Mynah authentication protocol resolves DPID duplication and provides confidentiality of data and authentication between the switch and the controller.

4) Develop and deploy the improved Mynah authentication protocol to open source controller ONOS and switch Open vSwitch to validate authentication and confidentiality. The experiment result shows that it can provide confidentiality of data and authentication between the switch and the controller.

2 Related Works

In the beginning of design and development, most SDN controllers [11, 21, 24] focus on the scheduling and control of network resources, ignoring the security considerations of the controller itself [27]. So SDN is facing security challenges, for example, the lack of trust mechanisms [28].

With SDN development and applications, attacks of the controller and the switch significantly increased. Kloti and Kotronis [13] use STRIDE tool and Attact Tree to provide a comprehensive analysis of the security of OpenFlow protocol, whether it is a controller or a channel between the controller and the switch. There are security risks such as information disclosure, denial of service and intervention vulnerabilities. The existing OpenFlow protocol [8, 10, 22, 30] often uses SSL/TLS protocol and does not guarantee the authentication between the controller and the switch [3]. SSL/TLS protocol itself is overloaded and is not good choice to large-scale deployment. In addition, the controller is facing a man-in-the-middle attack, denial of service, bypassing the firewall and other traditional networks already exist security risks [14].

About the authentication [29]. Shin *et al.* [26] present the FRESCO security application development framework in OpenFlow-based SDN. The main function of FRESCO is to provide modular interface and deployment platform to build security services, through the corresponding FRESCO scripting language to define and implement security services, simplifying the development of security applications and complexity of debugging. It facilitates the controller to update and extend security services in the operating mode. Based on Nox [9] and FRESCO [26], Porras *et al.* [23] introduce the FortNOX, a software add-on to improve the flaws in the OpenFlow control plane and to deploy new security modules while using existing security services, each of the flow rules is signed using the role-based data source authentication method and the identity of the user is verified by verifying the signature data to ensure the security of the session. Mattos and Duarte [17] present AuthFlow which is an authentication and access control mechanism based on host credentials. The mechanism uses IEEE 802.1X standard and RADIUS authentication server to authenticate the host above the MAC layer, but AuthFlow has not used the signed certificate as access credentials. Dangovas and Kuliesius [7] introduce an authentication and access control system that binds the name (users, addresses) and user machines to the unambiguously defined network appliances and its ports and register the switch and host information to the controller and authenticate, satisfied strong AAA (authentication, authorization and accounting) schemes.

Recently in order to address the vulnerability of DPID duplication and provide authentication between the controller and the switch, Kang *et al.* [12] propose Mynah authentication protocol and claim that it can address the two vulnerabilities. However, security analysis of Mynah protocol is not only not clear, but also DPID duplication problem has not fully been solved found by us.

3 The Applied PI Calculus & ProVerif

The applied PI calculus [1] is proposed by Abadi *et al.* in 2001, which is a formal language [6, 19] used to formalize the modeling of concurrent processes. Applied PI calculus builds on pure PI calculus [20]. From pure PI calculus, we inherit constructs for communication and concurrency, also add functions and equations. In applied PI calculus, messages may then consist of atomic names or consist of values constructed from names and functions. The advantage of this is that we can easily treat standard data types, reducing the limitation of data representation. The applied PI calculus using functions to represent generic cryptographic primitives, such as encryption, decryption, digital signatures, *etc.* It does not need to construct a new cryptographic primitive for each cryptographic operation with good versatility. We can also describe attacks against protocols that rely on (equational) properties of some of those primitives. Therefore, it can express and analyze fairly sophisticated security protocols.

The grammar for processes of applied PI calculus language is similar to the PI calculus. Process P, Q as the basic unit, the input process is 0 that empty process; $Q|P$ is the parallel composition of P and Q; the replication $!P$ behaves as innumerable copies of P running in parallel. The process $vn.P$ that defines the variable name and $in(M, x : t)$ indicates that it is input in the channel in the process and $out(M, x : t)$ indicates that the process is output in the channel, $if M = N then P else Q$ indicates that the execution process is selected according to the judgment condition, let $x = M$ in P else Q presents the event evaluation, $R(M1, \cdots, Mk)$ represents the macro definition.

ProVerif [5] is a mechanized tool based on the Dolev-Yao model for automated verification of security protocol properties and is developed by Blanchet in 2001. It can be used to analyze and validate security protocols that use Horn clauses or applied PI calculus to model various

cryptographic primitives. Includes shared key cryptography, public key cryptography, digital signature, hash function and Diffie-Hellman key exchange. At the same time, it avoids the problem of the state space explosion. It can analyze and verify the strong confidentiality, authenticity, more general consistency and process of observation equivalent. ProVerif has successfully analyzed a large number of complex security protocols.

4 Mynah Authentication Protocol

4.1 Review

Mynah authentication protocol [12] based on OpenFlow protocol is designed to address the vulnerability of DPID duplication and to provide the authentication security service based on DPID. OpenFlow protocol uses DPID as the identifier of the data plane, but does not provide any means to authenticate DPID of the switch. The messages in Mynah authentication protocol are shown in Figure 1.

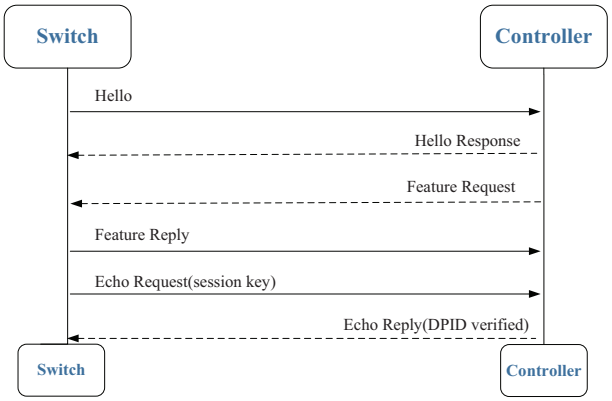


Figure 1: The messages of Mynah authentication protocol

Hello and Hello Response: After the switch and the controller establish a TCP connection, the switch sends a Hello message to the controller and the controller produces the Hello Reponse message to the switch to determine the negotiation on version of OpenFlow protocol used by the communicating parties. Hello message contains the highest version of OpenFlow protocol that the sender can support. The switch and the controller each received a Hello message from each other, compare the highest version supported by other parties with the highest version supported locally and finally the version with the lower version as the final version. If the negotiation process fails, a HELLO FAILED error message is returned to the peer and the connection is terminated.

Feature Request and Feature Reply: After the version of OpenFlow protocol is determined between the communicating parties, the controller sends a Feature Request message to the switch requesting configuration parameters and other related information for the switch. In the SDN network architecture, a controller manages the flow table updates of multiple switches at the same time. Therefore, it is necessary to save the independent information of the switch as an identification flag during the connection establishment process, so as to avoid interfering with the instructions sent. After receiving the Feature Request, the switch sends a Feature Reply message to the controller. Feature Reply message contains actions, DPID-based authentication and *etc.*

Echo Request and Echo Reply: The switch sends the Feature Reply message and indicates that the switch-controller can perform DPID-based authentication. The switch can send its session key in the Echo Request message. The session key depends on DPID, timestamp and transaction serial number. The session key should be encrypted using either asymmetric key algorithms or symmetric key algorithms. The switch encapsulates SessionKey encrypted with a public key into the Echo Request message and sends it to the controller. After the controller receives Echo Request message, it first checks DPID to verify the identity of the switch and then decrypts SessionKey using the corresponding private key. And then the controller checks whether the DPID, timestamp and transaction ID is valid or not. If any of the three parameters is invalid, the controller rejects the connection from the switch. If all information is valid but has a connection with the same DPID, the controller still rejects the connection. Finally, the controller generates a DPID verification message and encapsulates it into the Echo Reply message, which is encrypted with SessionKey and sends it to the switch.

4.2 Formalize Mynah Authentication Protocol Using the Applied PI Calculus

4.2.1 Function and Equational Theory

The functions and equations used in the modeling process are described in this section. This study uses applied PI calculus to formalize Mynah authentication protocol. Figure 2 depicts the Mynah authentication protocol function and equation theory.

The message x is encrypted by function $senc(x, PU)$ with public key PU and message x is decrypted by function $sdec(x, PU)$ with public key PU. The message x is encrypted by function $aenc(x, PU)$ with public key PU and the message x is decrypted with function $adec(x, PR)$ with private key PR. The private value is received by function $PR(y)$ as an input and a private key is generated as an output, at the same time the common value is received as an input through function $PU(y)$ and a public key is generated as an output.

4.2.2 Processes

The whole Mynah authentication protocol process consists of two processes: switch process and controller process. They together constitute the main process, as shown in Figure 3.

$$\begin{array}{l} Funaenc(x, PU). \\ Funadec(x, PR). \\ Funsenc(x, PU). \\ Funsdec(x, PU). \\ FunPU(y). \\ FunPR(y). \\ \\ equationadec(aenc(x, PU(y)), PR(y)) = x. \\ equationsdec(senc(x, PU(y)), PU(y)) = x. \end{array}$$

Figure 2: Function and equational theory

$$\|mainprocess = (processSwitch|processController)\|$$

Figure 3: Main process

$$\begin{array}{l} letprocessSwitch \triangleq \\ newmsgVersionS; newmsgTypeHelloS; newxid1; \\ out(c, (msgVersionS, msgTypeHelloSxid1)); \\ in(c, (= msgVersionCon, = msgType1, = xidRly1)); \\ in(c, (= msgType2, = xidRly2)); \\ newmsgTypeFeaReply; \\ out(c, (msgTypeFeaReply, xidRly2, datapathID)) \\ newtimestamp; newxid3; newmsgTypeEchoReq; \\ letsessionkeyS = getSessionKey \\ (timestamp, xid3, datapathID)in \\ letsecretKey = aenc(sessionkeyS, PU(keyop1)) \\ inout(c, (msgTypeEchoReq, xid3, secretKey)); \\ in(c, = msgType3, = xidRly3, = secretMessage); \\ ifsdec(secretMessage, PR(sessionkeyS)) \\ = OPmessagethenout(c, finished) \end{array}$$

Figure 4: Mynah authentication protocol switch process

The switch process is shown in Figure 4. First, it sends the protocol version number $msgVersionS$ to controller process through public channel c and then receives the protocol version number $msgVersionS$ from controller process through the public channel c for message version negotiation. After the version is determined, switch process receives the configuration information request Feature Request through public channel c, generates the response Feature Reply and sends its own DPID to the controller process through public channel c. After controller process receives the DPID, switch process uses the DPID, timestamp and transaction sequence xid3 to generate the SessionKey and uses asymmetric encryption algorithm to encrypt secretKey and sends it to controller process through public channel c. And then from controller process through open channel c to receive controller encrypted message, the use of existing SessionKey and symmetric decryption algorithm decryption secretMessage, if the decryption is successful to verify the correctness of key, though open channel c output finished, to the end of this protocol communication.

The controller process is shown in Figure 5. It sends the protocol version number $msgVersionS$ to switch process through public channel c and then receives protocol version number $msgVersionS$ of the switch from switch process through public channel c and performs the message version negotiation. This process is similar to the switch process. Once the version is determined, controller process immediately sends Feature Request over public channel c and waits for the Feature Reply of the receiving process. In the received Feature Reply response, the controller process obtains DPID of sender's process and saves it. And then through open channel c to receive the session process SessionKey, using private key $PR(keyop1)$ decryption secertkey get the session key $SessionKeyC$, the session key DPID and previously saved DPID comparison verification. If authentication is successful, the parameter OPmessage is encrypted using $SessionKeyC$ and sent to switch process via open channel c.

$$\begin{array}{l} letprocessController \triangleq \\ newmsgVersionC; newmsgTypeHelloC; \\ newxid4; \\ out(c, (msgVersionC, msgTypeHelloC, xid4)); \\ in(c, (= msgVersionSw, = msgType4, = xidRly4)); \\ newmsgTypeFeaReq, newxid5; \\ out(c, (msgTypeFeaReq, xid5)); \\ in(c, (= msgType5, = xidRly5, = datapathID)); \\ in(c, (= msgType6, = xidRly6, = secretkey)); \\ letsessionkeyC = adec(secretkey, PR(keyop1))in \\ newmsgTypeEchoReply; newflag4; \\ letsecretMessage = senc(OPmessage, \\ PR(sessionkeyC))in \\ newmsgTypeEchoReply, newxidRly6, newflag4; \\ out(c, (msgTypeEchoReply, xidRly6, \\ flag4, secretMessage)) \end{array}$$

Figure 5: Mynah protocol controller process

4.3 Automatic Verification of Authentication and Confidentiality of Mynah Authentication Protocol with ProVerif

Here we use the statements query attack (OPmessage) to verify confidentiality of OPmessage message and then use non-injective agreements to model authentication, Mynah protocol authentication is shown in Table 1.

The ProVerif inputs in Figure 7 are entered into the ProVerif and the analyze outputs are shown in Figure 8 to Figure 10.

Table 1: Authentication

Non-injective agreement	Authentication
ev:endauthcon_sMynah(x)==>ev:beginaauthcon_sMynah(x).	Verify the authentication from the controller to the switch
ev:endauthswit_cMynah(x)==>ev:beginaauthswit_cMynah(x).	Verify the authentication from the switch to the controller

Figure 8 is the result of confidentiality of the message OPmessage. The result is true. According to the specification of Mynah authentication protocol, the switch sends the session key in the Echo Request message. The session key is encrypted using either asymmetric key algorithms. The switch encapsulates SessionKey encrypted with a public key into Echo Request message and sends it to the controller. After the controller receives Echo Request message, it first checks DPID to verify the identity of the switch and then decrypts SessionKey using the corresponding private key. The attacker cannot obtain the private key and hence cannot decrypt the message OPmessage.

$$
\begin{array}{l}
funaenc/2. funadec/2. \\
funsenc/2. funsdec/2. \\
funPU/1. funPR/1. \\
fungetSessionKey/3. \\
\\
equationadec(aenc(x, PU(y)), PR(y)) = x. \\
equationsdec(senc(x, PU(y)), PU(y)) = x.
\end{array}
$$

Figure 6: Functions and equations in ProVerif

$$
\begin{array}{l}
queryattacker : OPmessage. \\
queryev : endauthcon\_sMynah(x) \\
==> ev : beginaauthcon\_sMynah(x). \\
(**ControllerauthenticatesSwitch**) \\
queryev : endauthswit\_cMynah(x) \\
==> ev : beginaauthswit\_cMynah(x). \\
(**SwitchauthenticatesController**) \\
..... \\
eventbeginaauthswit\_cMynah(echoRequest); \\
out(c, echoRequest); ..... \\
in(c, echoReply); \\
eventendauthcon\_sMynah(echoReply); \\
..... \\
in(c, echoRequest); \\
eventendauthswit\_cMynah(echoRequest); \\
..... \\
eventbeginaauthcon\_sMynah(echoReply); \\
out(c, echoReply).
\end{array}
$$

Figure 7: Mynah authentication protocol in ProVerif

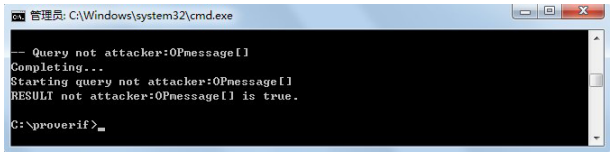


Figure 8: OPmessage confidentiality

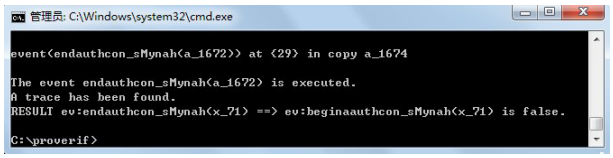


Figure 9: The analysis result of authentication from the controller to the switch

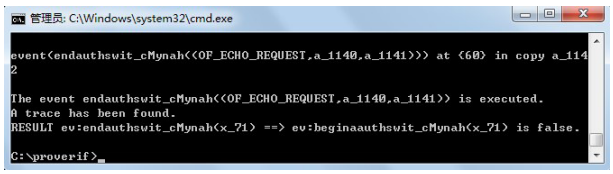


Figure 10: The analysis result of authentication from the switch to the controller

Figure 9 presents the result of *ev: endauthcon_sMynah(x) ==> ev: beginaauthcon_sMynah(x).* Figure 10 shows the result of *ev: endauthswit_cMynah(x) ==> ev: beginaauthswit_cMynah(x).* The results are false and show that the switch and the controller cannot authenticate each other. According to the specification of Mynah authentication protocol, there has no authentication mechanism between switch and controller.

About DPID duplication, owning to that the DPID is not classified, the attacker can get the DPID and then use the DPID to launch the communication early. According to the specification of Mynah authentication protocol, the attacker generates the Echo Request message and sends it to the controller. The controller checks whether the DPID, timestamp and transaction ID is valid or not. If any of the three parameters is invalid, the controller rejects the connection from the switch. If all information is valid but has a connection with the same DPID, the controller still rejects the connection. Because the DPID is

fresh and not is used, the controller generates a DPID verification message and encapsulates it into the Echo Reply message and sends it to the switch. So Mynah authentication protocol cannot prevent DPID duplication.

5 Improved Mynah Authentication Protocol

5.1 The Design of Improved Mynah Authentication Protocol

Improved Mynah automation protocol framework is shown in Figure 11. Firstly, there is a version negotiation between the switch and the controller. If it is successful, the controller gets switch configuration information, otherwise ends the conversation. Second, after the switch configuration information is obtained, the controller initiates the authentication request and then if the authentication request succeeds, the switch generates a session key. At the same time the digital signature mechanism is introduced to implement the authentication between the switch and the controller. If the request fails, terminate session. Finally, if authentication is successful, session key is used to encrypt the follow-up message. Otherwise, the session is terminated.

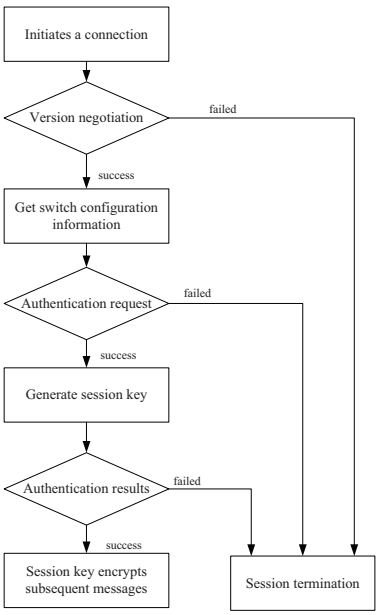


Figure 11: Improved Mynah authentication protocol framework

The improved Mynah authentication protocol introduces a digital signature to implement authentication between the switch and the controller, confidentiality of data and to prevent DPID duplication.

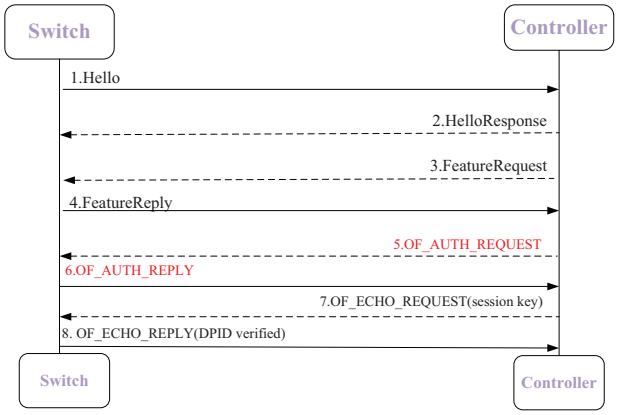


Figure 12: Improved Mynah authentication protocol messages

The improved Mynah message structures are shown in Figure 12. After the controller obtains DPID of the switch, it needs to verify the identity of the switch. The controller initiates an authentication request and uses a digital signature to generate a message digest for protocol type, event sequence number and DPID in the OF_AUTH_REQUEST message and encapsulates it into OF_AUTH_REQUEST message and then sends it to the switch. After receiving OF_AUTH_REQUEST message, the switch verifies the digital signature using public key of the controller. And then it generates a session key, encrypts the key using an asymmetric encryption algorithm, calculates the digital signature and encapsulates it in OF_AUTH_REPLY message to the controller. The controller verifies after receiving OF_AUTH_REPLY message. Finally, the controller encrypts subsequent communication message entries using the obtained session key.

1) The controller and the switch still need to complete version negotiation process. The controller obtains configuration information about the switch.

2) After obtaining DPID of the switch, the controller initiates the authentication request.

3) The controller uses its own private key to generate a digital signature for OF_AUTH_REQUEST message and appends the digital signature to message OF_AUTH_REQUEST as a whole message to switch. The switch verifies the digital signature through public key of the controller after receiving OF_AUTH_REQUEST message, verifies whether the initiator of request is indeed controller and then the switch generates session key and uses symmetric encryption algorithm to encrypt the session key, generates a digital signature of OF_AUTH_REPLY message using its own private key and sends it to the controller. After receiving OF_AUTH_REPLY message, the controller verifies the digital signature using the public key of the switch. If the verification of the digital signature is successful, the controller

Table 2: Improved Mynah authentication protocol message structures

Description of the improved Mynah authentication protocol field		
Message item	Field Name	Description
OF_AUTH_REQUEST	Header	Message head, Type=OFPT_AUTH_REQUEST
	DPID	Create a data plane identifier for the connected switch
	SignedMessage	Digital signature, authentication controller identity
OF_AUTH_REPLY	Header	Message head, Type=OFPT_AUTH_REPLY
	SecretKey	The encrypted session key
	SignedMessage	Digital signature, authentication switch identity
OF_ECHO_REQUEST	Header	Message head, Type=OFPT_ECHO_REQUEST
	SecretMessage	Encrypted message
OF_ECHO_REPLY	Header	Message head, Type=OFPT_ECHO_REPLY
	Flag	Verify that the authentication result is TRUE

obtains the session key sent by the switch using symmetric decryption algorithm. Otherwise the protocol is ended.

4) After the controller obtains the session key generated by the switch, the session key is used to encrypt data. And then the controller encapsulates it into OF_AUTH_REQUEST message and sends it to the switch. When the switch received OF_AUTH_REQUEST message, it uses the session key to decrypt it. Finally, the switch generates OF_ECHO_REPLY message and sends it to the controller.

OF_AUTH_REQUEST message is generated by the controller, which contains DPID of the switch and the digital signature generated by the controller using the private key. OF_AUTH_REPLY message is generated by the switch, which contains encrypted session key and the digital signature generated by the switch using the private key. The message fields and descriptions are shown in Table 2.

5.2 Formalize Improved Mynah Authentication Protocol Using the Applied PI Calculus

The function and the equation theory are shown in Figure 13 in formal model of the improved Mynah authentication protocol. The message x is digitally signed by function $sign(x, PR)$ with private key PR and the correctness of message x signature is verified by function $versign(x, PU)$ with public key PU. The message x is encrypted by function $senc(x, PU)$ with public key PU and message x is decrypted by function $sdec(x, PU)$ with public key PU. The message x is encrypted by function $aenc(x, PU)$ with public key PU and the message x is decrypted with function $adec(x, PR)$ with private key PR. The private value is received by function $PR(y)$ as an input and a private key is generated as an output and the common value is received as an input through function $PU(y)$ as an input and a public key is generated as an output.

$$
\begin{array}{l}
Funaenc(x, PU). \\
Funadec(x, PR). \\
Funsenc(x, PU).Funsdec(x, PU). \\
Funsign(x, PR).Funversign(x, PU). \\
FunPU(y).FunPR(y). \\
\\
equationadec(aenc(x, PU(y)), PR(y)) = x. \\
equationsdec(senc(x, PU(y)), PU(y)) = x. \\
equationversign(sign(x, PR(y)), PU(y)) = x.
\end{array}
$$

Figure 13: Improved Mynah authentication protocol function and equality theory

The switch process is shown in Figure 14. In the first part, the switch first completes the version negotiation and the FeatureReply response through public channel c, sends the relevant configuration information to the controller process and then switch process receives authentication request OF_AUTH_REQUEST through public channel c and then uses controller public key $PU(keyrp1)$ and function $versign(x, PU)$ to confirm the digital signature. If the verification result verifies the authenticity of signature, the session key is generated by DPID, timestamp and transaction sequence xid3 and the session key is encrypted using asymmetric encryption function $aenc(x, PU)$. Finally, switch private key $PR(keyrp2)$ and function $sign(x, PR)$ to sign above parameters and sends them to the controller process via open channel c. The second part, through public channel c from controller process to receive secretMessage, using the existing SessionKey and symmetric decryption algorithm $sdec(x, PU)$ to decrypt secretMessage. If the decryption is successful, the flag of OF_ECHO_REPLY message is set to true and then through public channel c sends the message to controller and the protocol communication ends.

The controller process is shown in Figure 15. First, it completes the version negotiation and message featureRequest to the switch process through open channel c and then obtains DPID of the switch. Second, use controller private key $PR(keyrp1)$ and function $sign(x, PR)$ to generate a digital signature and en-

capsulate it into the OF_AUTH_REQUEST message to send the authentication request through public channel c. Then the controller process receives the authentication response message OF_AUTH_REPLY through public channel c, it uses switch public key $PU(keyrp2)$ and function $versign(x, PU)$ to confirm the digital signature. If the verification result confirms the authenticity of signature, the function $adec(x, PU)$ decrypts the SessionKey and encrypts the OPmessage with session key, encapsulating it into the OF_ECHO_REQUEST message and sending it to the switch process through public channel c.

$$
\begin{array}{l}
\text{letprocessSwitch} \triangleq \\
newmsgVersionS; \\
newmsgTypeHelloS; newxid1; \\
out(c, (msgVersionS, msgTypeHelloS, xid1)); \\
in(c, (= msgType3, = xidRly3, \\
= datapathID, = SignedMessageC2S)); \\
ifversign(SignedMessageC2S, PU(keyrp1), \\
(msgType3, xidRly3, datapathID)) \\
= truethennewtimestamp; \\
newmsgTypeAuthReply; \\
letsessionkeyS = getSessionKey \\
(timestamp, xidRly3, datapathID) \\
inletsecretKey = aenc(sessionkeyS, \\
PU(keyop1))in \\
letSignedS2C = sign \\
((msgTypeAuthReply, xidRly3, secretKey), \\
PR(keyrp2))in \\
out(c, (msgTypeAuthReply, xidRly3, \\
secretKey, SignedS2C));
\end{array}
$$

Figure 14: The switch process

$$
\begin{array}{l}
letprocessController \triangleq \\
newmsgVersionS; \\
newmsgTypeHelloS; newxid1; \\
out(c, (msgVersionS, msgTypeHelloS, xid1)); \\
letSignedC2S = \\
sign((msgTypeAuthReq, xid7, datapathID), \\
PR(keyrp1))in \\
out(c, (msgTypeAuthReq, xid7, \\
datapathID2, SignedC2S, SignedC2S); \\
in(c, (= msgType7, = xidRly7, \\
= secretKey, = SignedMessage)); \\
ifversign(SignedMessageS2C, PU(keyrp2), \\
(msgType7, xidRly7, secretKey)) = true \\
thennewmsgTypeEchoReq; newxid8; \\
letsessionkeyC = \\
adec(secretKey1, PR(keyop1))in \\
letsecretMessage = \\
senc(OPmessage, PR(sessionkeyC))in \\
out(c, (msgTypeEchoReq, xid8, secretMessage));
\end{array}
$$

Figure 15: The controller process

$$
\begin{array}{l}
funaenc/2. \\
funadec/2. \\
funsdec/2. \\
funsenc/2. \\
funsign/2. \\
funversign/2. \\
funPU/1. \\
funPR/1. \\
\\
equationadec(aenc(x, PU(y)), PR(y)) = x. \\
equationsdec(senc(x, PU(y)), PU(y)) = x. \\
equationversign(sign(x, PR(y)), PU(y)) = x.
\end{array}
$$

Figure 16: Functions and equations in ProVerif

$$
\begin{array}{l}
queryattacker : OPmessage. \\
queryev : endauthcon\_s(x) \\
==> ev : beginaauthcon\_s(x). \\
queryev : endauthswit\_c(x) \\
==> ev : beginaauthswit\_c(x). \\
.....in(c, authRequest); \\
ifversign(SignedMessageC2S, PU(keyrp1)) = \\
(msgType3, xidRly3, datapathID1)then \\
eventendauthcon\_s(SignedMessageC2S); \\
.....eventbeginaauthswit\_c(SignedS2C); \\
out(c, authReply); \\
.....eventbeginaauthcon\_s(SignedS2C); \\
out(c, authRequest); \\
.....in(c, authReply); if \\
versign(SignedMessageS2C, PU(keyrp2)) = \\
(msgType7, xidRly7, secretKey1)then \\
eventendauthswit\_c(SignedMessageS2C);
\end{array}
$$

Figure 17: Improved Mynah authentication protocol in ProVerif

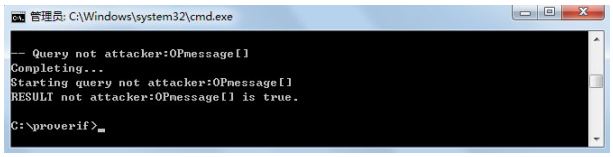


Figure 18: Confidentiality of OPmessage

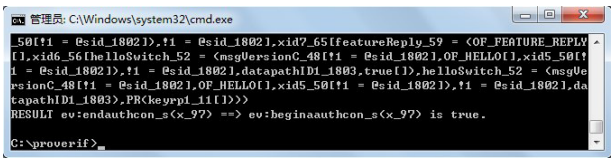


Figure 19: The analysis result of the authentication from the controller to the switch

Table 3: Authentication

Non-injective agreement	Authentication
ev:endauthcon_s(x)==>ev:beginaauthcon_s(x).	Verify the authentication from the controller to the switch
ev:endauthswit_c(x)==¿>ev:beginaauthswit_c(x).	Verify the authentication from the switch to the controller

Figure 20: The analysis result of the authentication from the switch to the controller

5.3 Automatic Verification of Authentication and Confidentiality of Improved Mynah Authentication Protocol with ProVerif

After the formal model of the improved Mynah authentication protocol was generated, ProVerif is used to perform the formal analysis. First the target that needs to be proved is defined and then the analysis with ProVerif is implemented. The authentication of the improved Mynah authentication protocol is shown in Table 3. This process is similar to the verification process of Mynah authentication protocol.

ProVerif scripts in Figure 17 are as input to ProVerif and the outputs of analysis are shown in Figure 18 to Figure 20.

Figure 18 shows the result of the formalize analysis of confidentiality of OPmessage and the result is true, it proved that the improved Mynah authentication protocol provides confidentiality of OPmessage.

Figure 19 shows the result of $ev : endauthcon\_s(x) ==> ev : beginaauthcon\_s(x)$. Figure 20 is the result of $ev : endauthswit\_c(x) ==> ev : beginaauthswit\_c(x)$.The two results are true and indicate that the switch and the controller can authenticate each other.

In the improved Mynah authentication protocol, because digital signature mechanism is adopted, the switch uses the private key to sign the message when sending the message OF_AUTH_REPLY. After receiving OF_AUTH_REPLY message, the controller needs to verify the digital signature using the public key of the switch, to ensure the authentication for the switch and integrity of the message OF_AUTH_REPLY. Similarly, the controller uses the digital signature for the message OF_ECHO_REQUEST, the switch receives the OF_ECHO_REQUEST and uses the controller's public key to verify the digital signature to ensure the authentication for the controller and the integrity of the message OF_ECHO_REQUEST.

About DPID duplication, according to the specification of the improved Mynah authentication protocol, the attacker cannot generate the digital signature for message OF_ECHO_REQUEST because the private key of controller is secret. At the same time the attacker also cannot produce the digital signature for OF_AUTH_REPLY because the private key of the switch is secret. So the improved Mynah authentication protocol can prevent DPID duplication.

6 Develop and Deploy the Improved Mynah Authentication Protocol

The improved Mynah authentication protocol was developed and deployed to open source controller ONOS [4] and switch Open vSwitch to validate its security. The improved Mynah authentication protocol program consists of the controller side developed with Java language and the switch side developed with C language. The improved Mynah authentication protocol program is deployed to the controller ONOS and the switch Open vSwitch and be recompiled. The improved Mynah authentication protocol development architecture is illustrated in Figure 21.

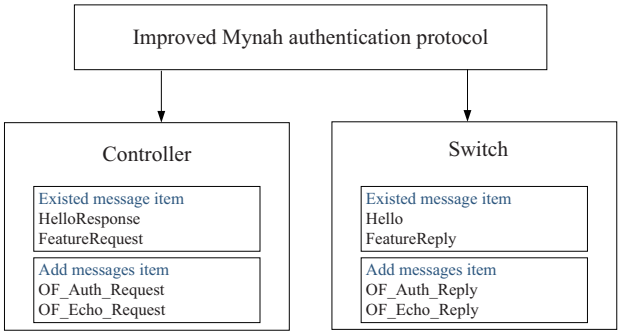


Figure 21: Improved Mynah authentication protocol development architecture

Running environment is composed of the hardware environment and the software environment. The hardware environment is for Intel Dore dual-core CPU, memory 2GB. The software environment is for the operating system for Ubuntu 14.0.1, the controller ONOS version 1.3, the switch Open vSwitch version 1.0, the virtual network simulation platform Mininet version 1.0, Apache Karaf version 3.0.2.

6.1 ONOS Controller Side Development

In the ONOS platform, the controller and the switch connection consist of three steps. The controller starts listening to port 6633, the switch launches the connection with controller, the controller and the switch make negotiation on version and the message transmission.

The main class in ONOS controller side is the OpenFlowControllerImpl class that implements the OpenFlowController interface. During the initialization of OpenFlowControllerImpl class, the controller object Controller class and OpenFlowSwitchAgent class are instantiated at first to monitor the state of the switch that has established the connection. And then it calls the Controller.start(OpenFlowAgent agent) method for parameter configuration and starts the server side, listens port, waits for the switch to establish a connection.

After the connection is established between the controller and the switch, the controller generates OFChannelHandler object and listens for the messages sent by the switch. After receiving the message sent by the switch, the controller first analyzes the type of message and performs different method calls according to the message type. When the message type is Feature_Reply, the controller should send the authentication request message OF_Auth_Request. When the message type is Auth_Reply, the controller should send the OF_Echo_Request message.

In ONOS design mode, the OFMessage interface is defined, which contains all the data items and operations in an OpenFlow message. Its subinterfaces are also defined for behavior and data items according to the explicitly defined message items in OpenFlow protocol specification. The implementation class developed by us process the data according to the method defined by the parent interface and the specific version information. The data that need to transmit between the controller and the switch is encapsulated into the instantiated object and communicates through the ChannelPipeline pipeline in ONOS platform. The protocol message structure is shown in Figure 22.

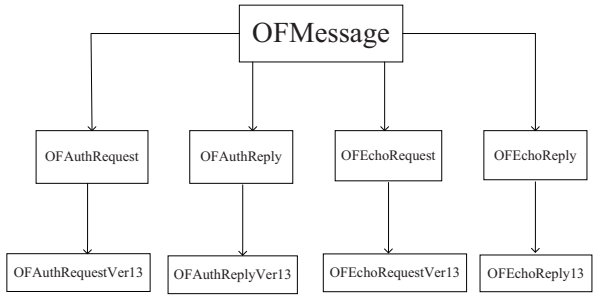


Figure 22: ONOS message structure

Because each message has a separate implementation class, the ONOS controller side need to check Type and Version of the message received and then find the corresponding implementation classes according to the Type and Version for message encapsulation, encryption, decryption and authentication *etc.* ONOS controller has implemented the implementation classes of HelloResponse message and FeatureRequest message, so we focus on the implementation classes and deployments of OF_Auth_Request message and OF_Echo_Request message.

When the controller sends an authentication request, it first needs to obtain parameters such as version number, Xid and DPID. Then the digital signature is generated for the DPID as part of the OF_Auth_Request message and sent to the switch. When the controller receives the OF_Auth_Reply message, it is also necessary to verify the digital signature using the public key. If the verification succeeds, the authentication from the controller to the switch is true. If the verification fails, the controller terminates the session and releases the connection. At this time the controller saves the DPID in its own database. If the attacker wants to use the same DPID to establish connection, then the controller needs to query database. The results show that there is a duplicate DPID, then the controller refused connection.

6.2 Open vSwitch Switch Side Development

When the switch receives the OpenFlow message, it also needs to perform the action according to the message type. When the message type is Auth_Request, the switch should send the OF_Auth_Reply message. When the message type is Echo_Request, the switch should send the OF_Echo_Reply message.

After receiving the OF_Auth_Request message, the switch first verifies the digital signature using the public key of the controller. If the verification succeeds, the authentication from the controller to switch is true. The switch then generates the session key and encrypts the session key and generates the digital signature as a field of the OF_Auth_Reply message sent to the controller. After receiving the OF_Auth_Reply message, the controller verifies the digital signature using the public key of the switch. If the verification is successful, the controller obtains the session key and can use it to encrypt the follow-up message to the switch. At the same time, the switch uses the session key to decrypt the message.

6.3 Results and Analysis

After the deployment of the improved Mynah authentication protocol program, we find that when DPID of the switch changes, the controller terminates and releases the connection, restarts the new session request by the switch and completes the authentication process again. Otherwise, the controller remains in listening state. When the digital signature verification fails, the controller or switch

also to terminate the session process. That is consistent with the results of the formal analysis with ProVerif.

7 Conclusion

With the rapid development and applications of SDN network, people have paid a special attention to its security. Recently Kang *et al.* propose an authentication protocol called Mynah authentication protocol and claim that it can address the vulnerability of DPID duplication and provide the authentication between the controller and the switch in OpenFlow-based SDN network. Owning to security analysis of Mynah authentication protocol is not clear, in this study we apply applied PI calculus in symbolic model to formalize Mynah authentication protocol and mechanized analyze it with mechanized tool ProVerif. We find that it does not provide mutual authentication between the controller and the switch. At the same time, Mynah authentication protocol can't prevent DPID duplication. Hence we propose an improved Mynah authentication protocol to address the vulnerabilities found by us. At the same time, the improved Mynah authentication protocol is modeled by applied PI calculus and mechanized analyzed with ProVerif. The results show that the improved Mynah authentication protocol can prevent DPID duplication and provide confidentiality of data and authentication between the switch and the controller. Finally, we develop and deploy the improved Mynah authentication protocol to open source controller ONOS and switch Open vSwitch to validate authentication and confidentiality. The experimental results show that it can provide confidentiality of data and authentication between the switch and the controller. In the near future, we will use the proof assistant Coq to prove the correctness of the improved Mynah authentication protocol implementation.

Acknowledgments

This study was supported in part by the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities No.CZZ18003 and by the natural science foundation of Hubei Province under the grants No. 2014CFB249.

References

[1] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," in *Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pp. 104–115, Mar. 2001.

[2] M. Azrour, Y. Farhaoui, and M. Ouanan, "A new secure authentication and key exchange protocol for session initiation protocol using smart card," *International Journal of Network Security*, vol. 19, no. 6, pp. 870–879, 2017.

[3] K. Benton, L. J. Camp, and C. Small, "OpenFlow vulnerability assessment," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 151–152, Aug. 2013.

[4] P. Berde, M. Gerola, J. Hart, Y. Higuchi, and M. Kobayashi, "ONOS: Towards an open, distributed SDN OS," in *Proceedings of the third workshop on Hot topics in software defined networking*, pp. 1–6, Aug. 2014.

[5] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in *Proceeding of the 14th IEEE Computer Security Foundations Workshop*, pp. 82–96, Cape Breton, June 2001.

[6] I. Bocic and T. Bultan, "Symbolic nodel extraction for web application verification," in *2017 IEEE/ACM 39th International Conference on Software Engineering*, pp. 724–734, Buenos Aires, Argentina, May 2017.

[7] V. Dangovas and F. Kuliesius, "SDN-driven authentication and access control system," in *The International Conference on Digital Information, Networking, and Wireless Communications*, pp. 20–23, Czech, June 2014.

[8] D. Erickson, "The beacon OpenFlow controller," in *Proceedings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, pp. 13–18, Hong Kong, China, Aug. 2013.

[9] N. Gude, T. Koponen, J. Pettit, B. Pfaff, and N. Mckeown, "NOX: Towards an operating system for networks," *ACM Sigcomm Computer Communication Review*, vol. 38, no. 3, pp. 105–110, 2008.

[10] F. Hu, Q. Hao, and K. Bao, "Survey on software-defined network and OpenFlow: From concept to implementation," *Communications Surveys & Tutorials IEEE*, vol. 16, no. 4, pp. 2181–2206, 2014.

[11] S. Jain, A. Kumar, S. Mandal, J. Ong, and L. Poutievski, "B4: Experience with a globally-deployed software defined WAN," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, pp. 3–14, Aug. 2013.

[12] J. W. Kang, S. H. Park, and J. You, "Mynah: Enabling lightweight data plane authentication for SDN controllers," in *International Conference on Computer Communication & Networks*, pp. 1–6, Las Vegas, USA, Aug. 2015.

[13] R. Kloti, V. Kotronis, and P. Smith, "OpenFlow: A security analysis," in *IEEE International Conference on Network Protocols*, pp. 1–6, Goettingen, German, Oct. 2014.

[14] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, pp. 55–60, Aug. 2013.

[15] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, and S. Azodolmolky,

"Software-defined networking: A comprehensive survey," in *Proceedings of the IEEE*, vol. 103, no. 1, pp. 10–13, 2014.

[16] J. Liu, Y. X. Lai, Z. P. Diao, and Y. N. Chen, "A trusted access method in software-defined network," *Simulation Modelling Practice and Theory*, vol. 74, pp. 28–45, 2017.

[17] D. M. F. Mattos and O. C. M. B. Duarte, "AuthFlow: Authentication and access control mechanism for software defined networking," *Annals of Telecommunications*, vol. 71, no. 11-12, pp. 607–615, 2016.

[18] J. Medved, R. Varga, A. Tkacik, and K. Gray, "OpenDaylight: Towards a model-driven SDN controller architecture," *World of Wireless, Mobile & Multimedia Networks*, pp. 1–6, 2014.

[19] D. Mery and M. Poppleton, "Towards an integrated formal method for verification of liveness properties in distributed systems: With application to population protocols," *Software & Systems Modeling*, vol. 16, no. 4, pp. 1083–1115, 2017.

[20] R. Milner, "Communicating and mobile systems: The π-calculus," *Cambridge: Cambridge University Press*, pp. 1–5, 1999.

[21] A. A. Mohammed, M. Gharbaoui, B. Martini, F. Paganelli, and P. Castoldi, "SDN controller for network-aware adaptive orchestration in dynamic service chaining," in *IEEE NetSoft Conference and Workshops (NetSoft'16)*, July 2016.

[22] S. Natarajan, A. Ramaiah, and M. Mathen, "A software defined cloud-gateway automation system using OpenFlow," in *IEEE 2nd International Conference on Cloud Networking (CloudNet'13)*, pp. 219–226, San Francisco, Nov. 2013.

[23] P. Porras, S. Shin, V. Yegneswaran, M. Fong, and M. Tyson, "A security enforcement kernel for OpenFlow networks," in *ACM SIGCOMM Workshop on Hot Topics in Software Defined Networks*, pp. 121–126, Helsinki, Finland, Aug. 2012.

[24] L. Schiff, S. Schmid, and P. Kuznetsov, "In-band synchronization for distributed SDN control planes," *ACM SIGCOMM Computer Communication*, vol. 46, no. 1, pp. 37–43, 2016.

[25] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2016.

[26] S. Shin, P. Porras, V. Yegneswaran, M. Fong, and G. Gu, "FRESCO: Modular composable security services for software defined networks," in *Proceedings of Network & Distributed Security Symposium*, 2013.

[27] R. Smeliansky, "SDN for network security," in *1st International Conference on Science and Technology*, Moscow, Russia, Oct. 2014.

[28] M. M. Wang, J. W. Liu, J. Chen andJ. Mao, and K. F. Mao, "Software defined networking: Security model, threats and mechanism(in chinese)," *Journal of Software*, vol. 27, no. 4, pp. 969–992, 2016.

[29] D. Yu, A. W. Moore, C. Hall, and R. Anderson, "Authentication for resilience: The case of SDN," *Lecture Notes in Computer Science*, vol. 8263, pp. 39–44, 2013.

[30] Q. Y. Zuo, M. Chen, G. S. Zhao, C. Y. Xin, and G. M. Zhuang, "Research on OpenFlow-based SDN technologies(in chinese)," *Journal of Software*, vol. 24, no. 5, pp. 1078–1097, 2013.

Biography

Lili Yao was born in 1993 in China. Now she is a postgraduate at School of Computer Science, South-Center for Nationalities, China. Her current research interests include protocol security and data storage security.

Jiabing Liu was born in 1993 and is now a postgraduate at the school of computer, South-Center University for Nationalities, China. His current research interest is the Formal analysis of security protocol.

Dejun Wang was born in 1974 and received his Ph.D. in information security at Wuhan University in China. Currently, he is an associate professor in the school of computer, South-Center University for Nationalities, China. He has authored/coauthored over 20 papers in international/national journals and conferences. His current research interests include security protocols and formal methods.

Jing Li was born in 1989 and graduate from the South-Center University for Nationalities, China. His main research direction includes the analysis of security protocols and formal methods.

Bo Meng was born in 1974 in China. He received his M.S. degree in computer science and technology in 2000 and his Ph.D. degree in traffic information engineering and control from Wuhan University of Technology at Wuhan, China in 2003. From 2004 to 2006, he worked at Wuhan University as a postdoctoral researcher in information security. From 2014 to 2015, he worked at University of South Carolina as a Visiting Scholar. Currently, he is a full Professor at the school of computer science, South-Center University for Nationalities, China. He has authored/coauthored over 50 papers in International/National journals and conferences. In addition, he has also published two books "Automatic generation and verification of security protocol implementations" and "secure remote voting protocol" in the science press in China. His current research interests include security protocols and formal methods.

Multidimensional Data Aggregation Scheme for Smart Grid with Differential Privacy

Xiuxia Tian[1,2], Qian Song[1] and Fuliang Tian[1]
(Corresponding author: Xiuxia Tian)

School of Computer Science and Technology, Shanghai University of Electric Power[1]
No. 2588 Changyang Road, Shanghai 200090, China
(Email: xxtian@fudan.edu.cn)
College of Data Science and Engineering, East China Normal University[2]
No. 3663 Zhongshan Road, Shanghai 200062, China
(Received Sept. 2, 2017; revised and accepted Nov. 28, 2017)

Abstract

The use of smart meters allows the power supplier to collect detailed consumer data from consumers, which may threaten consumers' personal information. In order to protect the privacy of consumers and prevent data leakage from specific consumers, we propose a multidimensional data aggregation scheme with differential privacy. The proposed scheme uses the Horner rule to deal with multidimensional data. The proposed scheme uses certificate-based aggregate short signature to achieve data authentication and data integrity, which reduces the number of bilinear pairing to a constant. Specially, our proposed scheme overcomes the differential attack problem by adding Laplace noise to aggregated data. We analyze the level of differential privacy utility. Compared to existing schemes, the proposed scheme is more efficient in terms of computational cost and communication overhead.

Keywords: Data Aggregation; Differential Privacy; Privacy Protection; Smart Grid

1 Introduction

In the past few years, we have seen increasing interest in smart grid technology around the world [2]. Smart grid, or future power grid, which is a combination of traditional grid systems and advanced information and communication technologies, improves the efficiency, reliability, economy and power generation continuity of the modern grid and provides more stable and reliable power for power users [19, 25]. Advanced communications and information technology applications solve many inherent problems in traditional grids, such as lack of load balancing, intelligent consumption and dynamic pricing [9]. Smart meters in the smart grid system collects consumer power consumption data and other information and send it to the remote control center [11, 20]. The widespread deployment of smart meters has also brought problems about privacy leaks [13]. Smart meters store consumer sensitive power consumption information because they can be used to analyze the user's lifestyle [10]. During the data transmission process, the authenticity, integrity and availability of the data may be destroyed, the user's personal sensitive information may be attacked by the attacker.

Varieties of security protection technologies have been developed in smart metering [21]. The privacy protection of existing smart grid communication process is mostly based on data aggregation technology. The user encrypts the usage data and sends it to the gateway. The gateway authenticates all the received data and sends them to the operation center after they are aggregated. Data aggregation technology refers to the use of encryption methods to enable power companies to calculate the total power of all users to analyze the data without knowing the power consumption of each user [25]. Existing data aggregation schemes use techniques such as homomorphic encryption [15, 16, 17, 19], blind factors [8] and differential privacy [3, 4, 18]. However, many of these schemes can not achieve both integrity and confidentiality. Also they can not resist some specific attacks. At the same time, many studies are concerned about the one-dimensional data, but with the development of smart meter technology we need to focus on dealing with multidimensional data.

In order to solve the existing problems of data aggregation scheme, we propose a multidimensional data aggregation scheme with differential privacy.

The contributions of this paper are in the following:

1) The proposed scheme uses certificate-based aggregate short signatures [12]. The aggregated signatures used in the scheme are short and efficient, which reduces the number of bilinear pairing to a constant. The security analysis demonstrates we can achieve data

authentication and data integrity.

2) To resist the differential attack, the proposed scheme provides ε-differential privacy by adding the Laplace noise selected from the Laplace distribution to the aggregated data of the community gateway.

3) Compared with others schemes, the proposed scheme has lightweight computational cost and communication overhead.

The remainder of this work works as follows: Section 2 describes the work of the existing data aggregation scenario. Section 3 describes the system model and the security model. Section 4 outlines the relevant preliminaries. Section 5 presents our multidimensional data aggregation scheme. Section 6 and Section 7 give the security and performance analysis. Finally we draw our conclusions in Section 8.

2 Related Works

In order to solve the privacy problem in the smart grid data aggregation, a variety of data aggregation privacy protection scheme are proposed. Li *et al.* [15] proposed a method of incremental aggregation in the network using homomorphic encryption, which did not solve the problem of authentication and data integrity. Li *et al.* [16] proposed a scheme about privacy protection demand response, which is based on homomorphic encryption and identity-based signature to achieve the security of the one-dimensional data aggregation. It also used adaptive key evolution technology for demand response. Bao *et al.* [3] proposed a lightweight data aggregation scheme that added symmetric geometric noise to resist differential attacks and achieved fault tolerance. The scheme used non-interactive session keys for source authentication and integrity protection.

Chen *et al.* [5] proposed a multifunctional data aggregation scheme that implemented statistical functions for usage data, such as averaging, variance and so on. Fan *et al.* [8] proposed the first one-dimensional data aggregation solution for internal attackers, which utilized blind factors to process confidential data and used small indexes to improve batch validation to achieve security utility. He *et al.* [10] improved the key leak problem in Fan's scheme, by reducing the number of bilinear pairing operations. In order to reduce the computational cost, He *et al.* [11] continued to improve the scheme, by using elliptic curve cryptography and implementing a lightweight data aggregation based on the *Schnorr* signature scheme. Abdalla *et al.* [1] used the $NTRU$ cryptosystem to achieve privacy protection, and the new ring signature NSS was signed to ensure integrity. But the scheme focused on the prediction of the demand for electricity from a group of customers in the same region instead of focusing on the process of data aggregation.It also restricted the connection with the provider only when the total clusters demand needed to be adjusted.

All the aforementioned schemes consider one-dimensional data aggregation. In order to deal with the problem of multidimensional data aggregation, Lu *et al.* [17] proposed the use of super-increasing sequence to process multidimensional electricity data. The *Paillier* homomorphic encryption system was used to encrypt the aggregated data during data transmission, and they used BLS short signature and batch verification. But the scheme had only one residential area and a gateway, which limited the size of the user and could not resist the differential attack. Fu *et al.* [9] used the elliptic curve *ElGamal* cryptography to encrypt multidimensional data and adopted the method of aggregated signature to carry out secure multidimensional data aggregation. However, the data aggregation result obtained by this scheme was the sum of all data. They could not separate the fine-grained data of each dimension. Zhou *et al.* [26] proposed a multilevel network aggregation scheme with fault tolerance and invalid signatures search. Shen *et al.* [19] used the Horner rule to handle multidimensional data by using two-level gateways to protect privacy. The aggregation scheme could handle dynamic users, but it could not resist differential attacks.

3 System Model And Security Requirements

In this section we will introduce the system model and security requirements.

3.1 System Model

The system is a four-layer smart grid communication network structure, which consists of the operation center, regional gateway, community gateway and home area network (*ie* users). The system model is shown in Figure 1. An operation center is responsible for a region, corresponding to the regional gateway; a region has m communities, corresponding to the community gatewayBGW_1, BGW_2,BGW_3...BGW_m. The first i community has n_i users, and each user collects their electricity data with a smart meter.

- OC: OC is a trusted entity that is responsible for the registration verification of the gateway and the user. It issues certificates for all gateway and users, generates keys for the entire system and issues public parameters. It also collects, processes and analyzes real-time data, such as the sum of power usage data for a given dimension or the power consumption during peak hours, which implements segmented power pricing decisions and appropriate resource allocation to provide reliable service for smart grid systems.

- DGW: DGW has the function of aggregation and relay. It's responsible for verifying messages from various BGWs and aggregating them. Then DGW forwards the messages to OC.

- *BGW*: *BGW* has the same function as *DGW*, responsible for verifying the confidential information received by the users. Then *BGW* aggregates the information and forwards them to the higher level gateway. In this process, *BGW* may be easily attacked by external attackers (such as differential attacks) because of the low level of security.
- *U*: The smart meter owned by the user is responsible for periodically (for example, every 15 minutes) to encrypt the coarse-grained l-dimensional data and report it to *BGW*.

The communication between the user and *BGW* generally uses *WiFi* technology, while *BGW* and *DGW* , *DGW* and *OC* generally use the wired link to communicate.

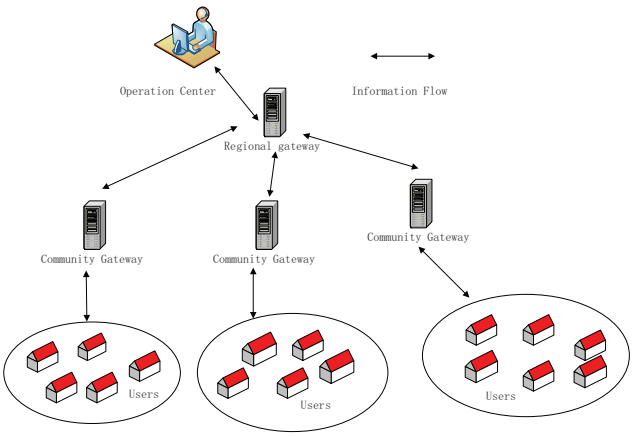


Figure 1: The proposed scheme

3.2 Security Requirements

In this system, we believe that *OC*, *DGW*,*BGW* are completely trusted, but users are semi-honest, which means users will not deliberately leak or change the information, but they are curious about others, trying to infer the usage information of others.

There may be an adversary A in the system who will steal the usage data when the user sends their data to the gateway; or an adversary attack (such as a differential attack) by analyzing the similar data sets obtained from the two aggregations may happen, trying to infer the individual user's sensitive information from the aggregation difference.

Adversary A may also invade the database of *DGW* and *BGW*, or invade communication links, which will destroy the authenticity and integrity of the data.

Confidentiality: Even if some users may collude with each other,they can not get the usage information of other users. Adversary A who steals the electricity data can not get the relevant information of a single user.

Authentication and data integrity: The user's electricity data in the transmission process requires authentication to avoid being tampering or forgery by malicious attackers.

Differential privacy: Even if the opponent A launches a differential attack, he/she can not get the individual user's sensitive electricity data.

4 Preliminaries

In this section we will outline the knowledge of Bilinear pairing, *Paillier* encryption algorithm, horner rule, and differential privacy as the basis of our scheme.

4.1 Bilinear Pairing

Let k be the security parameter and p be the prime with k bits. Let G_1,G_T be a cyclic addition group of order p generated by P (generator); a and b are elements in Z_p (Z_p is the prime p-order cyclic group).

Assume that the discrete logarithm problem in G_1 and G_T is a difficult problem. Bilinear pairing is a mapping that satisfies the following properties [22]:

- Bilinearity: For any $P, Q \in G_1$ and $a, b \in Z_p$, we have $e(aP, bQ) = e(P, Q)^{ab}$.
- Non-degenerative: There are $P, Q \in G_1$, making $e(P, Q) \notin 1$.
- Computability: For all $P, Q \in G_1$, there exists valid algorithms to calculate $e(P, Q)$.

4.2 Paillier Encryption Algorithm

In the *Paillier* cryptography system, the public key is $pk(N, g)$, the corresponding private key is $sk(\lambda, \mu)$. Let $E(\cdot)$, m and r represent encrypted functions, messages and random numbers respectively. The ciphertext is $c = E(m) = g^m \cdot r^N mod N^2$. The plaintext is $m = D(c) = L(c^{\lambda mod N^2}) \cdot \mu mod N$.

4.3 Horner Rule [19]

The Horner rule uses the least multiplication strategy to find the value of the polynomial $A = a_n x^n + a_{n-1} x^{n-1} + ...+a_1 x+a_0$ at x. Using this rule, n coefficients a_1,a_2,...,a_n are obtained by n multiplications and n additions.

4.4 Differential Privacy [6]

If the data aggregation result D includes the user Bob's power usage data, the algorithm M (D) is executed to obtain some calculation results. Assuming that the data aggregation result D is changed to D' after deleting of Bob's data , the execution of the algorithm M (D') or M (D) produces almost the same result. It is assumed that Bob's usage data is safe in the data set D under the algorithm M. It means whether Bob's data exists or not will not affect the output.

4.4.1 ε-Differential Privacy

If the data sets $D_1$and D_2 are different for at most one element, the randomization function K gives ε- differential privacy, that is, for any $s \in Range(k)$, we have $P[k(D_1) \in s] \leq e^{\varepsilon} P[k(D_2) \in s]$.

4.4.2 Laplace Mechanism [7]

Laplace mechanism is to use the Laplace distribution to produce noise. The probability density function of the Laplace distribution is $p(x) = \frac{1}{2b} e^{-\frac{|x|}{b}}$. From the Laplace distribution, noise r is randomly selected to be added to the original aggregation, the perturbed result can achieve ε- differential privacy.

5 Multidimensional Data Aggregation Scheme

In this paper, the multi-dimensional data aggregation scheme with differential privacy is divided into five stages: initialization phase, registration phase, user data encryption phase, secure aggregation phase and data recovery phase.

The processing of each stage is described in detail below and the meaning of each character symbol is shown in Table 1.

5.1 Initialization

At this stage, OC generates and publishes the parameters. Giving the security parameters k and k_1, OC guides the entire system.

Step 1. OC generates (q, P, G_1, G_2, e) by running $Gen(k)$. Then OC calculates the $Paillier$ encryption system's public key $(N = pq, g)$ and the corresponding private key (λ, μ).

Step 2. Define four secure hash functions $H_0 : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to Z_q^*$, $H_3 : \{0,1\}^* \to G_1$.

Step 3. Select two random factors R and R_1. After choosing the random number $s \in Z_q^*$ as the master key, OC compute the relevant public key $P_{pub} = sP$ and $Q_{pub} = H_1(P, P_{pub})$.

Step 4. Finally, OC publishes the system public information $\{q, P, G_1, G_T, e, N, g, R, R_1, H_0, H_1, H_2, H_3, P_{pub}, Q_{pub}\}$.

5.2 Registration Phase

In this section, we have to complete the registration of regional gateways , community gateways and users to ensure their legitimacy. The registration phase includes regional gateway registration, community gateway registration and user registration.

5.2.1 Regional Gateway Registration

DGW registers in OC and OC issues a certificate for it. After registration, DGW becomes a legal regional gateway. The process is as follows.

Step 1. DGW generates two random numbers $r, x \in Z_q^*$, calculates $X = xP$, $\alpha = rP$ and $\beta = r - xH_0(ID \parallel \alpha) mod q$ where is the x private key, X is the public key. DGW then sends the message$\{X, \alpha, \beta, ID\}$to the OC.

Step 2. OC checks the equation $\alpha = P\beta + XH_0(ID \parallel \alpha)$. If it does not exist, OC will deny the registration; otherwise, OC calculate $Q_{ID} = H_3(ID, X)$ and issues a certificate $cert_{ID} = sQ_{ID}$.

Verification of regional gateway registration:

$$\begin{aligned} & P\beta + XH_0(ID \parallel \alpha) \\ =& P(r - xH_0(ID \parallel \alpha) mod q) + XH_0(ID \parallel \alpha) \\ =& rP - xPH_0(ID \parallel \alpha) + XH_0(ID \parallel \alpha) \\ =& \alpha - XH_0(ID \parallel \alpha) + XH_0(ID \parallel \alpha) \\ =& \alpha \end{aligned} \tag{1}$$

5.2.2 Community Gateway Registration

BGW registers in OC and OC issues a certificate for it. After registration, BGW becomes a legal community gateway. The process is as follows.

Step 1. BGW_i generates two random numbers $r_i, x_i \in Z_q^*$, calculates $X_i = x_i P$, $\alpha_i = r_i P$ and $\beta_i = r_i - x_i H_0(ID_i \parallel \alpha_i) mod q$ where is the x_i private key, X_i is the public key. Then BGW sends the message $\{X_i, \alpha_i, \beta_i, ID_i\}$ to the OC.

Step 2. OC checks the equation $\alpha_i = P\beta_i + X_i H_0(ID_i \parallel \alpha_i)$. If it is not met, OC will deny the registration; otherwise, OC calculates $Q_{ID_i} = H_3(ID_i, X_i)$ and issues a certificate $cert_{ID_i} = sQ_{ID_i}$.

Verification of community gateway registration:

$$\begin{aligned} & P\beta_i + X_i H_0(ID_i \parallel \alpha_i) \\ =& P(r_i - x_i H_0(ID_i \parallel \alpha_i) mod q) + X_i H_0(ID_i \parallel \alpha_i) \\ =& r_i P - x_i P H_0(ID \parallel \alpha) + X_i H_0(ID_i \parallel \alpha_i) \\ =& \alpha_i - X_i H_0(ID_i \parallel \alpha_i) + X_i H_0(ID_i \parallel \alpha_i) \\ =& \alpha_i \end{aligned} \tag{2}$$

5.2.3 User Registration

U registers in OC and OC issues a certificate for it. After registration, U becomes a legal user. The specific process is as follows.

Step 1. U_{ij} generates two random numbers $r_{ij}, x_{ij} \in Z_q^*$, calculates $X_{ij} = x_{ij} P$, $\alpha_{ij} = r_{ij} P$ and $\beta_{ij} = r_{ij} - x_{ij} H_0(ID_{ij} \parallel \alpha_{ij}) mod q$ where the x_{ij} is private key, X_{ij} is the public key. Then U_{ij} sends the message $\{X_{ij}, \alpha_{ij}, \beta_{ij}, ID_{ij}\}$ to the OC.

Table 1: Notations

Notations	Description
OC	Operation Center
DGW	Regional Gateway
BGW	Community Gateway
U	User
$k, q, P,$	Bilinear pair parameter
k_i, p, q, g	Paillier password system parameters
H_0, H_1, H_2, H_3	Hash functions
R, R_i	The factor that handles multidimensional data
n	The maximum number of users in a community
n_i	The number of users in the i-th community
r	Random number
ε	Differential privacy budget

Step 2. OC checks the equation $\alpha_{ij} = P\beta_{ij} + X_{ij}H_0(ID_{ij} \parallel \alpha_{ij})$. If it is not met, OC will deny the registration; otherwise, OC calculates $Q_{ID_{ij}} = H_3(ID_{ij}, X_{ij})$ and issues a certificate $cert_{ID_{ij}} = sQ_{ID_{ij}}$.

Verification of user registration:

$$\begin{aligned} & P\beta_{ij} + X_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) \\ =& P(r_{ij} - x_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) mod q) + X_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) \\ =& r_{ij}P - x_{ij}PH_0(ID_{ij} \parallel \alpha_{ij}) + X_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) \\ =& \alpha_{ij} - X_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) + X_{ij}H_0(ID_{ij} \parallel \alpha_{ij}) \\ =& \alpha_{ij} \end{aligned} \tag{3}$$

5.3 User Data Encryption

The user data encryption generation phase is responsible for handling users' multidimensional data. Users regularly collect their l-dimensional usage data$(d_{ij1}, d_{ij2}, ..., d_{ijl})$. Like [19], we handle multi-dimensional data by synthesizing the l-dimensional data into a polynomial and implements the following steps:

Step 1. Structure a polynomial with l-dimensional usage data $M_{ij} = R_i^i(d_{ij1}R^1 + d_{ij2}R^2 + ... + d_{ijl}R^l)$;

Step 2. The user selects r_{ij}^* and calculates the ciphertext $C_{ij} = g^{M_{ij}}r_{ij}^{*N} mod N^2$;

Step 3. Calculate $h_{ij1} = H_0(ID_{ij} \parallel C_{ij} \parallel X_{ij} \parallel T \parallel P_{pub})$,$h_{ij2} = H_2(ID_{ij} \parallel C_{ij} \parallel X_{ij} \parallel T \parallel Q_{pub})$,$V_{ij} = h_{ij1} \cdot cert_{ID_{ij}} + x_{ij} \cdot h_{ij2} \cdot Q_{pub}$. The signature is $\sigma_{ij} = (C_{ij}, V_{ij})$;

Step 4. Send $(ID_{ij}, \sigma_{ij}, C_{ij}, T)$ to BGW_i.

5.4 Secure Aggregation Phase

In this section we mainly complete the secure aggregation of data in the community gateway and the regional gateway. Before the gateway data aggregation, we rely on the aggregation of certificate-based short signatures to complete the security certification, which ensures the integrity of the data during transmission process. The length of the signature and the number of bilinear pairing involved in the algorithm are independent of the number of users. After the community gateway data is aggregated, we add noise to the community gateway to achieve differential privacy.

5.4.1 Community Gateway Aggregation

The community gateway aggregates the signatures of the received data and verifies it. Then the community gateway aggregates the encrypted data for all users in their own community. During this process, the community gateway will add Laplace noise to the encrypted data to resist differential attack. To add Laplace noise to the aggregated data, the sensitivity of the data set need to be calculated.

Let D be a subset of the users and for two data sets D_1 and D_2 with only one element different, we have $\| A(D_1) - A(D_2) \|_1 \leq W$. Therefore, the sensitivity of A is $\Delta f = W$.

Step 1. Verify the received data $(ID_{ij}, \sigma_{ij}, C_{ij}, T)$. Then BGW calculates received n_i users aggregate signature $V_0 = \sum_{j=1}^{n_i} V_{ij}$ by using the aggregate signature generator. The corresponding signature set is $\{(C_{i1}, V_{i1}), (C_{i2}, V_{i2}), ..., (C_{in_i}, V_{in_i})\}$.

Step 2. Check that if the verification $e(V_0, P) = e(\sum_{j=1}^{n_i} h_{ij1}Q_{ID_{ij}}, P_{pub})e(\sum_{j=1}^{n_i} h_{ij2}X_{ij}, Q_{pub})$ is met.

Step 3. If the verification is successful, the BGW aggregates $n = n_i + n - n_i$ encrypted l-dimensional data items $C_{i1}, C_{i2}, ..., C_{in}$, where the n_i usage data reports are received from smart meters and the remaining $n - n_i$ data reports are constructed from

the zero-dimensional vector. Then aggregate n ciphertexts $C_{GW_i} = \prod_{j=1}^{n} C_{ij} mod N^2$.

Step 4. According the sensitivity $\Delta f = W$, BGW generates a noise $\tilde{m}_i$ from the Laplace distribution. The final result is calculated as $\tilde{C}_{GW_i} = C_{GW_i} \cdot g^{\tilde{m}_i}$. The resulting ciphertext is the disturbed data and the noise therein ensures the privacy of each user.

Step 5. BGW calculates $h_{i1} = H_0(ID_i \parallel \tilde{C}_{GW_i} \parallel X_i \parallel T \parallel P_{pub})$, $h_{i2} = H_2(ID_i \parallel \tilde{C}_{GW_i} \parallel X_i \parallel T \parallel Q_{pub})$, $V_i = h_{i1} \cdot cert_{ID_i} + x_i \cdot h_{i2} \cdot Q_{pub}$. The signature is $\sigma_i = (\tilde{C}_{GW_i}, V_i)$;

Step 6. BGW sends $(ID_i, \sigma_i, \tilde{C}_{GW_i}, T)$ to DGW_i.

Verification of correctness:

$$\begin{aligned} & e(V_0, P) \\ =& e(\sum_{j=1}^{n_i} V_{ij}, P) \\ =& e(\sum_{j=1}^{n_i} (h_{ij1} cert_{ID_{ij}} + x_{ij} h_{ij2} Q_{pub}), P) \\ =& e(\sum_{j=1}^{n_i} h_{ij1} cert_{ID_{ij}}, P) e(\sum_{j=1}^{n_i} x_{ij} h_{ij2} Q_{pub}, P) \\ =& e(\sum_{j=1}^{n_i} h_{ij1} Q_{ID_{ij}}, P_{pub}) e(\sum_{j=1}^{n_i} h_{ij2} X_{ij}, Q_{pub}). \end{aligned} \tag{4}$$

5.4.2 Regional Gateway Aggregation

The regional gateway aggregates the signatures of the received data and verifies it. Then the regional gateway aggregates the encrypted data for all users in its region.

Step 1. For the received data $(ID_i, \sigma_i, \tilde{C}_{GW_i}, T)$, DGW uses the aggregate signature generator to calculate $V_0^* = \sum_{i=1}^{m} V_i$. Then DGW uses the aggregated short signature verification method to verify if $e(V_0^*, P) = e(\sum_{i=1}^{m} h_{i1} Q_{ID_i}, P_{pub}) e(\sum_{i=1}^{m} h_i X_i, Q_{pub})$.

Step 2. If the above verification is successful, the aggregation operation $\tilde{C} = \prod_{i=1}^{m} \tilde{C}_{GW_i} mod N^2$ is performed by DGW.

Step 3. DGW calculates $h_1 = H_0(ID \parallel \tilde{C} \parallel X \parallel T \parallel P_{pub})$, $h_2 = H_2(ID \parallel \tilde{C} \parallel X \parallel T \parallel Q_{pub})$, $V = h_1 \cdot cert_{ID} + x \cdot h_2 \cdot Q_{pub}$. The signature is $\sigma = (\tilde{C}, V)$;

Step 4. DGW sends $(ID, \sigma, \tilde{C}, T)$ to OC.

Verification of correctness:

$$\begin{aligned} & e(V_0^*, P) \\ =& e(\sum_{i=1}^{m} V_i, P) \\ =& e(\sum_{i=1}^{m} (h_{i1} cert_{ID_i} + x_i h_{i2} Q_{pub}), P) \\ =& e(\sum_{i=1}^{m} h_{i1} cert_{ID_i}, P) e(\sum_{i=1}^{m} x_i h_{i2} Q_{pub}, P) \\ =& e(\sum_{i=1}^{m} h_{i1} Q_{ID_i}, P_{pub}) e(\sum_{i=1}^{m} h_{i2} X_i, Q_{pub}). \end{aligned} \tag{5}$$

5.5 Data Recovery

For the received $(ID, \sigma, \tilde{C}, T)$, OC verifies if the signature $e(V, P) = e(h_1 Q_{ID}, p_{pub}) e(h_2 X, Q)$. After successful verification, the $Paillier$ decryption algorithm is used to obtain the sum of all multidimensional data. Then We use Horner rules to analyze the sum of the data for each dimension.
Verification of correctness:

$$\begin{aligned} & e(V, P) \\ =& e(h_1 cert_{ID} + x h_2 Q_{pub}), P) \\ =& e(h_1 cert_{ID}, P) e(x h_2 Q_{pub}, P) \\ =& e(h_1 Q_{ID}, P_{pub}) e(h_2 X, Q_{pub}). \end{aligned} \tag{6}$$

$$\begin{aligned} \tilde{C} &= \prod_{i=1}^{m} C_{GW_i} \cdot g^{\sum_{i=1}^{m} \tilde{m}} mod N^2 \\ &= (\prod_{i=1}^{m} (\prod_{j=1}^{n} g^{M_{ij}} \cdot r_{ij}^* mod N^2)) g^{\sum_{i=1}^{m} \tilde{m}} \\ &= (\prod_{j=1}^{n} (\prod_{i=1}^{m} g^{M_{ij}} \cdot r_{ij}^* mod N^2)) g^{\sum_{i=1}^{m} \tilde{m}} \\ &= (\prod_{j=1}^{n} (g^{M_{1j}} \cdot g^{M_{2j}} \cdot \ldots \cdot g^{M_{mj}}) (\prod_{i=1}^{m} \prod_{j=1}^{n} r_{ij}^* mod N^2)) g^{\sum_{i=1}^{m} \tilde{m}} \end{aligned} \tag{7}$$

Let $R^* = \prod_{i=1}^{m} \prod_{j=1}^{n} r_{ij}^*$. We have

$$\begin{aligned} \tilde{C} &= g^{\sum_{j=1}^{n} M_{1j} + \sum_{j=1}^{n} M_{2j} + \ldots + \sum_{j=1}^{n} M_{mj} + \sum_{i=1}^{m} \tilde{m}} R^* mod N^2 \\ &= g^{R_1^1 \sum_{j=1}^{n} \sum_{v=1}^{l} R^v d_{1jv} + \ldots + R_1^m \sum_{j=1}^{n} \sum_{v=1}^{l} R^v d_{mjv} + \sum_{i=1}^{m} \tilde{m}} R^* mod N^2 \\ &= g^{R_1^1 \sum_{j=1}^{n} R^v \sum_{v=1}^{l} d_{1jv} + \ldots + R_1^m \sum_{j=1}^{n} R^v \sum_{v=1}^{l} d_{mjv} + \sum_{i=1}^{m} \tilde{m}} R^* mod N^2 \end{aligned} \tag{8}$$

Let $B_{iv} = \sum_{j=1}^{n} d_{ijv}$,which represents the sum of the

electricity data of the first v dimension of all users in community i. We have $B_i = \sum_{v=1}^{l} R^v \cdot B_{iv}$ and $\tilde{m} = \sum_{i=1}^{m} \tilde{m}_i$.

Let

$$\begin{aligned} M &= R_1^1 \sum_{j=1}^{n} R^v \sum_{v=1}^{l} d_{1jv} + ... + R_1^m \sum_{j=1}^{n} R^v \sum_{v=1}^{l} d_{mjv} \\ &= \sum_{i=1}^{m} R_1^i \sum_{v=1}^{l} R^v \cdot B_{iv} \\ &= \sum_{i=1}^{m} R_1^i \cdot B_i \end{aligned} \tag{9}$$

We have $\tilde{M} = M + \tilde{m}$. Because $\tilde{C} = g^{\tilde{M}} \cdot r_{ij}^{*N} mod N^2$ is still *Paillier* encryption algorithm form, we can get $\tilde{M}$ by using the corresponding private key (λ, μ). Here, although $\tilde{M}$ is the noisy data, the impact of noise added temporarily can be ignored. It will not affect the operation center for its analysis, because the accuracy of the meter level allows the existence of the error and the error can be controlled within the allowable range by changing the size of ε.

By executing the data recovery algorithm [19] in Table 2, using $\tilde{M}$ and R_1 as the input of the algorithm, OC can obtain B_i. Using B_i and R as the input of the algorithm, OC can get B_{iv}.

Algorithm 1 Data recovery algorithm

Input:A and x $//A = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x$
Output:$\{a_1, a_2, ...a_n\}$

1: $X_0 = A / x$
2: **for** $j = 1$ to l **do**
3: $\quad a_j = X_{j-1} \bmod x$
4: $\quad X_j = X_{j-1} \bmod x$
5: **end for**
6: **return** $\{a_1, a_2, ...a_l\}$

6 Security Analysis

In this section, we will show that our multidimensional data aggregation scheme implements the security requirements that are proposed in Section 3.

- Confidentiality: The confidentiality of user data is protected. Because the users' encrypted data exist in the form of ciphertext $C_{ij} = g^{M_{ij}} \cdot r_{ij}^{*N} mod N^2$ during the transmission process, and the *Paillier* cryptography system is semantically secure for the selected plaintext attacks, the adversary can not obtain the user's electricity information. Even if the adversary invades the gateway database, he/she still can not get the user's specific electricity information. The malicious users who want to analyze other people's usage information may collude with each other to share their own data, but they can not infer electricity consumption of other users because the user's private key is a secret storage.

- Unforgeability and Data Integrity: The authentication and integrity of user data and aggregation data are protected. In this scheme, the user's private key is composed of two parts, one part is the user certificate generated by OC, and the other part is the secret value, which is independently selected by the user. Therefore, the security certification of certificate-based signature is to prove that only know the user's certificate and secret value (*ie*, fully aware of the user's private key) to produce a valid signature. If an adversary wants to crack a signer's private key or certificate, it faces the difficulty of solving the discrete logarithm, which is safe in the random prediction model under the CDH model [12, 23, 24].

- Differential Privacy: User data can resist differential attacks. Differential attack is to change the input of the algorithm, through the output of the algorithm or the change value of the output to expose the information in the algorithm input. If we use an algorithm to compute the aggregation result of a group of users' usage data, the differential attack can obtain a set of aggregation results by using the algorithm again. If the data of the two aggregations differ by only one user U, then the power consumption data of the user U can be obtained by subtracting the value of the two aggregation results.

  In this scheme, ε-differential privacy is achieved by adding noise to the community gateway with a given privacy level of ε. Even if the external adversary initiates a differential attack by analyzing the similar data sets obtained from the two aggregations, he/she gets the data with noise and can not calculate the electricity usage information of a single user.

  Assume that the adversary A obtains two perturbed aggregations $s + \tilde{m}_s$ and $t + \tilde{m}_t$, where s and t are two data sets with only one element different and $\tilde{m}_s$ and $\tilde{m}_t$ are two corresponding *Laplacian* noise. Because$|s - t| \leq W$, for any integer k, we have

$$\begin{aligned} \theta &= P(s + \tilde{m}_s = k)/P(t + \tilde{m}_t = k) \\ &= P(\tilde{m}_s = k - s)/P(\tilde{m}_t = k - t) \\ &= \frac{1}{2b} e^{-\frac{|k-s|}{b}} / \frac{1}{2b} e^{-\frac{|k-t|}{b}} \\ &= e^{-\frac{|k-s|-|k-t|}{b}} \end{aligned} \tag{10}$$

  Because$-|s-t| \leq |k-s|-|k-t| \leq |s-t|$, we have $\theta \leq e^{|s-t|/b} \leq e^{W/b} = e^{\varepsilon}$ satisfying ε-differential privacy. So the aggregated data set is added enough noise to provide differential privacy for each participating user while still provides high efficiency. Our scheme is safe in ε-differential privacy and can provide a strong and provable privacy guarantee.

Table 2: Comparison of five multidimensional electricity data aggregation schemes

Performance	Our scheme	Lu's scheme	Shen's scheme	Fu's scheme	Zhou's scheme
Confidentiality	Yes	Yes	Yes	Yes	Yes
Unforgeability	Yes	No	Yes	No	Yes
Signature verification security	Yes	No	Yes	No	Yes
Multi-level gateway	Yes	No	Yes	No	Yes
Dynamic users	Yes	No	Yes	No	Yes
Differential privacy	Yes	No	No	No	No

7 Performance Analysis

This section describes our scheme from the implemented functions, the computational cost, the communication overhead and the differential privacy utility. Table 2 shows the performance of the proposed scheme and the other four multidimensional data aggregation schemes [9, 17, 19, 26]. We compared confidentiality, data integrity, unforgeability, signature verification security, multi-level gateway, dynamic users and differential privacy. Lu's scheme [17] and Fu's scheme [9] have problems in security of batch authentication signatures. Although Fu's scheme [9] can handle the aggregation of multidimensional data, the aggregated result is not the fine-grained data of each dimension. Shen's scheme [19] solves the problem of counterfeiting in batch verification. But the above schemes can not resist the differential attacks.

7.1 Computational Complexity

In our scheme, C_e,C_m and C_p represent the computational cost of an exponentiation operation in Z_{n^2}, a scalar multiplication operation in G_1 and a pairing operation. According to Shen's scheme [19], the computational cost of an exponential operation, a pairing operation and a multiplication operation is shown in Table 3. Compared with the exponential operations and pairing operations, the computational cost of the multiplication operations in Z_n and the hash operations are considered negligible.

For our proposed scheme, a user U_{ij} needs to perform two exponential operations in Z_{n^2} to generate C_{ij} and a scalar multiplication operation in G_1 to generate the signature. A community gateway needs to perform three pairing operations and $2n_i$ scalar multiplication operations to verify the aggregated signature. An exponential operation needed to be used to add noise. A community gateway generates the signature with a scalar multiplication operation. In order to verify the aggregated data from the BGWs, a regional gateway need to perform three pairing operations and $2m$ multiplication operations. A DGW need to generate the signature with a scalar multiplication operation. For the OC, three pairing operations and two multiplication operations are used to verify the signature.

In Table 4 we compare the computational cost of our scheme with Shen's scheme [19], Zhou's scheme [26] and our scheme. The computational cost of the user in Zhou's scheme is related to the dimension of the data, but our scheme and Shen's scheme are independent of the dimension of the data. Obviously our scheme has a better performance than Zhou's scheme. Through the following analysis, we show that our scheme is better than Shen's scheme too.

On the community gateway side, we assume that the maximum number of users per community is $n(n \geq n_i)$, let

$$\begin{aligned} 3C_p + C_e + (2n+1)C_m &\leq (n+2)C_p + C_m \\ 78.8 + 12.8n &\leq 20n + 46.4 \\ 7.2n &\geq 32.4 \\ n &\geq 4.5 \end{aligned} \tag{11}$$

When the number of users in a community is greater than or equal to 5, our scheme has a less computational cost. From Figure 2, it can be seen our scheme has a better performance on the community gateway side.

On the regional gateway side, m is the number of community gateways, let

$$\begin{aligned} 3C_p + (2m+1)C_m &\leq (m+2)C_p + C_m \\ 66.4 + 12.8m &\leq 20m + 46.4 \\ 7.2m &\geq 20 \\ m &\geq 2.78 \end{aligned} \tag{12}$$

When the number of community gateways is greater than or equal to 3, our scheme has a less computational cost.

From Figure 3, it can be seen our scheme has a better performance on the regional gateway side.

According to Table 4, we compared the total computational cost of our scheme, Shen's scheme and Zhou's scheme. The computational cost of Zhou's scheme is related to the dimension of the data, so we assume the dimension of the data is 3. From Figure 4, Figure 5 and Figure 6, it is obvious that our scheme has a better performance.

7.2 Communication Overhead

For each user encrypted data $(ID_{ij}, \sigma_{ij}, C_{ij}, T)$, the communication overhead for all users in a community to the

Table 3: Description Calculation time (ms)

Symbol	Description	Calculation time (ms)
C_e	Exponential operation	12.4
C_p	Bilinear pairing operation	20
C_m	Multiplication	6.4

Table 4: The cost comparison

Symbol	Our scheme	Shen's scheme	Zhou's scheme
$User$	$2C_e + C_m$	$2C_e + C_m$	$(l+1)C_e + C_m$
BGW	$3C_p + (n - n_i + 1)C_e + (2n_i + 1)C_m$	$(n_i + 2)C_p + (n - n_i)C_e + C_m$	$2C_p + (4n - 1)C_m + C_e$
DGW	$3C_p + (2m + 1)C_m$	$(m + 2)C_p + C_m$	$2C_p + (4m - 2)C_m$
OC	$3C_p + 2C_m$	$2C_p$	$2C_p$

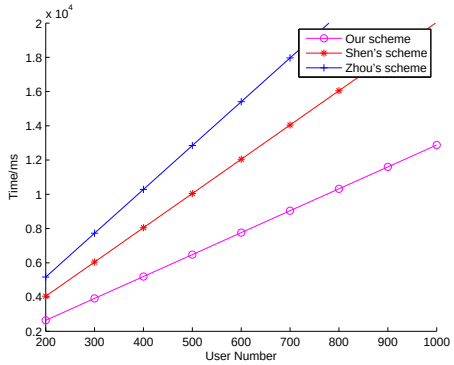


Figure 2: The computational cost of each BGW

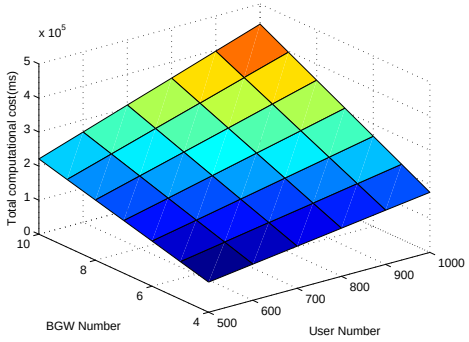


Figure 4: The total computational cost of our scheme

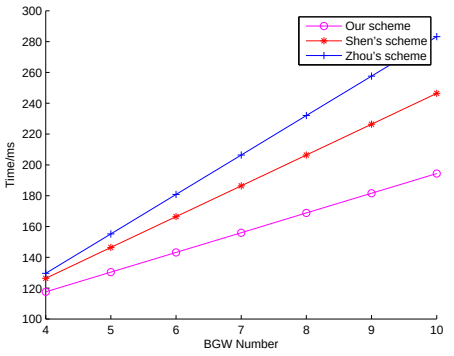


Figure 3: The computational cost of each DGW

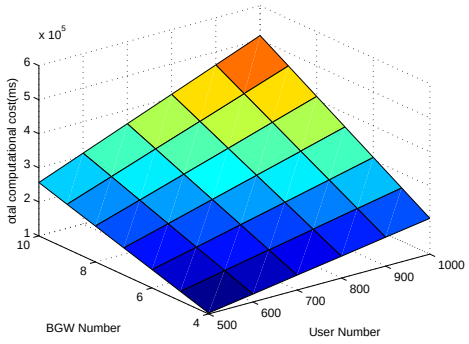


Figure 5: The total computational cost of Shen's scheme

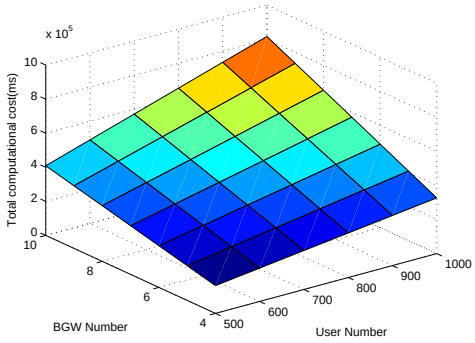


Figure 6: The total computational cost of Zhou's scheme

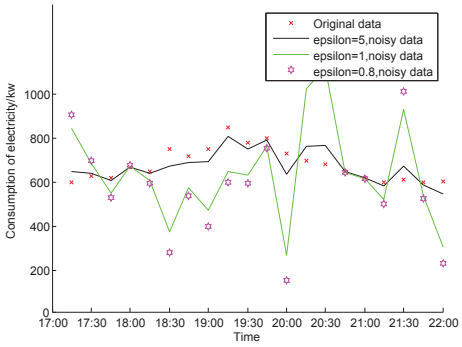


Figure 7: Differential privacy utility comparison

community gateway is $S_{U\to BGW} = (|ID_{ij}|+|\sigma_{ij}|+|C_{ij}|+|T|)n$. For each community gateway aggregated data $(ID_i, \sigma_i, \tilde{C}_i, T)$, the communication overhead for all community gateways in a region to the community gateway is $S_{BGW\to DGW} = (|ID_i| + |\sigma_i| + |\tilde{C}_i| + |T|)m$. For each regional gateway aggregated data $(ID, \sigma, \tilde{C}, T)$, the communication overhead for a regional gateway to the operations center is $S_{DGW\to OC} = |ID| + |\sigma| + |\tilde{C}| + |T|$.

We choose 1,024 bits N ($|N^2| = 2048$) and 160 bits G_1, set $|ID|+|T|$ to 64 bits. Table 5 shows the communication overhead comparison of our scheme and other two schemes [17, 19].

The total communication cost of our scheme is $2272 * m * n + 2272 * m + 2272$ and the total communication cost of Shen's scheme is $2308 * m * n + 2308 * m + 2308$. Our scheme has less communication overhead than the other schemes.

7.3 Differential Privacy Utility Comparison

In order to verify the effectiveness of differential privacy, we assume that a community has 1,000 users. Between 17: 00-22: 00, every 15 minutes of electricity data is aggregated, the community gateway adds Laplace noise to achieve ε - differential privacy. Through the inverse cumulative distribution function of the Laplace distribution, we obtain the Laplace noise by inputting the random variables uniformly distributed in the range of (-0.5, 0.5) for this inverse cumulative distribution function.

ε is the privacy budget, based on the data,we have $\Delta f = 200$.

From Figure 7, it can be seen that the smaller ε we use , the better the effect of privacy protection we have, but the utility is relatively poor. The large ε we use, the utility is better. The literature [14] made a more detailed introduction about how to choose ε.

8 Conclusions

In this paper, a secure multidimensional data aggregation scheme is proposed, which uses the Horner rule to deal with polynomials of multidimensional electricity data. The method of certificate aggregation is used to realize the unforgeability of authentication and signature. Time-consuming pairing is reduced to a constant; by adding Laplace noise to the community gateway to achieve ε - differential privacy to resist differential attacks; through performance analysis, the scheme's computational and communication overhead is improved.

Acknowledgments

This work was supported by NSFC Grants (No.61772327 No.61202020 No.61532021), Project of Shanghai Science and Technology Committee Grant (No.15110500700) and CCF-Tencent Open Fund Grant (No.IAGR20150109, RAGR20150114). We would like to express our gratitude to the anonymous reviewers for their valuable feedback and comments which helped us to improve the quality and presentation of this paper.

References

[1] A. Abdallah and X. Shen, "Lightweight security and privacy preserving scheme for smart grid customer-side networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064–1074, 2017.

[2] M. Badra and S. Zeadally, "An improved privacy solution for the smart grid," *International Journal of Network Security*, vol. 18, pp. 529-537, 2016.

[3] H. Bao and R. Lu, "A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 1–16, 2015.

[4] P. Barbosa, A. Brito and H. Almeida, "A technique to provide differential privacy for appliance usage in

Table 5: Comparison of communication overhead

	Our scheme	**Shen's scheme**	**Lu's scheme**
$U \rightarrow BGW$	2272	2308	2308
$BGW \rightarrow DGW$	2272	2308	
$DGW \rightarrow OC$	2272	2308	2308

smart metering," *Information Sciences*, vol. 370-371, pp. 355–367, 2016.

[5] L. Chen, R. Lu, Z. Cao, K. Alharbi and X. Lin, "Muda: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Networking and Applications*, vol. 8, no. 5, pp. 1–16, 2014.

[6] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of MODELS of Computation*, pp. 1–19, 2008.

[7] C. Dwork, F. Mcsherry and K. Nissim, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference*, pp. 265–284, 2006.

[8] C. I. Fan, S. Y. Huang and Y. L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666–675, 2013.

[9] S. Fu, J. Ma, H. Li and Q. Jiang, "A robust and privacy-preserving aggregation scheme for secure smart grid communications in digital communities," *Security & Communication Networks*, vol. 9, no. 15, pp. 2779–2788, 2016.

[10] D. He, N. Kumar and J. H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Networks*, vol. 22, no. 2, pp. 491-502, 2016.

[11] D. He, S. Zeadally, H. Wang and Q. Liu, "Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography," *Wireless Communications & Mobile Computing*, vol. 2017, pp. 1–11, 2017.

[12] L. Huimin, L. Hongmei, W. Haimin and Z. Jinhui, "An efficient certificate-based aggregate short scheme," *Journal of Ningxia University(Nature Science Edition)*, no. 1, pp. 52–57, 2017.

[13] K. Kursawe, G. Danezis and M. Kohlweiss, "Privacy-Friendly Aggregation for the Smart-Grid", in *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 175-191, 2011.

[14] J. Lee and C. Clifton, "How much is enough? choosing e for differential privacy," in *International Conference on Information Security*, pp. 325–340, 2011.

[15] F. Li, B. Luo and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *International Journal of Security & Networks*, vol. 6, no. 1, pp. 28–39, 2011.

[16] H. Li, X. Lin, H. Yang, X. Liang, R. Lu and X. Shen, "Eppdr: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel & Distributed Systems*, vol. 25, no. 8, pp. 2053–2064, 2014.

[17] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel & Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[18] S. Nath and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *ACM SIGMOD International Conference on Management of Data*, pp. 735–746, 2010.

[19] H. Shen, M. Zhang and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 6, pp. 1369–1381, 2017.

[20] R. Singh and M. S. Manu, "An energy efficient grid based static node deployment strategy for wireless sensor networks," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 32-40, 2017.

[21] X. Tian, L. Li, J. Li, H. Li, and C. Gu, "Secret share based program access authorization protocol for smart metering," *International Journal of Network Security*, vol. 18, no. 6, pp. 1071–1079, 2016.

[22] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[23] J. Xu, Z. Zhang and D. Feng, "Id-based aggregate signatures from bilinear pairings," *Lecture Notes in Computer Science*, vol. 3810, pp. 110–119, 2005.

[24] H. Xiong, Z. Qin and F. Li, "Identity-based threshold signature secure in the standard model," *International Journal of Network Security*, vol. 10, no. 1, pp. 75–80, 2010.

[25] T. xiuxia, L. lisha, S. Chaochao and L. D. Ming, "Review on privacy protection approaches in smart meter," *Journal of East China Normal University(Nature Science)*, no. 5, pp. 46–60, 2015.

[26] H. Zhou, J. Chen, Y. Y. Zhang and L. J. Dang, "A multidimensional data aggregation scheme in multi-level network in smart grid," *Journal of Cryptologic Research*, vol. 4, no. 2, pp. 114–132, 2017.

Biography

Xiuxia Tian Professor, received the MS degree in applied cryptography-based information security from Shanghai Jiaotong University in 2005, and the PhD degree in database security and privacy preserving in cloud computing from Fudan University in 2011. She is currently a professor in the College of Computer Science and Technology, Shanghai University of Electric Power. She is a visiting scholar of two years at UC Berkeley working with groups of SCRUB and SecML. She has published more than 40 papers and some papers are published in international conferences and journals such as DASFAA, ICWS, CLOUD, and SCN. Her main research interests include database security, privacy preserving (large dataand cloud computing), applied cryptography, and secure machine learning.

Qian Song Graduate, College of Computer Science and Technology in Shanghai University of Electric Power. Her research interests mainly focus on the security and privacy protection for the smart meter.

Fuliang Tian Graduate, Graduate. College of Computer Science and Technology in Shanghai University of Electric Power. He research interests mainly focus on the security and privacy protection for the smart meter. Email: tianflxs@163.com.

Secure Cloudlet-Based eHealth Big Data System With Fine-Grained Access Control and Outsourcing Decryption from ABE

Kittur Philemon Kibiwott[1], Zhang Fengli[1], Omala A. Anyembe[2], Daniel Adu-Gyamfi[3]

(Corresponding author: Kittur Philemon Kibiwott)

School of Information and Software Engineering, University of Electronic Science and Technology of China[1]

No. 2006, Xiyuan Ave, West Hi-Tech Zone, Chengdu, Sichuan 611731, China

(Email: phkibiwott@gmail.com)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[2]

University of Energy and Natural Resources, Ghana[3]

(Received June 19, 2017; revised and accepted Sept. 27, 2017)

Abstract

Integration of cloud computing and mobile computing with the proliferation of big data is making remarkable strides in the health care industry. Aside the benefits accrued from adopting this technologies, there are myriad of challenges to overcome such as confidentiality of data outsourced to the cloud, integrity of stored data, wide area network (WAN) latency delays, and the resource constraints of the mobile devices. In this paper we propose a Cloudlet-Based eHealth Big Data System with Outsourced Decryption (CBe-BDS-OD) to address the above challenges. To accommodate mobile devices with limited resources, the computation power is borrowed from the cloudlet server securely. Security analysis demonstrates that our scheme is secure. In addition, our performance approach through theory analysis and experimental simulation indicates a substantial improvement in computation efficiency by 99% and therefore the scheme can be deployed in resource-constrained mobile devices.

Keywords: Big Data; Cloud Computing; Cloudlet; eHealth; Outsourcing; Resource-constrained Device

1 Introduction

Big data describes a massive volume of both structured and unstructured data that are beyond the processing capability of traditional software and database techniques. Big data is grouped into four (4) major features commonly known as "4 Vs of Big data" thus Volume "scale of data", Velocity "analysis of streaming data", Variety "data in different forms" [10] and Veracity "uncertainty of data"[IBM]. The fifth other feature include Value "discoverable behavior of data" [ORACLE]. The high volume eHealth data is generated by different sources which include biometric devices, networked sensors, RFID, mobile devices (*i.e.* with Bluetooth and GPS etc) and others such as hospital systems, for instance, the adoption of Electronic Health Record (EHRs) and Electronic medical records (EMRs) [26, 32]. These are the major sources of eHealth big data. While big data has benefits attached to, it requires a large computation and storage [33] capacity, with which resource-constrained devices (*i.e.* with less storage, battery life, computation power) [16] like mobile smartphones do not have and hence leading to the leveraging of cloud to store such volume of data [23, 30].

Due to elastic scaling provided by the cloud [18], now big data can be stored [33] an edge which cloud has over traditional storage. This means the organization's data is outsourced to a third party on utility costing basis [22]. But cloud has notable limitations including requirement of fast, reliable internet connectivity and high latency [29]. For real time applications like in healthcare, the adoption of cloud computing achieves less because its located far away from the mobile users and incurs long WAN latency delays making inefficient [1, 23, 30] and therefore hurts the mobile 'thin clients'. The cloudlet concept was introduced in [29] to solve these issues. A cloudlet which is also referred to as mini cloud, can be considered as a "data center in a box" whose objective is to bring the cloud closer to the user [30] as shown in Figure 1. It is a resource-rich server with Internet access that is well connected to mobile devices via a high-speed local area network (LAN) [23]. Mobile devices can migrate expensive computations to the cloudlet stationed on discoverable, localized, stateless servers running on single or multiple virtual machines (VMs) [1]. As a result, it preserves mo-

bile device battery, provides a more powerful computation, enhances flexibility and mobility [16]. During task migration, mobile device does not need to communicate with the Cloud directly instead it communicates with the closest cloudlet [29].

Many works have been proposed to overcome the storage limitations of massive data, where data is now outsourced to the cloud. However, practical adoption of those techniques, poses security and privacy challenges [15, 22, 25]. To overcome these, the data needed to be shared are encrypted before they are uploaded to the cloud, and fine-grained access control should be enforced [31]. An Attribute Based Encryption technique proposed by Sahai and Waters [28] enables the data owners to encrypt their data such that only end users that satisfy given criteria can, perhaps, succeed in decrypting the data. In ABE scheme [28], private key can decrypt a given ciphertext only if the associated attributes and access policy tally. There are two flavours of ABE schemes: Key-Policy ABE (KP-ABE) [13] and Ciphertext-Policy ABE (CP-ABE) [2, 31]. In KP-ABE scheme, each ciphetext are labeled with sets of descriptive attributes and the access policy of this attributes are associated with end user's private key.

Decryption is realized only if the attributes on the ciphertext satisfy the access policy of the user's private key [13]. While in CP-ABE scheme, each ciphertext is associated with an access policy, and every end user's private key is associated with a set of descriptive attributes. To rightly recover the message, the attributes in the user's private key need to satisfy the access policy [2, 31]. ABE is one of the powerful cryptographic tool for realizing fine grained data access control in the cloud storage system [24, 28]. However, with the majority of ABE schemes, the major drawback is inefficiency since the size of ciphertext and decryption overhead (number of pairing operations) grow with the complexity of the access policy [17]. This becomes a bottleneck when ABE runs on the resource-constrained device's applications for example on smartphones applications [6, 21, 25].

To minimize the workload operations on the end user's side while executing decryption algorithm, Green *et al.* [11] proposed a scheme where expensive computation operations is offloaded to the third-party. In this scheme, a key blinding technique (*i.e.* transformation key) TK is sent to the third-party (proxy) for translation of any ciphertext CT satisfied by end user's attributes or access policy into a simple ciphertext CT'. The end user incurs minimal overhead to recover plaintext from transformed ciphertext CT' [14, 19] using the retrieving key RK. While carrying out this, the proxy cannot learn any information about the original plaintext. In [5], Chase proposed a multi-authority ABE scheme which is secure against selective ID security model. To avoid a single authority issuing keys which can lead to key compromise, decentralized key-policy attribute-based encryption with privacy preserving was proposed in [12] and decentralized CP-ABE with fully hidden access structure was proposed in [27]. The scheme proposed in [11] provides fine-grained access control solution to the resource-constrained devices such as mobile phones in the cloud. However, in our scheme we introduce a new architecture where cloudlet is stationed between mobile device user and cloud as shown in Figure 1. This means the security infrastructure has to be modified also. In our work each mobile user with attribute list $\boldsymbol{F}$ is associated with a private key/decrypt$_{out}$ key while the cloudlet is labeled with access policy $\mathbb{P}$ which describes the rightful users of the data.

The main contribution of this paper can be summarized as follows:

1) Our CBe-BDS-OD proposed scheme, introduces an efficient encryption for a cloudlet that achieves confidentiality, collusion resistance and integrity of data based on ciphertext policy-attribute based encryption.

2) To minimize the pairing load operations on end user's side with resource-constrained devices and thereby reducing expensive computation, we adopted server-aided transformation where the computational processing power is borrowed from the server by the mobile user. The mobile cloudlet server provided with blinding key, transforms the complex ciphertext into a simple one. In the process of performing this, the mobile cloudlet server cannot reveal anything about the underlying plaintext.

3) We have implemented our scheme to evaluate the performance. The results in our protocol with server-aided decryption demonstrate a substantial improvement in computation efficiency by 99% at the end user's side compared to its counterpart and therefore can be deployed in resource-constrained mobile devices.

The rest of this paper is organized as follows: In Section 2 we give the preliminaries related to our proposal. In Section 3 we provide our scheme proposal which is IND-AND-sAS-CCA2 secure for CP-ABE with outsourced decryption for eHealth big data in cloudlet computing, we also give the IND-AND-sAS-CCA2 security model. In Section 4 we give concrete construction for our scheme. Thereafter we give security proof for our proposal defined in our proposed IND-AND-sAS-CCA2 security model in Section 5 and in Section 6 we give experiment and analysis results. Lastly we give our conclusion.

2 Preliminaries

2.1 Bilinear Maps

Let $\mathbb{G}$ and $\mathbb{G}_\tau$ be two multiplicative cyclic groups of prime order p. Let g_1, g_2 be generators of $\mathbb{G}$ and e be a bilinear map; e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Bilinear map e has the following properties:

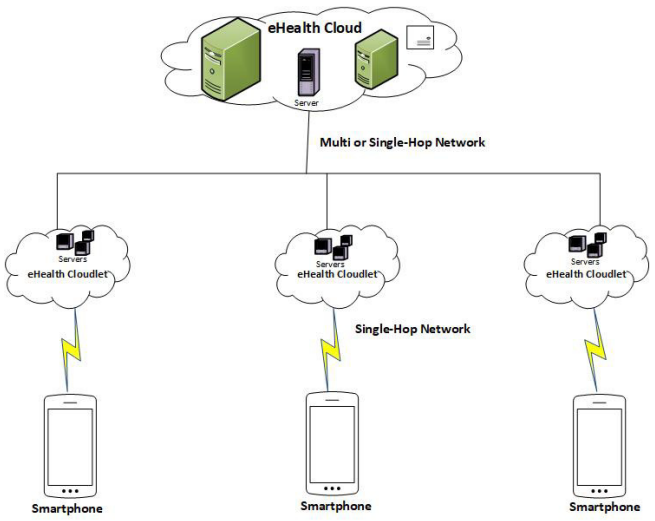


Figure 1: Three-tier architecture; Mobile device-eHealth; Cloudlet-eHealth cloud

1) *Bilinearity* : $\forall g_1, g_2 \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$ we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} = e(g_1^b, g_2^a)$.
2) $Non - degeneracy : e(g_1, g_2) \neq 1$.
3) *Computability*: There is an efficient algorithm to compute $e(g_1, g_2)$.

2.2 Definition of Access Structures

Our proposed Protocol is based on AND-gates multi-valued attributes [8].

Definition 1. *Access structure [8]:*
We let $\mathcal{U} = \{a_1, a_2, ...a_n\}$ *be a set of attributes. For* $a_i \in \mathcal{U}$ *the set of possible values is denoted as* $\mathbb{A}_i = \{q_{i,1}, q_{i,2}, ...q_{i,n_i}\}$, *where* n_i *is the size of possible values for* a_i. *We let* $F = F_1, F_2, .., F_n$, *where* $F_i \in \mathbb{A}_i$ *be an attribute list for a user, and* $\mathbb{P} = \mathbb{P}_1, \mathbb{P}_2, ..., \mathbb{P}_n$, $\mathbb{P}_i \in \mathbb{A}_i$ *be an access structure. From the notation* $F \vDash \mathbb{P}$, *an attribute list* F *is satisfying an access structure* $\mathbb{P}$ *where* $F_i = \mathbb{P}_i (i = 1, 2, .., n)$.

The size of the access structures corresponds to $\prod_{i=1}^{n} n_i$. *In every* a_i, *the hospital has to demonstrate a status* $q_{i,*}$ *from* $\mathbb{A}_i = \{q_{i,1}, q_{i,2}, ...q_{i,n_i}\}$.

2.3 Taget-collision Resistant Hashing [7]

A function H: X→ Y is a target-collision resistant(TCR) hash function if given a random preimage x∈ X it is hard to realize x′≠x with H(x′)=H(x).

2.4 The Decisional Bilinear Diffie-Hellman (DBDH) Assumption [28]

Let $x,y,z,c \in \mathbb{Z}_p^*$ be randomly chosen and g be a generator of $\mathbb{G}$. The decisional BDH assumption [28] is that no probabilistic polynomial-time $\mathbb{AD}$ can distinguish the tuple$(g, X = g^x, Y = g^y, Z = g^z, e(g,g)^{xyz})$ from the tuple $(g, X = g^x, Y = g^y, Z = g^z, e(g,g)^c)$ with more than a negligible advantage. An algorithm $\mathbb{AD}$ has advantage of ϵ in solving DBDH problem in $\mathbb{G}$ if $Adv_{DBDH}(\mathbb{AD}) := |Pr[\mathbb{AD}(g, g^x, g^y, g^z, e(g,g)^{xyz}) = 0] - Pr[\mathbb{AD}(g, g^x, g^y, g^z, e(g,g)^c) = 0]| > \epsilon$.

We say that the DBDH assumption holds in $\mathbb{G}$ and $\mathbb{G}_\tau$ if ϵ is negligible.

2.5 The Modified Decisional Diffie-Hellman (MDDH) Assumption [34]

Let $x, y, z \in \mathbb{Z}_p^*$ be randomly chosen and g be a generator of $\mathbb{G}$. The Modified DDH assumption [34] is that no probabilistic polynomial-time adversary $\mathbb{AD}$ can distinguish the tuple$(g, X = g^x, B = e(g,g)^y, C = e(g,g)^{xy})$ from the tuple $(g, A = g^x, B = e(g,g)^y, C = e(g,g)^z)$ with more than a negligible advantage. An algorithm $\mathbb{AD}$ has advantage ϵ in solving MDDH problem in $\mathbb{G}$ if $Adv_{MDDH}(\mathbb{AD}) := |Pr[\mathbb{AD}(g, g^x, e(g,g)^y, e(g,g)^{xy}) = 0] - Pr[\mathbb{AD}(g, g^x, e(g,g)^y, e(g,g)^z) = 0]| > \epsilon$.

We say that the MDDH assumption holds in $\mathbb{G}$ and $\mathbb{G}_\tau$ if ϵ is negligible.

2.6 Notations

For convenience and better understanding the notations used in our protocol and their description is as shown in Table 1.

Table 1: Notations

ACRONYM	DESCRIPTION
$\mathcal{U}$	Attribute universe
$\mathbb{P}$	Access structure
$\mathbb{A}$	Set of attributes
AA	Attribute Authority
ISP	Internet Service Provider
M	Message
CT	CipherText
MSK	Master Secret Key
PK	Public Key
SK	Private Key
TK	Transformation Key
RK	Retrieval key
k	length of a string
$\oplus$	An exclusive-OR(XOR)
CSP	Cloud Service Provider
H_1, H_2, H_3	Three hash functions
F	Attribute list

2.7 Generic ABE Definition [28]

There are two variants of ABE schemes; key-policy ABE (KP-ABE)[13] and ciphertext policy ABE (CP-ABE) [2, 31]. Each ciphertext is associated with a set of attributes and each secret key is associated with an access policy for the case of KP-ABE while in CP-ABE, the attribute

sets are associated with secret keys and access policies are associated with ciphertext.

Definition 2. *Attribute-Based Encryption (ABE) [28, 21]: ABE has an attribute universe defined by $\mathcal{U}$ with access structure $\mathbb{P}$ and is described using the following polynomial-time algorithms:*

Setup(1^{β},$\mathcal{U}$) $\rightarrow$ (PK, MSK): *This algorithm acquires as an input a security parameter β and an attribute universe $\mathcal{U}$ and yields a public key PK and a master secret key MSK.*

KeyGen(PK,MSK,$L_{key}$$\rightarrow$SK: *The algorithm acquires as input public key PK, the master secret key MSK and list of descriptive attributes $L_{key} \in \mathbb{P}$ for key generation in the case of KP-ABE and $L_{key} \subseteq \mathcal{U}$ for the case of CP-ABE. It yields the secret key SK.*

Encrypt(PK,m,L_{enc})$\rightarrow$$CT$: *This algorithm acquires as input a public key parameter PK, a message m, and an attribute list $L_{enc} \subseteq \mathcal{U}$ for KP-ABE or $L_{enc} \subseteq \mathbb{P}$ for CP-ABE. It yields ciphertext CT.*

Decrypt$(SK, CT) \rightarrow m$**:** *This algorithm acquires as input secret key SK and a ciphertext CT. It yields message m if the function G(L_{key},L_{enc})=1 holds, otherwise yields $\perp$.*

Correctness.
$\forall$(PK,MSK)$\leftarrow$Setup(1^{β},$\mathcal{U}$),$SK \leftarrow$KeyGen(PK, MSK, L_{key}), $\forall m$ in message space, if G(L_{key},L_{enc})=1 holds, m=Decrypt(SK,Encrypt(PK,m,L_{enc}).

2.8 Attribute-Based with Outsourcing Decryption [11]

Has the following polynomial-time algorithms:

Setup(1^{β},$\mathcal{U}$): Takes as an input a security parameter β and a universe $\mathcal{U}$. It yields public parameters PK and master key MSK.

Encrypt(PK,m,(A,ρ)): Takes as an input public parameter PK and a message m to be encrypted. It also takes as input LSSS access structure(A,ρ). It yields ciphertext CT.

KeyGen$_{out}$(MSK,S): Takes as input master key MSK and set S. It yields transformation key TK and a secret key SK.

Transform$_{out}$(TK,CT): Takes as input transformation key TK and ciphertext CT. It yields CT$'$.

Decrypt$_{out}$(SK,CT$'$): Takes as input a secret key SK and transformed ciphertext CT$'$. yields message m.

3 Our Secured CP-ABE with Outsourced Decryption in Cloudlet Computing

3.1 Algorithm Definition

Our new scheme consist of seven algorithms as in [14]:

Setup(1^{β},$\mathcal{U}$): This algorithm takes as input security parameter β and universe $\mathcal{U}$. It returns as an output public parameter PK and master secret key MSK.

KeyGen(PK,MSK,F): This algorithm takes as input public parameter PK, master key MSK and a set F. Returns as an output private key SK_F.

Encrypt(PK,m,$\mathbb{P}$): This algorithm takes as input public parameters PK, message m and access structure $\mathbb{P}$. Returns as an output the ciphertext CT.

Decrypt(PK,SK$_F$,CT): Takes public parameter PK, private key SK_F for the list F. Returns as an output message m if SK_F associated with F satisfies $\mathbb{P}$

TKGen$_{out}$(PK,SK$_F$): This algorithm takes as input public parameter PK and private key SK$_F$ associated with list F. It returns as an output transformation key TK_F associated with F and its corresponding retrieving key RK_F.

PartialDecrypt$_{out}$(PK,TK$_F$,CT): This algorithm takes as an input public parameter PK, transformation key TK_F and ciphertext CT. Returns as an output partially decrypted ciphertext CT'.

Decrypt$_{out}$(PK,RK$_F$,CT,CT$'$): This algorithm takes as an input public parameter PK,retrieving key RK_F, ciphertext CT and transformed ciphertext CT'. Returns as an output message m.

Correctness:

1) $Decrypt(PK, SK_F, Encrypt(PK, m, \mathbb{P})) = m$

2) $Decrypt_{out}(PK, RK_F$,PartialDecrypt(Encrypt(PK, m, $\mathbb{P}$),PK, TK_F))=m

3.2 Definition of Security Model

We define security notions in this section. We propose **selective AND access structure and chosen ciphertext security**(IND-AND-sAS-CCA2) game in our CBeBDS-OD scheme. We have two kinds of chosen ciphertext variants similar to [20, 34]:

1) The challenge ciphertext is original.

2) The challenge ciphertext is server-aided.

3.2.1 The challenge ciphertext is original

Init: The adversary $\mathbb{AD}$ sends challenge access structure $\mathbb{P}^*$ to the challenger $\mathbb{BD}$.

Setup: Challenger $\mathbb{BD}$ invokes setup algorithm to obtain public parameter (PK) and master secret key(MSK). $\mathbb{BD}$ then sends PK to the adversary $\mathbb{AD}$ and keeps MSK secret.

Phase 1: In the find stage $\mathbb{AD}$ has access to the following oracles queries:

Private Key query oracle $\mathcal{OR}_{SK_F}$, for the attribute list $F \not\models \mathbb{P}^*$: $\mathbb{BD}$ runs $SK_F \leftarrow$ Keygen(PK, MSK, F). The challenger then sends the private key SK_F to $\mathbb{AD}$.

Partial decryption key query oracle $\mathcal{OR}_{TK}$, for the attribute list F: On input F and access structure $\mathbb{P}^*$, challenger $\mathbb{BD}$ returns equivalent transformation key TK_F.

Retrieving key query oracle $\mathcal{OR}_{RK}$, for attribute list F: Challenger $\mathbb{BD}$ returns equivalent retrieving key RK_F on input of F.

Partial decryption query oracle $\mathcal{OR}_{PDec}$, for attribute list F and ciphertext $\boldsymbol{CT}$: On input of ($\boldsymbol{CT}$, F), $\mathbb{BD}$ outputs PartialDecrypt$_{out}$($\boldsymbol{PK}$,TK_F,$\boldsymbol{CT}$).

Decryption query oracle $\mathcal{OR}_{Dec}$, for attribute list F and ciphertext $\boldsymbol{CT}$. $\mathbb{BD}$ invokes $\boldsymbol{m}\leftarrow$Decrypt(PK, SK_F, CT), where $SK_F \leftarrow$Keygen(PK, MSK, F) and $F \models \mathbb{P}^*$ if the input ciphertext is original. Otherwise $\boldsymbol{m}\leftarrow$ Decrypt(PK, RK_F, CT) where $RK_F \leftarrow (SK_F, F)$ if ciphertext is server-aided. $\boldsymbol{m}$ is send to $\mathbb{AD}$.

Challenge: $\mathbb{AD}$ submits two plaintext messages m_0^* and m_1^* of equal length from the message space M and the access policy $\mathbb{P}^*$ on which it wishes to challenge with the constraint that F cannot satisfy $\mathbb{P}^*$. $\mathbb{BD}$ flips a random coin γ to choose $\gamma\in\{0,1\}$ and encrypts m_γ^* under the access structure $\mathbb{P}^*$ *i.e.* CT^*=*Encrypt(PK,*m_γ^**,*$\mathbb{P}^*$*)*. Then $\mathbb{BD}$ sends the challenge ciphertext CT^* to $\mathbb{AD}$.

Phase 2: $\mathbb{AD}$ maintains query as in *phase 1* adaptively for private key, transformation key, retrieving key, decryption and decryption$_{out}$ with the following constraints:

1) $\mathbb{AD}$ should not make private key query that results in attribute list F that will satisfy access policy $\mathbb{P}^*$.
2) $\mathbb{AD}$ should not trivially issue decryption queries.

Guess: The adversary $\mathbb{AD}$ gives $\gamma'\in\{0,1\}$ for γ and wins the game if $\gamma'=\gamma$. $|\Pr(\gamma'=\gamma)\text{-}\frac{1}{2}|$ is defined as the advantage for adversary $\mathbb{AD}$ in the game.

Definition 3. *Cloudlet-Based eHealth Big Data System with Outsourced Decryption (CBe-BDS-OD) is said to be IND-AND-sAS-CCA2-or secure*[1] *if for all polynomial adversaries the advantage* $\boldsymbol{Adv}_{CBe-BDS-OD}^{IND-AND-sAS-CCA-or}(\beta)$ *is negligible.*

The challenge ciphertext is server-aided:

Phase 1: Similar to the one of original challenge ciphertext.

Challenge: $\mathbb{AD}$ submits two plaintext messages m_0^* and m_1^* of equal length derived from the message space M and the access policy $\mathbb{P}^*$ which it wishes to challenge with the constraint that F has not been used to query $\mathcal{OR}_{RK}$. $\mathbb{BD}$ flips a random coin γ to choose $\gamma\in\{0,1\}$ and sets CT^*=(TK^*,Encrypt(PK, m_γ^*, F^*)). Then $\mathbb{BD}$ sends the challenge ciphertext CT^* to $\mathbb{AD}$.

Phase 2: Nearly similar to *phase 1* with the following restrictions:

$$\mathcal{OR}_{TK} : F = F^*$$
$$\mathcal{OR}_{Dec} : CT = CT^* \quad \text{also} \quad F = F^*.$$

Guess: Similar to that in original challenge ciphertext scenario. $|\Pr(\gamma'=\gamma)\text{-}\frac{1}{2}|$ is defined as the advantage for adversary $\mathbb{AD}$ in the game.

Definition 4. *Cloudlet-Based eHealth Big Data System with Outsourced Decryption (CBe-BDS-OD) is said to be IND-AND-sAS-CCA2-sa secure*[2] *if for all polynomial adversaries the advantage* $\boldsymbol{Adv}_{CBe-BDS-OD}^{IND-AND-sAS-CCA2-sa}(\beta)$ *is negligible.*

3.3 System Model

In this Section we give some intuition for the idea behind our scheme. Our scheme is partly based on scheme [8]. To realize outsourced decryption, our scheme partially follows [11, 34]. The hospital encrypts the data with public key PK_i. After which it outsources the encrypted data to the cloud for storage. Mobile device does not need to communicate with the Cloud directly instead it communicates with the closest cloudlet [29]. The mobile user offloads some intensive tasks to the cloudlet by letting it do partial decryption using token key (TK). Final decryption is carried out by the user using retrieving key RK. To achieve CCA2 security in our protocol we follow [4, 9] where decryptor is allowed to check whether the ciphertext is valid;

1) Before proxy transforms the original ciphertext by employing [4].
2) Before end user does final decryption utilizing [9].

[1] or stands for original
[2] sa stands for server-aided

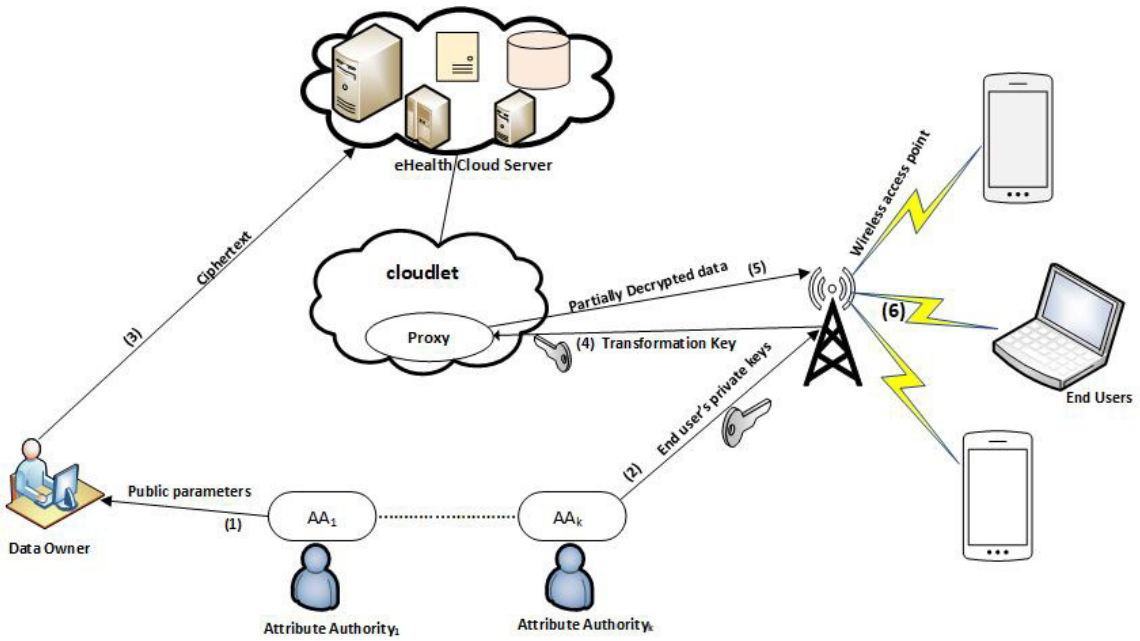


Figure 2: System model

We employ a cloudlet storage system that has multiple authorities as shown in Figure 2. The model has the following entities: cloud server, cloudlet, proxy, Trusted Authority/ authorities (AA), hospital, users.

1) *Trusted Authority (TA)*: Also referred to as an Attribute Authority (AA). It generates system public and secret keys. It is the only entity fully trusted by all other entities participating in the system. TA is used interchangeably with AA.

2) *Cloud server:* Cloud server stores eHealth big data for the hospital and also offers access service of data to the users.

3) *Cloudlet:* Cloudlet is located closer to mobile users.It hosts the offloaded tasks.

4) *Proxy:* Performs outsourced decryption for eHealth data user. It reduces the decryption load on users with resources-constrained devices.

5) *Hospital:* Describes the access policies and encrypts its data under those policies before sending them to the cloud.

6) *Users:* The user that uses resource-constrained device is assigned with the key and can access the ciphertext freely from the cloudlet.They can recover the plaintext only when its attributes satisfy the access policy stated in the ciphertext.

3.4 Threat Model

Users need solid assurance of the existence of adequate security and privacy aspects in cloud before trusting their data to it. In this subsection, we put into account the possible attackers and their corresponding attacks to our proposed protocol. Since cloudlet is closer to the user, fierce attacking can be realized than ever (active attacks). In addition, cloudlet proxy is assumed to be honest but curious (passive). It may deviate from the scheme specifications norms and may try to acquire as much private information as possible. To obtain the key to access data which individually could not access, authorized users can collude by combining their attributes (inner threats). Furthermore, the proxy can collude with unauthorized users to obtain some data. Integrity is another major issue as data may be mutated or get corrupted. The user must verify the integrity of outsourced data before decrypting.

3.5 Design Goals

Based on the possible attacks discussed in the preceding subsection our system achieves the following design security goals:

1) Confidentiality: The cloudlet service provider and malicious users cannot recover encrypted data without the owners consent. As shown by our system in Figure 2, only intended users are able to decrypt their messages. This ensures the privacy of the owner's data in storage, during partial decryption and final decryption.

2) Integrity: Our system verifies the correctness of original and transformed ciphertext.

3) Minimal overhead: Due to the resource-constraints in mobile devices, minimal overhead costs must be

provided during the time both of computation and communication.

4 Main Construction

As mentioned in Subsection 3.3 above, our CBe-BDS-OD is based on [8]. To realize outsourced decryption it follows partly [11, 34].

Our new scheme is composed of seven algorithms as in [14]:

Setup(1^β,$\mathcal{U}$): This algorithm takes as input security parameter β and universe $\mathcal{U}$. A trusted authority(TA) chooses a pairing group $\mathbb{BG}$=(p,e,$\mathbb{G}$,$\mathbb{G}_\tau$), two generators $g, h \in \mathbb{G}$, then selects two elements $b \in_R \mathbb{Z}_p$ and $\upsilon_{i,j} \in_R \mathbb{Z}_p (i \in [1,n], j \in [1,n_i])$. Trusted Authority furthermore computes $\mathbb{Y} = e(g,h)^b$ and $V_{i,j} = g^{\upsilon_{i,j}} (i \in [1,n], j \in [1,n_i])$ and selects the following TCR hash functions:

$$H_1 : \{0,1\}^* \to \mathbb{Z}_p^*,$$
$$H_2 : \mathbb{G}_\tau \to \{0,1\}^{2k},$$
$$H_3 : \{0,1\}^* \to \mathbb{G}.$$

It publishes public parameters $PK = (g,\ h,\ e,\ \mathbb{Y},\ V_{i,j},\ H_1,\ H_2,\ H_3)$ and master secret key $MSK = (b, \{\upsilon_{i,j}\}_{i\in[1,n],j\in[1,n_i]})$. Note that $\forall F, F' (F \neq F'), \sum_{q_{i,j}\in F} \upsilon_{i,j} \neq \sum_{q_{i,j}\in F'} \upsilon_{i,j}$ is assumed.

KeyGen(PK, MSK, F): This algorithm takes as input public parameter PK, master key MSK and a set F. TA then choses $\alpha \in \mathbb{Z}_p^*$. Next he sets

$$\begin{aligned} K_1 &= h^b (g^{\sum_{q_{i,j}\in F} \upsilon_{i,j}})^\alpha. \\ K_2 &= g^\alpha \\ SK_F &= (K_1, K_2). \end{aligned}$$

Encrypt($PK, m, \mathbb{P}$): This algorithm takes public parameters PK, message $m \in \{0,1\}^k$ and access structure $\mathbb{P}$ as input. The encryption algorithm works as follows.

1) Hospital chooses $\lambda \in \{0,1\}^k$ and sets $s = H_1(\mathbb{P}, m, \lambda)$, then it computes,

$$\begin{aligned} B_1 &= H_2(e(g,h)^{b.s}) \oplus (m \| \lambda) \\ B_2 &= g^s \\ B_3 &= (\prod_{q_{i,j}\in\mathbb{P}} V_{i,j})^s \\ B_4 &= h^s. \end{aligned}$$

Finally hospital computes $E = H_3(\mathbb{P} \| B_1 \| B_2 \| B_3 \| B_4)^s$.

2) The hospital then generates $\boldsymbol{CT}$=($\mathbb{P}$, B_1, B_2, B_3, B_4, E) then it sends to the cloud.

TKGen$_{out}$(PK, SK_F): This algorithm takes as input public parameter PK and private key SK_F associated with set F. Token key generation works as follows:
The user chooses $\sigma \in \mathbb{Z}_p^*$ then generates a partial decryption key pair as: $TK_F = (K'_{T1}, K'_{T2})$ where

$$\begin{aligned} K'_{T1} &= K_1^{1/\sigma} \\ K'_{T2} &= K_2^{1/\sigma}. \end{aligned}$$

Retrieving key is $RK_F = \sigma$.

It returns as an output transformation key TK_F associated with F and corresponding retrieving key RK_F.

PartialDecrypt$_{out}$(PK, TK_F, CT): This algorithm is executed by CSP. It takes as input public parameter PK, transformation key TK_F and ciphertext CT the proxy confirms first whether

$$\begin{aligned} e(B_2, h) &\stackrel{?}{=} e(g, B_4), \\ e(B_2, H_3(\mathbb{P}\|B_1\|B_2\|B_3\|B_4)) &\stackrel{?}{=} e(g, E), \\ e(\prod_{q_{i,j}\in\mathbb{P}} V_{i,j}, B_2) &\stackrel{?}{=} e(B_3, g), \\ F &\models \mathbb{P}. \end{aligned} \quad (1)$$

If does not hold it aborts with $\perp$, otherwise calculates the following:

$$\begin{aligned} T' &= \frac{e(B_2, K'_{T1})}{e(B_3, K'_{T2})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} \upsilon_{i,j}})^{\alpha/\sigma})}{e((\prod_{q_{i,j}\in\mathbb{P}} V_{i,j})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} \upsilon_{i,j}})^{\alpha/\sigma})}{e((\prod_{q_{i,j}\in\mathbb{P}} g^{\upsilon_{i,j}})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} \upsilon_{i,j}})^{\alpha/\sigma})}{e((g^{\sum_{q_{i,j}\in\mathbb{P}} \upsilon_{i,j}})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g,h)^{s.b/\sigma}.e(g,g)^{\alpha.s/\sigma \sum_{q_{i,j}\in F} \upsilon_{i,j}}}{e(g,g)^{\alpha.s/\sigma \sum_{q_{i,j}\in\mathbb{P}} \upsilon_{i,j}}} \\ T' &= e(g,h)^{s.b/\sigma}. \end{aligned}$$

Returns as an output partially decrypted ciphertext $CT' = (B_1, T')$.

Decrypt(PK, SK_F, CT): Since there are two types of ciphertexts likewise two computations are to be carried out.

1) Parsing Original ciphertext as an input.
2) Parsing Server-aided ciphertext *i.e.* transformed data as an input.

Parsing Original ciphertext as an input: The decryption key employed is the private key $SK_F = (K_1, K_2)$ that corresponds to set F. The user confirms

Table 2: Performance evaluation benchmark

Operation	**Notation**	**Time computation in μs**	
		Desktop PC setting	**Smartphone setting**
Exponentiation in $\mathbb{G}_\tau$	T_e	0.067	42
Bilinear Pairing	T_p	16.06	63

the validity of the ciphertext as in PartialDecrypt$_{out}$ above. If it does not hold, he outputs $\perp$, otherwise he proceeds by taking public parameter PK, private key SK_F for the set F and original ciphertext CT then calculates the following.

$$\begin{aligned} T'' &= \frac{e(B_2, K_1)}{e(B_3, K_2)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((\prod_{q_{i,j}\in \mathbb{P}} V_{i,j})^s, g^\alpha)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((\prod_{q_{i,j}\in \mathbb{P}} g^{v_{i,j}})^s, g^\alpha)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((g^{\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}})^s, g^\alpha)} \\ &= \frac{e(g,h)^{sb}.e(g,g)^{\alpha.s\sum_{q_{i,j}\in F} v_{i,j}}}{e(g,g)^{\alpha.s\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}}} \\ T'' &= e(g,h)^{sb}. \end{aligned}$$

Computes $m\|\lambda = H_2(T'') \oplus B_1$. Finally it outputs m if $B_1 = H_2(\mathbb{Y}^{H_1(\mathbb{P},m,\lambda)}) \oplus (m\|\lambda)$ holds, otherwise outputs $\perp$.

Parsing Server-aided ciphertext *i.e.* transformed data as an input: The input ciphertext is the partially decrypted one (CT') and decryption key employed here is the retrieving key $RK_F{=}\sigma$ that corresponds to attribute set F. If F satisfies $\mathbb{P}$ then the user computes:

$$m\|\lambda = H_2(T'^\sigma) \oplus B_1.$$

Finally it outputs m if $B_1 = H_2(\mathbb{Y}^{H_1(\mathbb{P},m,\lambda)}) \oplus (m\|\lambda)$ and $\mathbb{Y}^{H_1(\mathbb{P},m,\lambda)} = T'^\sigma$ holds, otherwise outputs $\perp$.

Correctness Analysis
Two faces:

1) Correctness for Original ciphertext.

2) Correctness for Server-aided ciphertext.

Correctness for Original ciphertext:

$$\begin{aligned} T'' &= \frac{e(B_2, K_1)}{e(B_3, K_2)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((\prod_{q_{i,j}\in \mathbb{P}} V_{i,j})^s, g^\alpha)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((\prod_{q_{i,j}\in \mathbb{P}} g^{v_{i,j}})^s, g^\alpha)} \\ &= \frac{e(g^s, h^b(g^{\sum_{q_{i,j}\in F} v_{i,j}})^\alpha)}{e((g^{\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}})^s, g^\alpha)} \\ &= \frac{e(g,h)^{sb}.e(g,g)^{\alpha.s\sum_{q_{i,j}\in F} v_{i,j}}}{e(g,g)^{\alpha.s\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}}} \\ T'' &= e(g,h)^{sb}. \end{aligned}$$

Therefore we have, $H_2(T'') \oplus B_1 = H_2(e(g,h)^{sb}) \oplus (m\|\lambda) \oplus H_2(e(g,h)^{sb}) = m\|\lambda$.

Correctness for Server-aided ciphertext:

$$\begin{aligned} T' &= \frac{e(B_2, K'_{T1})}{e(B_3, K'_{T2})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} v_{i,j}})^{\alpha/\sigma})}{e((\prod_{q_{i,j}\in \mathbb{P}} V_{i,j})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} v_{i,j}})^{\alpha/\sigma})}{e((\prod_{q_{i,j}\in \mathbb{P}} g^{v_{i,j}})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g^s, h^{b/\sigma}(g^{\sum_{q_{i,j}\in F} v_{i,j}})^{\alpha/\sigma})}{e((g^{\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}})^s, g^{\alpha/\sigma})} \\ &= \frac{e(g,h)^{s.b/\sigma}.e(g,g)^{\alpha.s/\sigma\sum_{q_{i,j}\in F} v_{i,j}}}{e(g,g)^{\alpha.s/\sigma\sum_{q_{i,j}\in \mathbb{P}} v_{i,j}}} \\ T' &= e(g,h)^{s.b/\sigma}. \end{aligned}$$

Therefore, $H_2(T'^\sigma) \oplus B_1 = H_2(e(g,h)^{s.b/\sigma)^\sigma} \oplus (m\|\lambda) \oplus$ and $H_2(e(g,h)^{s.b}) = m\|\lambda$.

5 Efficiency Evaluation

In this Section we present the performance evaluation for both original and server-aided proposed schemes in Personal Computer (PC) and Mobile setting environments. For better understanding we defined the following notations: T_e and T_p for pairing exponentiation and bilinear pairing respectively as shown in Table 2. We omitted

scalar multiplication intentionally as its running time is minimal. Our performance evaluation is based on experimental results we carried out in our PC settings with Core i-5 2.5GHz platform processor with memory 4 GB and the Windows XP operating system and for Mobile settings we adopted the experiment results due to [3], where the hardware platform is Samsung Galaxy S2 smartphone with a Dual-core Exynos 4210 1.2GHz processor ARM Cortex-A9 with the Android OS, V2.3(Gingerbread). In PC setting as indicated in Table 3 (PC setting), the total running time of original proposed scheme is 32.12 m/s while in mobile setting Table 4 it is 126 m/s. In Server-aided scheme(PC setting) the total running time is 16.127 m/s while for its counterpart in mobile setting it is 105 m/s. Figure 3 and Figure 4 shows the relative running times of the considered operations for both original and server-aided schemes in PC setting and mobile setting respectively. Based on the above results it is evident that the server-aided scheme is more practical to devices which are resource-constrained in nature.

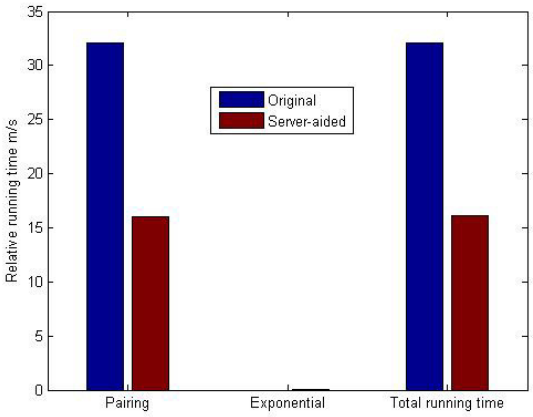


Figure 3: PC setting

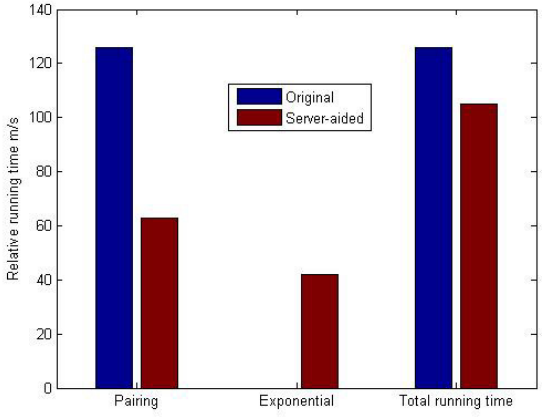


Figure 4: Mobile setting

6 Security Analysis

In our security analysis we show that our CBe-BDS-OD protocol is IND-AND-sAS-CCA2-secure in the definition of our proposed IND-AND-sAS-CCA2 security. The fundamental idea behind our security proof is similar to [34].

Theorem 1. *Suppose the DBDH assumption[28] holds in* $(\mathbb{G}, \mathbb{G}_\tau)$ *and* H_1, H_2, H_3 *are the TCR hash functions, then our CBe-BDS-OD is IND-AND-sAS-CCA2-or secure in the random oracle model.*

Proof. We show that if there exist an adversary $\mathbb{AD}$ that can break the IND-AND-sAS-CCA2-or security of the proposed CBe-BDS-OD scheme then we construct an algorithm $\mathbb{BD}$ using $\mathbb{AD}$ as a subroutine to solve DBDH problem. First DBDH challenger flips a fair coin δ and if δ=0, it sets $(g, X, Y, Z, C) := (g, g^x, g^y, g^z, e(g,g)^{xyz})$; otherwise it sets $(g, X, Y, Z, C) := (g, g^x, g^y, g^z, e(g,g)^c)$ where $x, y, z, c \in \mathbb{Z}_p$ are randomly chosen. The challenger then gives $\mathbb{BD}$ $(g, X, Y, Z, C) := (g, g^x, g^y, g^z, C)$. To be specific $\mathbb{BD}$ will act as a challenger with $\mathbb{AD}$ to play the following IND-AND-sAS-CCA2-or game.

Init: $\mathbb{AD}$ sends the challenge structure $\mathbb{P}^*$ to $\mathbb{BD}$. Let $\mathbb{P}^* = [\mathbb{P}_1^*, ..., \mathbb{P}_n^*]$.

Setup: $\mathbb{BD}$ sets $h = g^\omega$ and $\mathbb{Y} = e(g^x, (g^y)^\omega) = e(g,h)^{xy}$ where $\omega \in \mathbb{Z}_p^*$ is chosen randomly. Furthermore, $\mathbb{BD}$ chooses $\upsilon'_{i,j} \in \mathbb{Z}_p$(where i$\in$ [1,n], j$\in$ [1,n$_i$]). There are two cases: 1) where $q_{i,j} = \mathbb{P}_i^*$ he sets $\upsilon_{i,j} = \upsilon'_{i,j}$. 2) where $q_{i,j} \neq \mathbb{P}_i^*$ sets $\upsilon_{i,j} = y\upsilon'_{i,j}$. Then computes public keys $V_{i,j}$ (where $i \in n[1,n], j \in n_i[1,n_i]$) in the following manner:

$$V_{i,j} = g^{\upsilon_{i,j}} = \begin{cases} g^{\upsilon'_{i,j}}, & \text{where } q_{i,j} = \mathbb{P}_i^* \\ g^{\upsilon_{i,j}}, & \text{where } q_{i,j} \neq \mathbb{P}_i^* \end{cases} \quad (2)$$

$\mathbb{BD}$ then chooses the TCR hash functions as in the actual scheme and sends parameters=(p,$g, h, \mathbb{G}, \mathbb{G}_\tau, e, \mathbb{Y}, V_{i,j}$) to $\mathbb{AD}$. $\mathbb{AD}$ can adaptively query random oracles $H_i (i \in \{1, ., 3\})$ that are controlled by $\mathbb{BD}$. $\mathbb{BD}$ maintains the list $H_i^{List} (i \in \{1,.,3\})$ which originally were empty. If the query has been responded and recorded previously in the list, $\mathbb{BD}$ responds with the same result. $\mathbb{BD}$ response to random oracle queries is as follows:

1) H_1: Upon receiving H_1 query on ($\mathbb{P}^*$,m,λ), $\mathbb{BD}$ first confirms whether there's a tuple $(\mathbb{P}^*, m, \lambda, s)$ in the list H_1^{List}. If it exists it returns the predefined s to $\mathbb{AD}$, where $s \in \mathbb{Z}_p^*$. Otherwise, $\mathbb{BD}$ computes H_1($\mathbb{P}^*$,$m, \lambda) = s$, answers $\mathbb{AD}$ with s, then the tuple $(\mathbb{P}^*, m, \lambda, s)$ is added to the list H_1^{List}.
2) H_2: Upon receiving H_2 query on $RC \in \mathbb{G}_\tau$, $\mathbb{BD}$ first confirms whether there's a tuple(RC, κ_1) in the list H_2^{List}. If it exists it returns κ_1 to $\mathbb{AD}$. Otherwise $\mathbb{BD}$ computes $H_2(RC) = \kappa_1$, answers $\mathbb{AD}$ with κ_1 then the tuple(RC, κ_1) is added to the $H_2^{List}, \kappa_1 \in \{0,1\}^{2k}$.

Table 3: PC setting

	Number of operations and running time (m/s)				
	Exponential		Pairing		
Our scheme	**No.**	**Time(m/s)**	**No.**	**Time(m/s)**	**Total time (m/s)**
Original	0	0	2	32.12	32.12
Server-aided	1	0.067	1	16.06	16.127

Table 4: Mobile setting

	Number of operations and running time (m/s)				
	Exponential		Pairing		
Our scheme	**No.**	**Time(m/s)**	**No.**	**Time(m/s)**	**Total time (m/s)**
Original	0	0	2	126	126
Server-aided	1	42	1	63	105

3) H_3: Upon receiving H_3 query on tuple $(\mathbb{P}^*\|\mathrm{B}_1\|\mathrm{B}_2\|\mathrm{B}_3\|\mathrm{B}_4)$, $\mathbb{BD}$ first confirms whether there exists such tuple $(\mathbb{P}^*\|\mathrm{B}_1\|\mathrm{B}_2\|\mathrm{B}_3\|\mathrm{B}_4, \kappa_2, \eta)$ in the list H_3^{List}, $\mathbb{BD}$ returns the predefined value κ_2 to $\mathbb{AD}$ where $\kappa_2 \in \mathbb{G}, \eta \in \mathbb{Z}_p$. Otherwise $\mathbb{BD}$ computes $\kappa_2 = g^{\eta}$, returns κ_2 to $\mathbb{AD}$ and the tuple $(\mathbb{P}^*\|\mathrm{B}_1\|\mathrm{B}_2\|\mathrm{B}_3\|\mathrm{B}_4, \kappa_2, \eta)$ is added to the list H_3^{List}, $\eta \in \mathbb{Z}_p$.

Furthermore $\mathbb{BD}$ maintains the following lists which originally are empty:

- $SK^{List_{sk}}$ that stores (F, SK_F) tuple which are responds from $\mathcal{OR}_{SK_F}(F)$ queries.
- $TK^{List_{tk}}$ that stores (F, SK_F, TK_F, RK_F) tuple which are responds from $\mathcal{OR}_{TK_F}(F, \mathbb{P}^*)$ queries
- $RK^{List_{rk}}$ that stores (F, SK_F, TK_F, RK_F) tuple which are responds from $\mathcal{OR}_{RK_F}(F, \mathbb{P}^*)$ queries.

Phase 1: $\mathbb{AD}$ issues sequence of queries to which $\mathbb{BD}$ answers as follows:

Private key extraction oracle $\mathcal{OR}_{SK_F}$(F): $\mathbb{BD}$ computes the private key for the attribute list F in the following manner; If $F \vDash \mathbb{P}^*$ $\mathbb{BD}$ aborts with $\perp$, otherwise if $F \nvDash \mathbb{P}^*$ as in [8] there exist $q_{i,l}$ such that $q_{i,l} = F_i \wedge q_{i,l}$. Thus $\sum_{q_{i,j} \in F} \upsilon_{i,j} = V_1 + yV_2$ such that $V_1, V_2 \in \mathbb{Z}_p$. Also V_1, V_2 are represented by the sum of $\upsilon'^{i,j}$. Therefore $\mathbb{BD}$ can compute V_1 and V_2. $\mathbb{BD}$ selects $\phi \in \mathbb{Z}_p$, sets $\alpha = \frac{\phi - \omega x}{V_2}$ then computes the following:

$$\begin{aligned} SK_F &= (K_1, K_2) \\ K_1 &= (g^y)^{\phi} g^{\frac{V_1}{V_2}\phi} (g^x)^{-\frac{V_1 \omega}{V_2}} \\ K_2 &= g^{\frac{\phi}{V_2}} (g^x)^{-\frac{\omega}{V_2}} \end{aligned}$$

As in [8], we establish that SK_F is valid private key in the following manner:

$$\begin{aligned} K_1 &= (g^y)^{\phi} g^{\frac{V_1}{V_2}\phi} (g^x)^{-\frac{V_1 \omega}{V_2}} \\ &= g^{\omega xy}.g^{-\omega xy} (g^y)^{\phi} g^{\frac{V_1}{V_2}\phi} (g^x)^{-\frac{V_1 \omega}{V_2}} \\ &= g^{\omega xy}.g^{\frac{V_1}{V_2}(\phi - \omega x)} g^{y(\phi - \omega x)} \\ &= g^{\omega xy} (g^{V_1}.g^{yV_2})^{\frac{\phi - \omega x}{V_2}} \\ &= g^{\omega xy} (g^{V_1 + yV_2})^{\frac{\phi - \omega x}{V_2}} \\ &= h^b (g^{\sum_{q_{i,j} \in F} \upsilon_{i,j}})^{\alpha}. \end{aligned} \quad (3)$$

Note that in the above Equation 3, expression $g^{\omega xy}.g^{-\omega xy}$ is introduced as it is =1, since subtracting exponents $\omega xy - \omega xy$=0.

$K_2 = g^{\frac{\phi}{V_2}} (g^x)^{-\frac{\omega}{V_2}} = g^{\frac{\phi - \omega x}{V_2}} = g^{\alpha}$.
Therefore if V_2=0 mod p then $\mathbb{BD}$ outputs $\perp$. In the case V_2=0 mod p holds then it means there exists list F such that $\sum_{q_{i,j} \in F} \upsilon_{i,j} = \sum_{q_{i,j} \in \mathbb{P}^*} \upsilon_{i,j}$ holds. For more information we refer the reader to [8]. Finally $\mathbb{BD}$ stores the tuple(F, SK_F) to the $SK^{List_{sk}}$ and returns SK_F to $\mathbb{AD}$.

Transformation key extraction oracle $\mathcal{OR}_{TK_F}(F)$: Upon receiving attribute list F and access structure $\mathbb{P}^*$, $\mathbb{BD}$ confirms if there exists tuple (F, SK_F, TK_F, RK_F) in the list $TK^{List_{tk}}$. If it exists, $\mathbb{BD}$ returns the equivalent TK_F. Otherwise, if $F \nvDash \mathbb{P}^*$, $\mathbb{BD}$ responds with an equivalent private key SK_F by invoking $\mathcal{OR}_{SK_F}$ and its equivalent transformation key TK_F as in the actual scheme.

$$\begin{aligned} SK_F &= (TK_F, RK_F) \\ TK_F &= (K_1^{1/\sigma}, K_2^{1/\sigma}) \\ RK_F &= \sigma. \end{aligned}$$

If $F \vDash P^*$, then $\mathbb{BD}$ selects $\sigma \in \mathbb{Z}_p, (S_1, S_2) \in \mathbb{G}$ then computes $SK_F = (TK_F, RK_F) = ((S_1^{1/\sigma}, S_2^{1/\sigma}), \sigma)$. Finally $\mathbb{BD}$ adds the tuple(F, SK_F, TK_F, RK_F) to the list $TK^{List_{tk}}$ and responds $\mathbb{AD}$ with TK_F.

Retrieving Key extraction oracle $\mathcal{OR}_{RK_F}$: Almost similar to $\mathcal{OR}_{TK_F}$. It responds with retrieving key RK_F.

Partial decryption query oracle $\mathcal{OR}_{PDec}$: Upon receiving the tuple (CT, F), $\mathbb{BD}$ verifies whether $F \vDash \mathbb{P}$ embedded in CT. If it does not satisfies, it aborts with $\perp$. Otherwise it returns $PartialDecrypt_{out}(TK_F, CT)$. TK_F is the transformation key generated from $\mathcal{OR}_{TK_F}$.

Decryption query oracle $\mathcal{OR}_{Dec}$: Upon receiving the tuple (CT, F), $\mathbb{BD}$ verifies whether $F \vDash \mathbb{P}$ lodged in CT. If it does not satisfies, it aborts with $\perp$. Otherwise it carries out the following actions:

- If the ciphertext is original, first $\mathbb{BD}$ checks whether Equation 1 above is satisfied. If not $\mathbb{BD}$ outputs $\perp$. Else if $(F, SK_F) \in SK^{List_{sk}}$, $\mathbb{BD}$ recovers the message m using SK_F as in the actual scheme. Otherwise $\mathbb{BD}$ checks whether $(\mathbb{P}, m, \lambda, s) \in H_1^{List}$ and also $(RC, \kappa_1) \in H_2^{List}$ in such way that $\mathrm{B}_1{=}\kappa_1 \oplus (\mathrm{m}\|\lambda)$ while $RC = e(g,h)^{s.b}$. If such kind of tuple exists $\mathbb{BD}$ outputs m. Otherwise aborts with $\perp$.
- If the ciphertext is server-aided, first $\mathbb{BD}$ confirms if there exists tuple (F, SK_F, TK_F, RK_F) in the list $TK^{List_{tk}}$. If it does not exist, it aborts with $\perp$. Else $\mathbb{BD}$ checks whether $(\mathbb{P}, m, \lambda, s) \in H_1^{List}$ and also $(RC, \kappa_1) \in H_2^{List}$ in such way that $\mathrm{B}_1{=}\kappa_1 \oplus (\mathrm{m}\|\lambda)$ while $RC = e(g,h)^{sb}$. If such kind of tuple does not exists it outputs $\perp$. Otherwise $\mathbb{BD}$ confirms whether $T' = e(g,h)^{sb}/\varphi$ where $\varphi = H_1(\varepsilon)$ if its true it outputs m. Otherwise aborts with $\perp$.

Challenge: $\mathbb{AD}$ submits two plaintext messages m_0^* and m_1^* of equal length from the message space $\{0,1\}^k$. $\mathbb{BD}$ flips a random coin γ to choose $\gamma \in \{0,1\}$ and encrypts m_γ^* as follows:
$\mathbb{BD}$ selects $\lambda^* \in \{0,1\}^k, B_1^* \in \{0,1\}^{2k}$ then sets:

1) Compute $B_1^* = H_2(Z) \oplus (m_\gamma^* \| \lambda^*)$, $B_2^* = g^s$, $B_3^* = (\prod_{q_{i,j} \in \mathbb{P}^*} V_{i,j})^s$, and $B_4^* = (g^s)^\omega$.
2) Issue a H_3 query on $(\mathbb{P}^* \| B_1^* \| B_2^* \| B_3^* \| B_4^*)$ to obtain the tuple $(\mathbb{P}^* \| B_1^* \| B_2^* \| B_3^* \| B_4^*, \kappa_2, \eta)$. Finally computes $E^* = (g^s)^\eta$. Outputs the challenge ciphertext $CT^* = (\mathbb{P}^* \| B_1^* \| B_2^* \| B_3^* \| B_4^* \| E^*)$ to $\mathbb{AD}$. If $C = e(g,g)^{xyz}$, the challenge ciphertext is valid in relation to analysis in[8].

Phase 2: Nearly similar to phase 1 with stated constraints.

Guess: $\mathbb{AD}$ yields guess $\gamma' \in \{0,1\}$. If $\gamma' = \gamma$, $\mathbb{BD}$ outputs true (decides $C = e(g,g)^{xyz}$). Otherwise $\mathbb{BD}$ outputs false (decides $C \neq e(g,g)^{xyz}$).

From analysis in [9], the preceding simulation will terminate with negligible probability. Therefore we get the theorem. □

Theorem 2. *Suppose the MDDH assumption [34] holds in $(\mathbb{G}, \mathbb{G}_\tau)$ and H_1, H_2, H_3 are the TCR hash functions, then our CBe-BDS-OD is IND-AND-sAS-CCA2-sa secure in the random oracle model.*

Proof. We show that if there exist an adversary $\mathbb{AD}$ that can break the IND-AND-sAS-CCA2-sa security of the proposed CBe-BDS-OD scheme then we construct an algorithm $\mathbb{BD}$ using $\mathbb{AD}$ as a subroutine to solve MDDH problem. First MDDH challenger flips a fair coin δ and if δ=0, it sets $(g, X, Y, C) := (g, g^x, e(g,g)^y, e(g,g)^{xy})$; otherwise it sets $(g, X, Y, C) := (g, g^x, e(g,g)^y, (g,g)^c)$ where $x, y, c \in \mathbb{Z}_p$ are randomly chosen. The challenger then gives $\mathbb{BD}$ $(g, X, Y, C) := (g, g^x, e(g,g)^y, C)$. To be specific $\mathbb{BD}$ will act as a challenger with $\mathbb{AD}$ to play the following IND-AND-sAS-CCA2-sa game.

Init: Same as in Theorem 1.

Setup: $\mathbb{BD}$ selects two random elements $b \in_R \mathbb{Z}_p^*$ and $\upsilon_{i,j} \in_R \mathbb{Z}_p^*$ $(i \in [1,n], j \in [1, n_i])$. $\mathbb{BD}$ then computes $\mathbb{Y} = e(g,h)^b$ and $V_{i,j} = g^{\upsilon_{i,j}}$. It also maintains and responds to the TCR list $H_i^{List}(i \in \{1,.,3\})$ as in theorem 1. It chooses H_3 as the actual execution. It yields master secret key $\mathrm{MSK}{=}(b, \{\upsilon_{i,j}\}_{i \in [1,n], j \in [1,n_i]})$ which is known to $\mathbb{BD}$.

Phase 1: $\mathbb{AD}$ issues sequence of queries to which $\mathbb{BD}$ answers as follows:

Private key extraction oracle $\mathcal{OR}_{SK_F}$(F): $\mathbb{BD}$ receives attribute list F from $\mathbb{AD}$. $\mathbb{BD}$ then invokes $KeyGen(PK, MSK, F)$ to obtain SK_F the private key for the attribute list F.

Transformation key extraction oracle $\mathcal{OR}_{TK_F}(F)$: Upon receiving attribute list F and access structure $\mathbb{P}^*$, $\mathbb{BD}$ confirms if there exists tuple (F, SK_F, TK_F, RK_F) in the list $TK^{List_{tk}}$. If it exists, $\mathbb{BD}$ returns the equivalent TK_F. Otherwise, if $F \nvDash \mathbb{P}^*$, $\mathbb{BD}$ responds with a related private key SK_F by invoking $\mathcal{OR}_{SK_F}$ and the related server-aided key pair $(TK_F, RK_F) = ((K_1^{1/\sigma}, K_2^{1/\sigma}), \sigma)$ as in the actual scheme. if $F \vDash \mathbb{P}^*$, $\mathbb{BD}$ gets the related private key SK_F by querying $\mathcal{OR}_{SK_F}(F)$ with F^*, and the equivalent server-aided key pair $(TK_F, RK_F) = (((X^t)^b (X^{\sum_{q_{i,j} \in F} \upsilon_{i,j}})^\alpha, X^\alpha), \bullet)$ where t, α are randomly chosen elements to generate the private key SK_{F^*}, while

the • means the RK_F is undisclosed. In the case where $F \vDash P^*$, $\mathbb{BD}$ sets $\sigma = a$ that is undisclosed. Finally records (F, SK_F, TK_F, RK_F) in the list $TK^{List_{tk}}$.

Retrieving Key extraction oracle $\mathcal{OR}_{RK_F}$: Almost similar to $\mathcal{OR}_{TK_F}$. It responds with retrieving key RK_F.

Partial decryption query oracle $\mathcal{OR}_{PDec}$: Upon receiving the tuple (CT, F), $\mathbb{BD}$ verifies whether $F \vDash \mathbb{P}$ in CT. If it does not satisfies, it aborts with $\perp$. Otherwise it returns $PartialDecrypt_{out}(TK_F, CT)$. TK_F is the transformation key generated from $\mathcal{OR}_{TK_F}$.

Decryption query oracle $\mathcal{OR}_{Dec}$: Upon receiving the tuple (CT, F), $\mathbb{BD}$ verifies whether $F \vDash \mathbb{P}$ in CT. If it does not satisfies, it aborts with $\perp$. Otherwise it carries out the following actions:

- If the ciphertext is original, $\mathbb{BD}$ invokes $SK_F \leftarrow KeyGen(PK, MSK, F)$ and $m \leftarrow Decrypt(PK, SK_F, CT)$.
- If the ciphertext is server-aided, $\mathbb{BD}$ confirms if there exists tuple (F, SK_F, TK_F, RK_F) in the list $TK^{List_{tk}}$. If it does not exist, it aborts with $\perp$. Otherwise $\mathbb{BD}$ carries out the following actions:
  - if attribute list $F \nvDash P^*$ it employs the corresponding RK_F to retrieve the message m and sends it to $\mathbb{AD}$.
  - Else if attribute list $F \vDash P^*$, $\mathbb{BD}$ establishes whether $(\mathbb{P}, m, \lambda, s) \in H_1^{List}$ and also $(RC, \kappa_1) \in H_2^{List}$ in such way that $B_1 = \kappa_1 \oplus (m \| \lambda)$ where $RC = e(g,h)^{sb}$. If such kind of tuple does not exists it outputs $\perp$. Otherwise $\mathbb{BD}$ confirms whether $T'' = e(X,h)^{bH_1(\mathbb{P},m,\lambda)}$ if its true it outputs m. Otherwise aborts with $\perp$.

Challenge: $\mathbb{AD}$ submits two plaintext messages m_0^* and m_1^* of equal length from the message space $\{0,1\}^k$. $\mathbb{BD}$ flips a random coin γ to choose $\gamma \in \{0,1\}$ and encrypts m_γ^* as follows:
$\mathbb{BD}$ selects $\lambda^* \in \{0,1\}^k$, $B_1^* \in \{0,1\}^{2k}$ then sets

$$\begin{aligned} B_1^* &= H_2(Y^b) \oplus (m_\gamma^* \| \lambda^*) \\ T' &= C^{1/b}. \end{aligned}$$

If $C = e(g,g)^{xy}$, the challenge ciphertext is valid in relation to analysis in [8]

Phase 2: Nearly similar to phase 1 with the stated constraints.

Guess: $\mathbb{AD}$ outputs guess $\gamma' \in \{0,1\}$. If $\gamma' = \gamma$, $\mathbb{BD}$ outputs true (decides $C = e(g,g)^{xy}$). Otherwise $\mathbb{BD}$ outputs false(decides $C \neq e(g,g)^{xy}$).

□

From analysis in [9], the preceding simulation will terminate with negligible probability. Therefore we get the theorem.

7 Conclusion

In this paper, we proposed server-aided decryption in cloudlet for eHealth big data. We offloaded heavy computation to the server, in order to minimize pairing and reduce computation cost on the end user's (client) side. The validity of ciphertext is confirmed before partial decryption and final decryption is carried out by server and end user respectively. Further, the security analysis of the scheme has proven its authenticity in the random oracle model. We evaluated the performance of the scheme and the analysis of the output indicates that our proposal is IND-AND-sAS-CCA2 secure and practical and hence it's applicable to resource-constrained devices.

Acknowledgments

This work was supported by the Sichuan Province Science Technology Project [grant numbers 2014GZ0109 and 2015JY0178].

References

[1] A. Bahtovski and M. Gusev, "Cloudlet challenges," *Procedia Engineering*, vol. 69, pp. 704–711, 2014.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[3] S. Canard, N. Desmoulins, J. Devigne, and J. Traoré, "On the implementation of a pairing-based cryptographic protocol in a constrained device," in *Proceedings of the 5th International Conference on Pairing-Based Cryptography*, pp. 210–217, 2013.

[4] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 207–222, 2004.

[5] M. Chase, "Multi-authority attribute based encryption," in *Proceedings of the 4th Conference on Theory of Cryptography*, pp. 515–534, 2007.

[6] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *IInternational Journal Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[7] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM Journal on Computing*, vol. 33, no. 1, pp. 167–226, 2003.

[8] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proceedings of the 5th International Conference on Information Security Practice and Experience*, pp. 13–23, 2009.

[9] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pp. 537–554, 1999.

[10] Gartner, "Gartner's three-part definition of big data," 2013. `http://www.dataversity.net/gartners-three-part-definition-of-big-data/`.

[11] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in *Proceedings of the 20th USENIX Conference on Security*, pp. 34–34, 2011.

[12] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, pp. 2150–2162, Nov. 2012.

[13] P. Hu and H. Gao, "A key-policy attribute-based encryption scheme for general circuit from bilinear maps," *International Journal Network Security*, vol. 19, no. 5, pp. 704–710, 2017.

[14] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[15] C. C. Lee, P. S. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal Network Security*, vol. 15, pp. 231–240, 2013.

[16] G. Lewis, S. Echeverria, S. Simanta, B. Bradshaw, and J. Root, "Tactical cloudlets: Moving cloud computing to the edge," in *IEEE Military Communications Conference*, pp. 1440–1446, Oct. 2014.

[17] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2201–2210, 2014.

[18] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. PP, no. 99, 2016.

[19] K. Li and H. Ma, "Outsourcing decryption of multi-authority abe ciphertexts," *International Journal Network Security*, vol. 16, pp. 286–294, 2014.

[20] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 552–559, 2013.

[21] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2119–2130, 2015.

[22] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[23] F. Liu, P. Shu, H. Jin, L. Ding, J. Yu, D. Niu, and B. Li, "Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications," *IEEE Wireless Communications*, vol. 20, pp. 14–22, June 2013.

[24] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," *International Journal Network Security*, vol. 16, pp. 437–443, 2014.

[25] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 5, pp. 533–546, 2016.

[26] I. Olaronke and O. Oluwaseun, "Big data in healthcare: Prospects, challenges and resolutions," in *Future Technologies Conference (FTC'16)*, pp. 1152–1157, Dec. 2016.

[27] H. Qian, J. Li, and Y. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in *15th International Conference on Information and Communications Security*, pp. 363–372, 2013.

[28] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, pp. 457–473, 2005.

[29] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing," *IEEE Pervasive Computing*, vol. 8, pp. 14–23, Oct. 2009.

[30] T. Verbelen, P. Simoens, F. D. Turck, and B. Dhoedt, "Cloudlets: Bringing the cloud to the mobile user," in *Proceedings of the Third ACM Workshop on Mobile Cloud Computing and Services*, pp. 29–36, 2012.

[31] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography*, pp. 53–70, 2011.

[32] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[33] M. Xiao, M. Wang, X. Liu, and J. Sun, "Efficient distributed access control for big data in clouds,"

in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'15)*, pp. 202–207, Apr. 2015.

[34] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "Cca-secure {ABE} with outsourced decryption for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 730 – 738, 2018.

Biography

Kittur Philemon Kibiwott is currently pursuing Ph.D. degree at the University of Electronic Science and Technology of China (UESTC). He received Bsc degree in Computer Science from Periyar University (India) and Msc degree Computer Science from Bharathiar University (India). His research area of interest include cloud computing, cryptography and information security.

Zhang Fengli received her Ph.D. degree from the University of Electronic Science and Technology of China (UESTC) in 2007 and M.S. degree in 1986. She is currently a Professor at the University of Electronic Science and Technology of China (UESTC). She has published more than eighty papers in refereed international journals and conferences which more than 50 are indexed by SCI and EI. Her research area of interest include mobile data management and application, network security, database.

Omala A. Anyembe is currently a Ph.D candidate in the school of Computer Science and Engineering at the University of Electronic Science and Technology of China (UESTC). His research area of interest include cryptography, IoT and information security.

Daniel Adu-Gyamfi is currently a Ph.D candidate in the school of Information and Software Engineering at the University of Electronic Science and Technology of China (UESTC). His research area of interest include privacy preservation in cloud computing, Trajectory, cryptography and information security.

Image-based Multimodal Biometric Authentication Using Double Random Phase Encoding

Eman Tarek, Osama Ouda, and Ahmed Atwan
(Corresponding author: Eman Tarek)

Department of Information Technology, Faculty of Computers and Information Sciences
El Gomhouria St, Mansoura, Dakahlia Governorate 35516, Egypt
(Email: eman_tarek@mans.edu.eg)
(Received Aug. 20, 2017; revised and accepted Nov. 21, 2017)

Abstract

This paper presents an image-based multimodal biometric authentication scheme that utilizes a popular image encryption technique, known as double random phase encoding (DRPE). The proposed scheme aims at protecting biometric templates against unauthorized disclosure without deteriorating the recognition accuracy. Unlike conventional feature-based biometric authentication methods, the proposed scheme uses phase-based image matching of images captured from the employed biometric modalities; namely, palmprint and fingerprint, in order to enhance both accuracy and security of the suggested recognition system. A palmprint image is used as a secret key to encrypt a fingerprint image, captured from the same user, using DRPE. The encrypted fingerprint image can be successfully decrypted only if the phase-only-correlation between enrollment and authentication palmprint images is sufficiently high (*i.e.* the two images belonging to the same user). Then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, and the overall authentication process succeeds if the matching result exceeds a predefined threshold. The experimental results illustrate the efficacy of the proposed scheme and show that it can improve the security of biometric data without deteriorating the recognition accuracy.

Keywords: Double Random Phase Encoding; Image-Based Matching; Multimodal Biometric Authentication

1 Introduction

Traditional authentication systems that rely on user-specific passwords and/or tokens are susceptible to several usability issues. For instance, passwords can be forgotten or stolen and tokens can easily be lost, shared or misplaced [3, 5, 11]. Biometric authentication systems, on the other hand, identify individuals using their physiological or behavioral traits such as iris, face, fingerprint, palmprint, signature, and voice. These traits are unique across individuals and thereby cannot be duplicated, forgotten, or lost [10,14]. Despite these inherent advantages, the widespread deployment of biometric technology has been impeded due to several reasons; the most crucial are the issues of template security and the less than desirable recognition accuracy of biometric systems [4].

These issues need to be addressed in order to enhance public acceptance of biometric technology. Compromising biometric templates leads to serious security threats during every authentication attempt since such templates, unlike passwords and tokens, cannot be revoked or reissued. As a result, several template protection schemes have been proposed over the past few years [9, 15, 16] in order to address the issue of template security. Unfortunately, such schemes cannot preserve the recognition accuracy exhibited by original (unprotected) biometric systems [20].

On the other hand, many multimodal biometric authentication schemes have been proposed in the past decade [30, 34] in order to improve recognition accuracy as well as security of biometric-based authentication systems. Obviously, chances of compromising biometric templates derived from multiple biometric modalities are small compared to chances of compromising templates generated from a single biometric modality. However, these biometric templates are stored as unprotected templates in central databases.

In this paper, we present a new multi-modal biometric authentication scheme based on the well-known image encryption technique: Double Random Phase Encoding (DRPE) [17]. The DRPE scheme benefits from the high correlation existing between phase components of encryption and decryption keys (masks) to recover the encrypted image. In the case of biometric authentication, enrollment and verification samples, belonging to the same

user, can be employed as encryption and decryption keys in DRPE [22–25, 28, 31] since the Phase-Only Correlation (POC) between these samples is expected to be high enough to restore the encrypted image [6, 7]. The goal of our proposed scheme is to protect the stored biometric templates (images) using DRPE without deteriorating the recognition accuracy through utilizing two different biometric modalities; namely, fingerprint and palmprint, for authenticating individuals. That is, images acquired from one biometric modality will be used to encrypt images captured from the other modality using DRPE.

The rest of this paper is organized as follows. Section 2 provides a brief overview of both POC-based image matching and DRPE. Section 3 introduces the proposed image-based multi-modal biometric authentication scheme. Section 4 presents the experimental results and discusses the efficacy of the proposed method. Finally, Section 5 concludes the paper.

2 Preliminaries

In this section, we first give a brief overview of phase-only correlation (POC), describe a band-limited variant of POC (BLPOC), and explains how both techniques can be employed for image matching. Then, a brief description of DRPE is provided.

2.1 Phase Only Correlation (POC)

The demand for highly accurate image matching techniques is rapidly increasing in many fields, such as computer vision, image sensing and analysis, biometrics and security [1, 2, 6, 7, 21, 33]. POC-based image matching techniques, which uses the phase components in Discrete Fourier Transforms (DFTs) of images, have demonstrated their effectiveness in implementing several biometric authentication schemes [6,7]. In this subsection, we describe the basic definition and mathematical formula of the POC function used for image matching.

Consider two $M \times N$ images $f_1(x, y)$ and $f_2(x, y)$ with index ranges $x = -M_0, \cdots, M_0 (M_0 > 0)$ and $y = -N_0, \cdots, N_0 (N_0 > 0)$, and $M = 2M_0 + 1$ and $N = 2N_0 + 1$ for mathematical simplicity. Let $F_1(u, v)$ and $F_2(u, v)$ denote the 2D discrete Fourier transforms of $f_1(x, y)$ and $f_2(x, y)$ in which $u = -M_0, \cdots, M_0$ and $v = -N_0, \cdots, N_0$, given by:

$$\begin{aligned} F_1(u,v) &= \mathrm{DFT}[f_1(x,y)] \\ &= \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} f_1(x,y) e^{-j2\pi(\frac{mu}{M}+\frac{nv}{N})} \\ &= A_{F1}(u,v) e^{j\theta_{F_1}(u,v)}, \end{aligned} \tag{1}$$

$$\begin{aligned} F_2(u,v) &= \mathrm{DFT}[f_2(x,y)] \\ &= \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} f_2(x,y) e^{-j2\pi(\frac{mu}{M}+\frac{nv}{N})} \\ &= A_{F2}(u,v) e^{j\theta_{F_2}(u,v)}, \end{aligned} \tag{2}$$

where DFT[·] denotes the 2D discrete Fourier transform, $A_{F1}(u, v)$ and $A_{F2}(u, v)$ are the amplitude components, and $e^{j\theta_{F_1}(u,v)}$ and $e^{j\theta_{F_2}(u,v)}$ are the phase components of the two images. The cross phase spectrum $R_{F_1F_2}(u, v)$ between $F_1(u, v)$ and $F_2(u, v)$ is given by:

$$\begin{aligned} R_{F_1F_2}(u,v) &= \frac{F_1(u,v)\overline{F_2(u,v)}}{|F_1(u,v)\overline{F_2(u,v)}|} \\ &= e^{j\{\theta_{F_1}(u,v)-\theta_{F_2}(u,v)\}} \\ &= e^{j\theta(u,v)}, \end{aligned} \tag{3}$$

where $\overline{F_2(u, v)}$ is the complex conjugate of $F_2(u, v)$ and $e^{j\theta(u,v)}$ is the phase difference of $F_1(u, v)$ and $F_2(u, v)$. Then POC function is the 2D inverse Fourier transform of $R_{F_1F_2}(u, v)$:

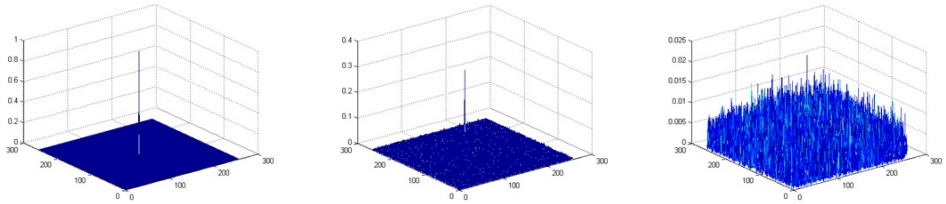
$$P_{f_1f_2}(x,y) = \frac{1}{MN} \sum_u \sum_v R_{F_1F_2}(u,v) e^{j2\pi(\frac{ux}{M}+\frac{vy}{N})}. \tag{4}$$

If there is a similarity between two matched images, their POC function gives a distinct sharp peak. If not, a random noise with lower peaks are observed. The height of the correlation peak is a good similarity measure for image matching and the location of the peak is also a good measure for translational displacement between two images. Figure 1 illustrates an example of fingerprint image matching using POC function and their corresponding POC similarity.

2.2 Band-Limited Phase Only Correlation (BLPOC)

In POC-based image matching, all the phase components of the 2D-DFT of given images are involved. However, some phase components in high frequency domain are not reliable and can be prone to error. It has been observed that the height of the correlation peak, resulting from matching similar images, is significantly reduced if the high frequency components are taken into account in the matching process [6, 7, 21, 33]. Ito *et al.* [6] proposed the Band-Limited Phase-Only Correlation (BLPOC) function that eliminates meaningless phase components in high frequency region and only uses the effective frequency band of matched images to improve the performance of image matching.

Figure 2 illustrates a fingerprint image and its corresponding amplitude components of the 2D-DFT. The frequency components that are higher than this dominant frequency band have very low power, and hence thier phase components are not reliable. Assuming that the ranges of an effective frequency band of given matched images are defined by $u = -U_0, \cdots, U_0 (U_0 > 0)$, $v = -V_0, \cdots, V_0 (V_0 > 0)$, $L_1 = 2U_0 + 1$, and $L_2 = 2V_0 + 1$, where L_1 and L_2 define the effective band size, the BLPOC function is defined as:



(a) POC of identical images (b) POC of similar images (c) POC of different images

Figure 1: Fingerprint image matching using POC function

$$P_{f_1 f_2}^{U_0 V_0}(x,y) = \frac{1}{L_1 L_2} \sum_{u=-U_0}^{U_0} \sum_{v=-V_0}^{V_0} R_{F_1 F_2}(u,v) e^{j2\pi(\frac{xu}{L_1}+\frac{yv}{L_2})}. \quad (5)$$

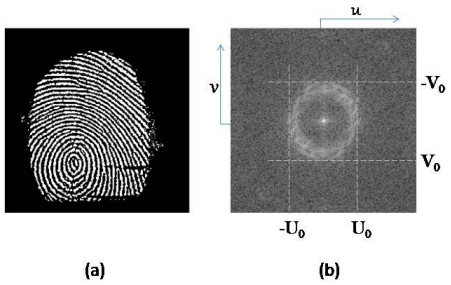


Figure 2: Fingerprint image with its corresponding amplitude components of the 2D-DFT

Figure 3 shows an example of palmprint image matching, where the figure compares the original POC and the BLPOC functions. The BLPOC provides a higher correlation peak than that of the original POC. Thus, the BLPOC function exhibits a much higher discrimination capability than the original POC function.

2.3 Double Random Phase Encoding (DRPE) Scheme

The DRPE scheme is an optical image encryption technique proposed by Refergier and Javidi [17]. The idea of this scheme is to encode the original image into a complex stationary white noise, employing two statistically independent random phase masks; namely, $RPM1$ and $RPM2$, in the spatial and Fourier domains respectively. The DRPE scheme can be implemented optically or digitally. An optical setup, also called $4f$ setup, which is commonly used to optically implement DRPE is illustrated in Figure 4. This setup consists of two cascaded optical Fourier transformation lenses separated by two focal lengths, with one focal length outside the lens with each of the input and output image planes, and hence the total is four focal lengths $4f$.

The overall process of the DRPE scheme can be described as follows. Let $f(x,y)$ denotes the input image to be encoded and $\psi(x,y)$ denotes the encrypted image. Let $n(x,y)$ and $m(u,v)$ are two independently random noisy functions uniformly distributed over the interval $[0,1]$ where(x,y) denotes the spatial domain coordinates and(u,v) denotes the Fourier domain coordinates.

As illustrated in Figure 4(a), two random phase masks are used in the encryption process; namely,
$RPM1 = exp[j2\pi n(x,y)]$ and $RPM2 = exp[j2\pi m(u,v)]$.

The encrypted image $\psi(x,y)$ is obtained by multiplying the input image $f(x,y)$ with $RPM1$ in the spatial domain and then convolving the resulting image with the function $h(x,y)$. That is, the encrypted image is given by:

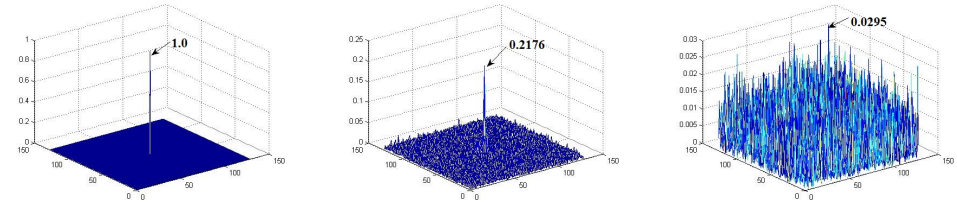
$$\psi(x,y) = \{f(x,y)exp[j2\pi n(x,y)]\} * h(x,y), \quad (6)$$

where $h(x,y)$ is the impulse response of $h(u,v) = exp[j2\pi m(u,v)]$ and $*$ denotes the convolution operation. To recover back (decrypt) the original image, as shown in Figure 4(b), the encrypted image $\psi(x,y)$ is Fourier transformed and multiplied with the complex conjugate of the $RPM2$ used in the frequency domain $exp[-j2\pi m(u,v)]$, and then inverse Fourier transformed to produce the output $f(x,y)exp[j2\pi n(x,y)]$ whose absolute value is the decrypted image $f(x,y)$ since $f(x,y)$ is a positive image. The decryption process can be expressed as:

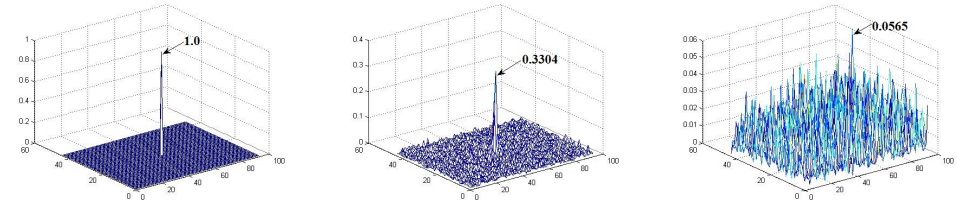
$$\begin{aligned} & f(x,y)exp[j2\pi n(x,y)] \\ = \; & IFT\{FT\{\psi(x,y)\}exp[-j2\pi m(v,w)]\}, \end{aligned} \quad (7)$$

where $FT[\cdot]$ and $IFT[\cdot]$ donate the Fourier Transform and the Inverse Fourier Transform, respectively.

The statistical analysis of DRPE [18, 27] proved its efficiency as a secure image protection scheme because of its efficient reconstruction of the original image and its robustness against blind deconvolution. Moreover, it has been shown that it is difficult to recover the encoded image without knowing the employed random phase mask [18]. Due to these attractive advantages, several schemes based on the main idea of DRPE have been proposed [8, 12, 29]. In addition, many security systems are devised to merge DRPE with other methods such as holographic methods [26, 32], watermarking [19], information hiding [13] and Biometric authentication [22–25, 28, 31].



(a) POC of identical images (b) POC of similar images (c) POC of different images



(d) BLPOC of identical images (e) BLPOC of similar images (f)BLPOC of different images

Figure 3: Example of palmprint image matching using the original POC and the BLPOC

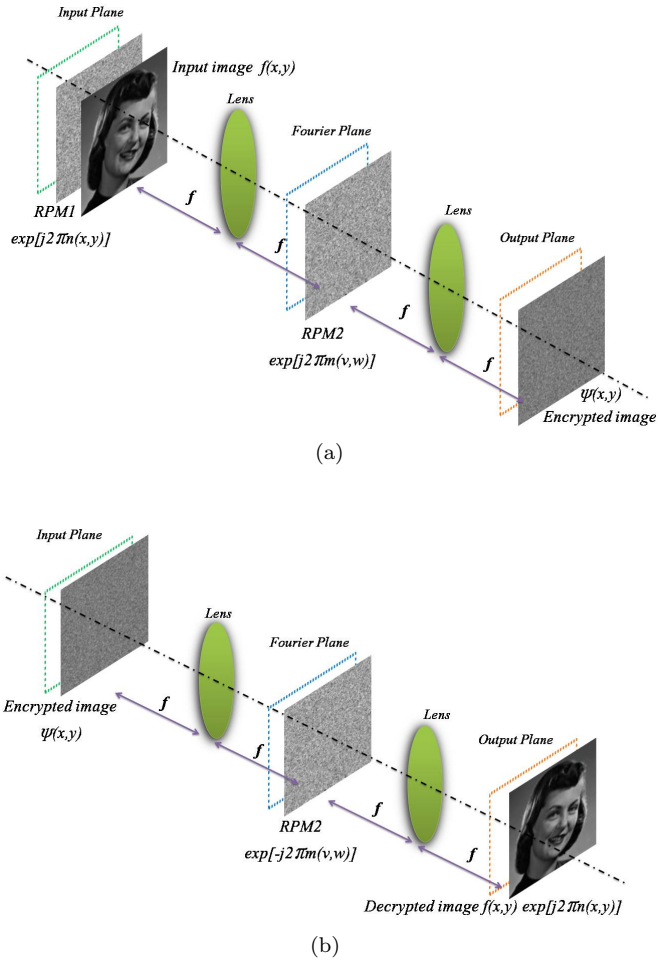
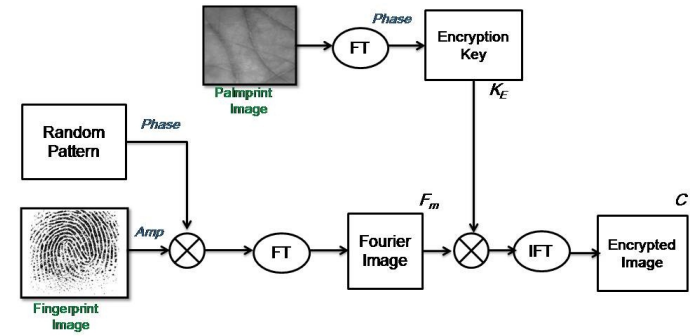


Figure 4: Optical implementation of the DRPE scheme (a) Encryption process and (b) Decryption process

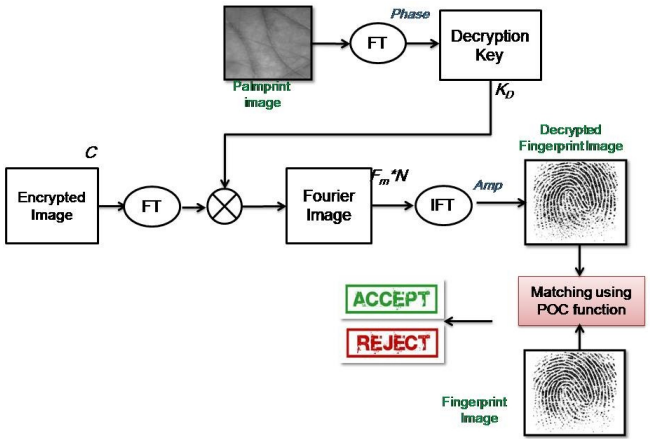
3 Proposed Scheme

This paper presents a secure multimodal biometric authentication scheme that uses a palmprint image as a secret key to encrypt a fingerprint image, both belonging to the same individual, using DRPE. In DRPE, it is possible to recover the original image even if the two encryption and decryption keys are not identical. In other words, the restoration accuracy of decrypted image relies on the similarity between two keys. Therefore, the DRPE is appropriate as encryption method for fingerprint image when uses the palmprint image as a cipher key. Figure 5 illustrates the main idea behind the proposed multi-modal authentication scheme. During the enrollment stage, DRPE is employed to encrypt a fingerprint image, taken from the fingertip of the user being enrolled, using a key represented by the phase components of the 2D-DFT of a palmprint image captured from the palm of the same user. The encrypted random image (complex amplitude) is safely stored as a protected template in a central database.

At verification, the encrypted fingerprint image can be successfully decrypted only if the phase only correlation between enrollment and authentication palmprint images is sufficiently high *i.e.* the two images belonging to the same user). Then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC-based image matching and the overall authentication process succeeds if the matching result, of the fingerprint images, exceeds a predefined threshold. This improves the security of the overall authentication system since the user must present genuine fingerprint and palmprint images in order to successfully authenticate himself to the system. In other words, if some adversary managed to present a true image of one of the two modalities to the authentication system, he/she would not be able to pass the authentication test successfully unless he present a genuine sample of the other



(a)



(b)

Figure 5: Image-based multimodal biometric authentication using DRPE (a) Encryption process and (b) Decryption process

modality.

3.1 Encryption

Let $F_E(x,y)$ and $P_E(x,y)$ denote fingerprint and palmprint images, captured during enrollment (encryption). At enrollment, the amplitude of $F_E(x,y)$ is multiplied by the first phase mask extracted from a random pattern $R(x,y)$ to obtain a phase modulated image $F_{Em}(x,y)$ as follows:

$$F_{Em}(x,y) = F_E(x,y)exp[jR(x,y)]. \tag{8}$$

The obtained phase modulated image, $F_{Em}(x,y)$, is then transformed into the frequency domain using the 2D-DFT and the resulting coefficients matrix, $F_{Em}(u,v)$, is multiplied by the second phase mask $exp[jK_E(u,v)]$, that represents the phase components of 2D-DFT of the user's palmprint image $P_E(x,y)$ (encryption key) and is given by:

$$\begin{aligned} P_E(u,v) &= FT[P_E(x,y)] \\ &= A_E(u,v)exp[jPh_E(u,v)], \end{aligned} \tag{9}$$

where $A_E(u,v)$ is the amplitude components and $Ph_E(u,v)$ is the phase components of the 2D-DFT of the palmprint image. That is, using $K_E(u,v) = Ph_E(u,v)$, the encrypted image $C(x,y)$ is obtained as a complex amplitude random image expressed as follows:

$$C(x,y) = IFT[F_{Em}(u,v)exp[jK_E(u,v)]]. \tag{10}$$

3.2 Decryption

Let $F_D(x,y)$ and $P_D(x,y)$ denote fingerprint and palmprint images, captured during verification (decryption). To decrypt, the complex conjugate of encrypted image, $C^*(u,v) = F^*_{Em}(u,v)exp[-jK_E(u,v)]$, is multiplied by the phase mask (Decryption Key), $exp[jK_D(u,v)]$, extracted from a fresh palmprint image $P_D(x,y)$, captured during verification as follows:

$$\begin{aligned} & C^*(u,v)exp[jK_D(u,v)] \\ = \; & F^*_{Em}(u,v)exp\{j[-K_E(u,v) + K_D(u,v)]\}, \end{aligned} \tag{11}$$

where the image $K_D(u,v)$ represents the phase components, $Ph_D(u,v)$, of the palmprint decryption image $P_D(x,y)$. That is,

$$\begin{aligned} P_D(u,v) &= FT[P_D(x,y)] \\ &= A_D(u,v)exp[jPh_D(u,v)]. \end{aligned} \tag{12}$$

Obviously, the inverse Fourier transform of the obtained result releases the decrypted image as follows:

$$\begin{aligned} & F_r(x_d,y_d) \\ & = IFT[F^*_{Em}(u,v)exp\{j[-K_E(u,v) + K_D(u,v)]\}] \\ & = F^*_{Em}(x,y) * n(x_d,y_d), \end{aligned} \tag{13}$$

where $*$ denotes the convolution and $n(x_d,y_d) = FT[exp\{j[-K_E(u,v) + K_D(u,v)]\}]$ represents the phase

only correlation(POC) between enrollment and authentication palmprint images.That is, $n(x_d, y_d)$ approximately satisfies the following relation

$$n(x_d, y_d) \cong \begin{cases} \delta(x_d - \alpha, y_d - \beta)(geniunepalmprint) \\ random\ sequence(imposterpalmprint), \end{cases}$$

where $\delta()$ denotes the Dirac delta function and α and β represent the shift between enrollment and authentication palmprint images. When a correct palmprint is used, the restored image $F_r(x_d, y_d)$ is expressed as $F^*_{Em}(x - \alpha, y - \beta)$ with the same intensity pattern as that of $F_E(x, y)$. When an incorrect palmprint is used, $F_r(x_d, y_d)$ produces a random image, which is the convolution of$F_{Em}(x, y)$ and a random sequence.

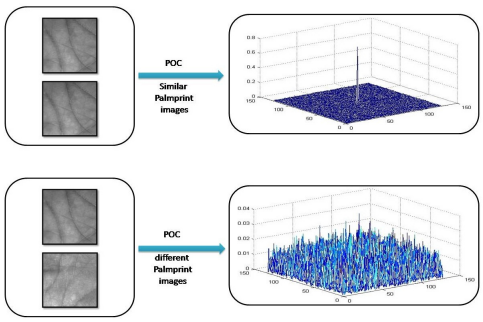


Figure 6: Palmprint image matching using POC

Apparently, the result of the decryption process in DRPE equal to the result of the convolution between enrollment fingerprint image and the phase only correlation (POC) between enrollment and authentication palmprint images. As illustrated in Figure 6, if the two palmprint images are belonging to the same user, the POC exhibits a distinct sharp peak. Otherwise, it exhibits a random noise. Then, the encrypted fingerprint image can be successfully decrypted only if the phase only correlation between the two palmprint images is sufficiently high.

3.3 POC-based Image Matching

After decryption, the decrypted image is matched against a fresh fingerprint image $F_D(x, y)$, captured during verification, using POC-based image matching method to decide the acceptance or the rejection of an individual based on a predefined threshold. The POC-based method uses the phase components of the Fourier transformed fingerprint images for effective image matching [6]. As discussed earlier, POC-based image matching has proven its efficiency even for low quality fingerprint images [6, 7] as illustrated eariler in Figure 1. An example of POC-based fingerprint image matching after geniune and imposter decryption is illustrated in Figure 7. Figure 7 (a) illustrates geniune fingerprint image, captured during verification, matched against (b) the correctly decrypted fingerprint image and (c) shows the POC similarity between matched image. Figure 7 (d) illustrates imposter fingerprint image, captured during verification, matched against (e) randomly decrypted image and (f) shows the POC similarity between matched image.

4 Experimental Results

In this section, we describe a set of experiments that have been carried out to evaluate the verification accuracy of our proposed encoding method and to confirm the randomness of images decrypted using an imposter key.

4.1 Experimental Setup

All experiments have been implemented using Matlab R2011a on a $core^{TM}$ 2 Duo 2 GHz processor with 2GB RAM. We used CASIA palmprint image dataset with three different fingerprint image datasets to check the robustness of the proposed method against shift and rotation variations in the fingerprint images and to compare its performance with the existing fingerprint verification method that is also based on the DRPE scheme [22–25, 28]:

1) *The 1st fingerprint dataset.* This dataset was employed to test the robustness of methods proposed in [22, 25, 28]. It contains 8 experimental subjects; each contributes with 6 fingerprint images captured using a capacitive fingerprint sensor developed by NTT Electronics Corporation [25]. This dataset has a good quality fingerprint images whose shift and rotation are aligned.

2) *The 2nd fingerprint image dataset.* This dataset contains 210 fingerprint images captured from 21 experimental subjects (10 fingerprint images per person) [24]. These fingerprint images are collected with some shift change.

3) *The 3rd fingerprint image dataset.* The popular CASIA fingerprint image database (ver. 5.0). Images in this dataset have various levels of shift and rotation changes.

For each individual, one fingerprint image and one palmprint image are used for enrollment (encryption) and the others are used for verification (decryption). Each fingerprint and palmprint images are originally 8 bit gray-level BMP files with palmprint image resolution 128*128 and with fingerprint image resolution 256*256 in the 1st and the 2nd datasets but 356 x 328 in the 3rd dataset, which is reduced to 128*128 in the spatial domain and encoded as binary images to be encrypted with the secret key generated from the palmprint image. The verification accuracy is then evaluated under genuine and imposter decryption.

4.2 Robustness of Decryption Process

In this section, we evaluate the robustness of the proposed scheme under geniune and imposter decryption.

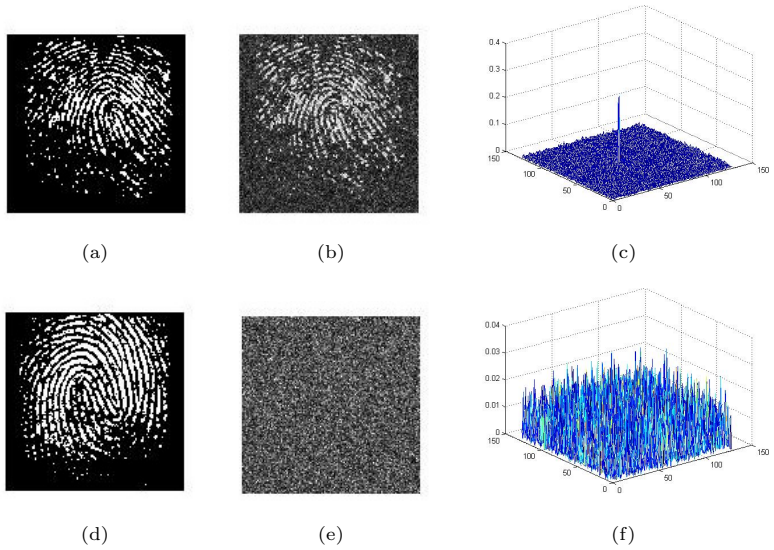


Figure 7: Example of POC-based fingerprint image matching after decryption in the proposed scheme

Figure 8 shows an example of a fingerprint image for enrollment, a palmprint image used as a secret key for encryption, captured from the same user and the encrypted random image which is safely stored as a protected template in a central database for verification.

At verification (Decryption and POC-based image matching), the encrypted fingerprint image can be successfully decrypted only if the same user's palmprint image is used as a secret key for decryption. then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC. To test the effectiveness of the proposed method in improving the security of the overall authentication system since the user must present genuine fingerprint and palmprint images in order to successfully authenticate himself to the system. As illustrated in Figure 9, we implemented and tested all possible combinations of fingerprint and palmprint images,captured during verification:genuine palmprint for decryption with genuine fingerprint for poc-matching,genuine palmprint for decryption with imposter fingerprint for poc-matching,imposter palmprint for decryption with genuine fingerprint for poc-matching, and imposter palmprint for decryption with imposter fingerprint for poc-matching.

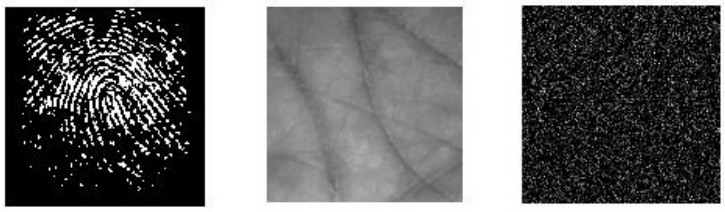
1) *Decryption with geniune palmprint image.* The encrypted fingerprint image can be successfully decrypted only if the same user's palmprint image is used as a secret key for decryption. Figure 9 (a) and (f) show the encrypted image, Figure 9 (b) and (g) show a palmprint image captured from the same user,used as a decryption key, and Figure 9 (c) and (h) the correctly decrypted fingerprint image.

2) *Decryption with imposter palmprint image.* Figure 9 (k) and (p) show the encrypted image, Figure 9 (l) and (q) show a palmprint image captured from different user,used as a decryption key, and (m) and (r) the randomly decrypted image.

As a result, the proposed scheme has proven its robustness against imposter decryption since the imposter-decrypted image has high degree of randomness. Whereas the encrypted fingerprint image can be successfully reconstructed only if the POC between enrollment and verification palmprint images is sufficiently high (*i.e.* the two images belonging to the same user), otherwise, the encrypted fingerprint image becomes a random image.

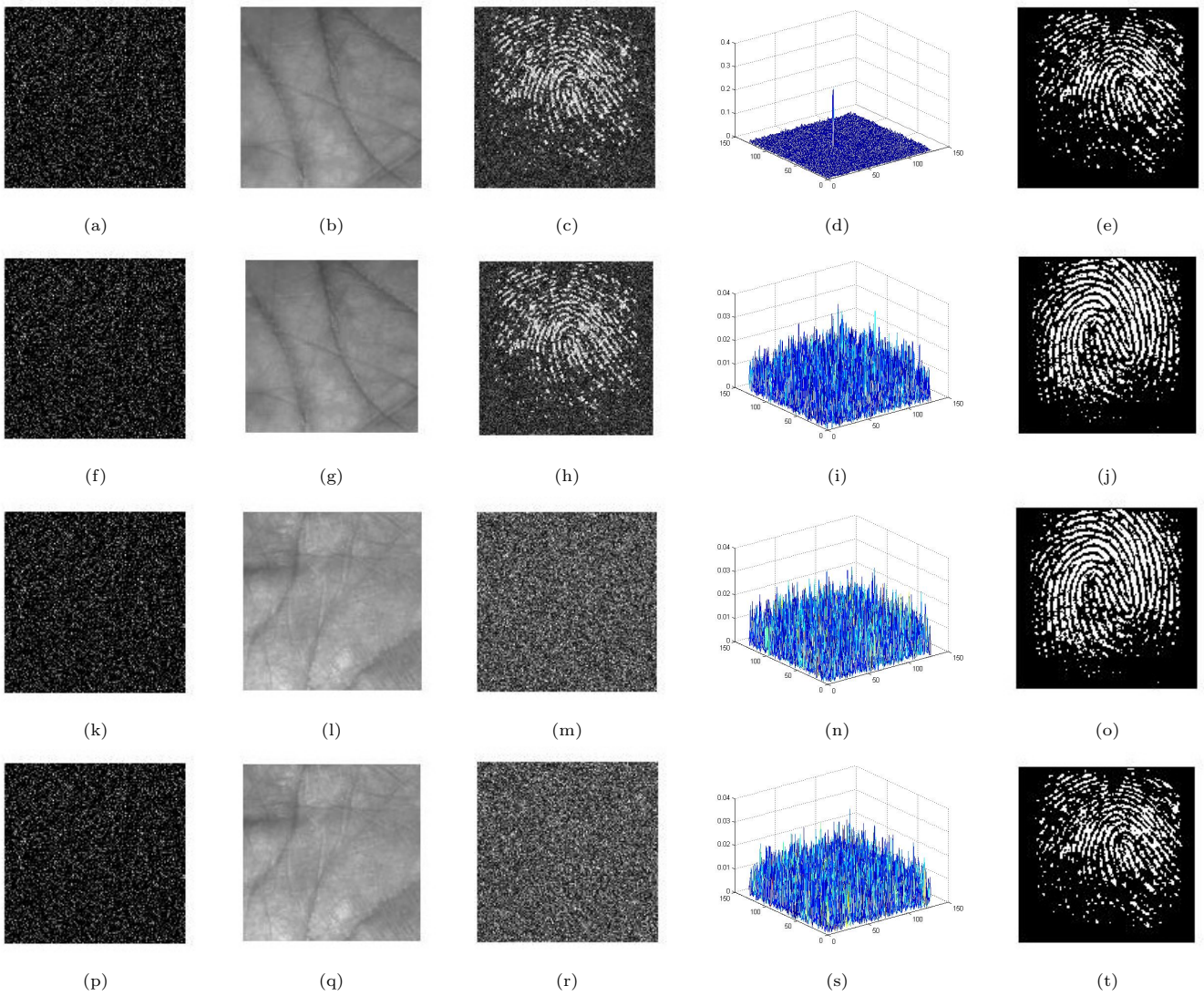
4.3 Matching Score Calculation

After decryption, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC-based image matching function to calculate the matching score between matched images and the overall authentication process succeeds only if the matching result exceeds a predefined threshold. The height of correlation peak in POC function is a good similarity measure to calculate matching scores between matched images. Figure 9 also illustrates the matching scores of the four different decryption cases using POC function. Figure 9 (c) shows the correctly decrypted fingerprint image that matched against a geniune fingerprint image shown in Figure 9 (e) and Figure 9 (d) illustrates the poc similarity as a distinct sharp peak. Figure 9 (h) shows the correctly decrypted fingerprint image that matched against an imposter fingerprint image shown in Figure 9 (j) and Figurer 9 (i) illustrates the poc similarity as a random noise with lower peaks. Figure 9 (m) shows the randomly decrypted image that matched against an imposter fingerprint image shown in Figure 9 (o) and Figure 9 (n) illustratws the poc similarity as a random noise with lower peaks.Figure 9 (r) shows the randomly decrypted image that matched against a genuine fingerprint image shown in Figure 9 (t) and Figure 9 (s) illustrates the poc similarity as a random noise with lower peaks.



(a) (b) (c)

Figure 8: Examples of resultant images in Encryption process. (a) fingerprint image for enrollment, (b) palmprint image (encryption key) and (c) the encrypted image



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

(p) (q) (r) (s) (t)

Figure 9: Examples of resultant images, It is confirmed that the fingerprint image is reconstructed correctly using same individual's palmprint image for decryption, and nothing appears using different individual's palmprint image for decryption, (a) the encrypted image, (b) the same individual's palmprint image for decryption, (c) the correctly decrypted fingerprint image using (b), (d) POC similarity between (c) and (e), (e) the same individual's fingerprint image for verification, (f) the encrypted omage, (g) the same individual's palmprint image for decryption, (h) the correctly decrypted fingerprint image using (g), (i) POC similarity between (h) and (j), (j) different individual's fingerprint image for verification, (k) the encrypted image, (l) different individual's palmprint image for decryption, (m) the randomly decrypted image using (l), (n) POC similarity between (m) and (o), (o) different individual's fingerprint image for verification, (p) the encrypted image, (q) different individual's palmprint image for decryption, (r) the randomly decrypted image using (q), (s) POC similarity between (r) and (t), (t) the same individual's fingerprint image for verification.

As a result, the proposed method increases the system security since the user must present geniune fingerprint and palmprint images in order to successfully authenticate himself to the system. In other words, if some adversary manages to present a true image of one of the two modalities, he would not be able to pass the authentication unless he present a true sample of the other modality.

Since the BLPOC proves its effeiciency than POC by providing much higher correlation peaks.We implemented the proposed method using either POC and BLPOC to calculate the matching scores and evaluate verification accuracy of the proposed method in either case (POC and BLPOC). Figure 10 illustrates the matching score calculations of the four different decryption cases found in Figure 9 using POC and BLPOC matching functions.

4.4 Verification Accuracy

The performance of our proposed method is measured by using the false reject rate (FRR) and the false accept rate (FAR) criteria that calculated by:

$$FAR = \frac{N_{FN}}{N_S}$$

$$FRR = \frac{N_{FP}}{N_S}$$

Where N_{FN} is the number of the false negative trails, N_{FP} is the number of the false positive trails and N_S is the total number of trails in the experiment.

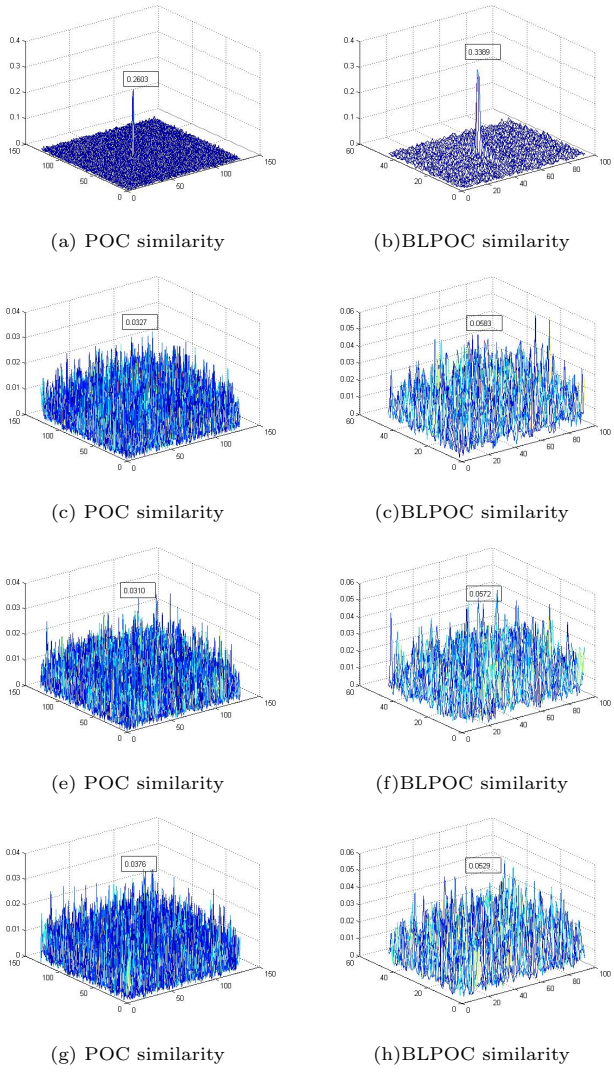
To test the efficacy of our proposed method, we implemented it using the same fingerprint image datasets of [22–25, 28] (1st and 2nd Databases) to make a comparison with the only existing fingerprint verification method that also based on DRPE scheme [22–25, 28]. The results in Table 1, shows that the verification accuracy of the proposed encoding method outperforms the existing fingerprint verification method also based on DRPE [22–25] by improving the little high FRR while keeping the FAR enough low, especially with the BLPOC matching function besides ensuring the security of biometric data without deteriorating the recognition accuracy by employing a multimodal system and also using POC image matching method that proved its effectiveness in low quality biometric images [1, 2, 6, 7, 21, 33] since it is highly robust against noise, image shift and brigthnes change. So it is very appropriate for matching decrypted fingerprint images that represent enrollment fingerprint images with some noise.

We also implemented the unimodal POC-based fingerprint matching [6], the unimodal POC-based palmprint matching [7] and POC-based multimodal fingerprint and palmprint score level fusion methods to make a comparison between them and our proposed multimodal encoding method. As illustrated in Table 1, we used the 1st and 2nd fingerprint image Datasets to check the effectiveness of using a mix of fingerprint and palmprint images for a secure template in our proposed method (POC and BLPOC) with POC-based fingerprint matching and POC-based palmprint matching. With the 1st dataset, we conduct 40 genuine trails and 280 imposter trails for all possible combinations and conduct 189 genuine trails and 3780 imposter trails for all possible combinations with the 2nd dataset. Table 1 shows the verification accuracy for each method using the two datasets.

From experimental results in Table 1, we can observe that the FRR of our proposed encoding method that secure a fingerprint image by a key extracted from a palmprint image is little high compared to the FRR of POC-based fingerprint matching because the restoration accuracy of the decrypted fingerprint image is related to the similarity between enrollment and authentication palmprint images, so that the encrypted fingerprint image can be successfully decrypted only if the phase-only-correlation between enrollment and authentication palmprint images is sufficiently high and hence the decrypted fingerprint image is similar, not exact to the enrolled fingerprint image. And hence this little high FRR can be acceptable specially with improving the security of biometric data by using DRPE and a multimodal system. Despite, the little FRR of POC-based multimodal score fusion that insecurely stores the enrollment fingerprint and palmprint images for verification, our proposed method can safely stores the enrollment fingerprint and palmprint images as a mix template for a secure verification.

We also tested our proposed method with three different fingerprint image datasets; using the same number of subjects for each dataset to check the robustness of the proposed method against shift and rotation variation in fingerprint images. We conduct 32 genuine trails and 224 imposter trails for all possible combinations in each dataset. Table 2 illustrated the verification accuracy of the proposed method for each dataset.

From experimental results in Table 2, the proposed method is based on POC image matching, which is shift invariant method. When authentication fingerprint image shifted from enrollment one, the correlation peak is shifted with the same translational displacement between two fingerprint images but the value of the correlation peak is not influenced by shift change. And thus the probability of accurate verification cannot influence with respect to image shift change. POC, on the other hand, is very sensitive to image rotation. So, image rotation cant be acceptable because the verification accuracy decreases remarkably and some improvements are required to achieve high tolerance for a variety of fingerprint images. Figure 11 shows the ROC curves for the experimental results from Tables 1 and 2.



(a) POC similarity (b)BLPOC similarity

(c) POC similarity (c)BLPOC similarity

(e) POC similarity (f)BLPOC similarity

(g) POC similarity (h)BLPOC similarity

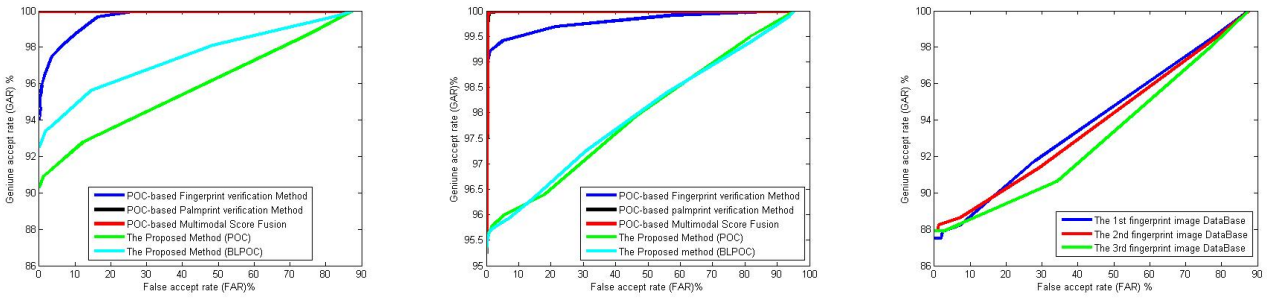
Figure 10: Matching score calculation between matched images using POC and BLPOC functions

Table 1: The verification accuracy of Experiment 1

Experiment.1	The 1st fingerprint image database FRR% at FAR%=0	The 2nd fingerprint image database FRR% at FAR%=0
POC-based Fingerprint image matching	5.63	3.25
POC-basedPalmprint image matching	0.0	0.63
POC-based multimodal score fusion	0.0	0.25
The proposed method (POC)	9.38	4.59
The proposed method (BLPOC)	7.50	4.43

Table 2: The verification accuracy of Experiment 2

Experiment.2	**The Proposed Method (POC)** FRR% at FAR%=0
The 1st fingerprint image database	9.77
The 2nd fingerprint image database	10.16
The 3rd fingerprint image database	11.33



(a) (b) (c)

Figure 11: ROC curves for: (a) the 1st dataset, (b) the 2nd dataset, (c) comparision between three different fingerprint datasets

5 Conclusions

This paper presented an optical template protection scheme, produces a secure biometric template as a mix of fingerprint image and palmprint image based on the principles of the optical (DRPE) scheme. Through the experimental results we confirmed that the verification accuracy of the proposed encoding method under genuine and imposter decryption was found to be effectively comparable with the existing fingerprint verification method that also based on the (DRPE) [22–25, 28] by effectively improving the FRR besides a higher level of security by using a multibiometrics and POC image matching.

References

[1] M. Abe, X. Zhang and M. Kawamata, "An efficient subpixel image registration based on the phase-only correlations of image projections," in *International Symposium on Communications and Information Technologies (ISCIT'10)*, pp. 997–1001, 2010.

[2] S. Almaadeed, I. Rida and A. Bouridane, "Gait recognition based on modified phase-only correlation," *Signal, Image and Video Processing*, vol. 10, no. 3, pp. 463–470, 2016.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[4] S. C. Draper, S. Rane, Y. Wang and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, 2013.

[5] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", *International Journal of Informatica*, vol. 12, no. 2, pp.297–302, Apr. 2001.

[6] K. Ito and *et al.*, "A fingerprint matching algorithm using phase-only correlation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 87, no. 3, pp. 682–691, 2004.

[7] K. Ito and *et al.*, "A palmprint recognition algorithm using phase-based image matching," in *IEEE International Conference on Image Processing*, pp. 2669–2672, 2006.

[8] R. Kumar and B. Bhaduri, "Double image encryption in fresnel domain using wavelet transform, gyrator transform and spiral phase masks," in *Fifth International Conference on Optical and Photonics Engineering*, pp. 104490O, June 2017.

[9] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181-2188, May 2010.

[10] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[11] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, July 2006.

[12] Z. Liu and *et al.*, "Image encryption algorithm by using fractional fourier transform and pixel scrambling operation based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 51, no. 1, pp. 8–14, 2013.

[13] X. Lu, P. Lu, Z. Xu and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 16, pp. 2514–2518, 2013.

[14] D. Maltoni, J. Wayman, A. Jain and D. Maio, "An introduction to biometric authentication systems," *Biometric Systems*, pp. 1–20, 2005.

[15] A. Nagar, *Biometric template security*, Michigan State University, Computer Science, 2012.

[16] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 3, 2011.

[17] P. Refregier and B. Javid, "Optical image encryption based on input plane and fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[18] P. Refregier and B. Javid, "Optical image encryption using input plane and fourier plane random encoding," in *Proceeding of SPIE*, pp. 767–769, 1995.

[19] Z. Shao and *et al.*, "Combining double random phase encoding for color image watermarking in quaternion gyrator domain," *Optics Communications*, vol. 343, pp. 56–65, 2015.

[20] K. Simoens and *et al.*, "Criteria towards metrics for benchmarking template protection algorithms," in *5th IAPR International Conference on Biometrics (ICB'12)*, pp. 498–505, 2012.

[21] S. A. Suandi, M. S. M. Asaari and B. A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," *Expert Systems with Applications*, vol. 41, no. 7, pp. 3367–3382, 2014.

[22] H. Suzuki and *et al.*, "Fingerprint verification for smart-card holders based on optical image encryption scheme," in *Proceeding of SPIE Vol*, vol. 5202, pp. 89, 2003.

[23] H. Suzuki and *et al.*, "File encryption software using fingerprint keys based on double random encoding," in *Frontiers in Optics*, pp. JWA50, 2005.

[24] H. Suzuki and *et al.*, "Experimental evaluation of fingerprint verification system based on double random phase encoding," *Optics Express*, vol. 14, no. 5, pp. 1755–1766, 2006.

[25] H. Suzuki and *et al.*, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack," *Optics Express*, vol. 18, no. 13, pp. 13772–13781, 2010.

[26] H. Suzuki, M. Takeda, K. Nakano and M. Yamaguchi, "Encrypted sensing based on digital holography for fingerprint images," *Optics and Photonics Journal*, vol. 5, no. 01, pp. 6, 2015.

[27] M. Takeda, K. Nakano and H. Suzuki, "Key-length analysis of double random phase encoding," *Applied Optics*, vol. 56, no. 15, pp. 4474–4479, 2017.

[28] M. Takeda and *et al.*, "Encoding plaintext by fourier transform hologram in double random phase encoding using fingerprint keys," *Journal of Optics*, vol. 14, no. 9, pp. 094003, 2012.

[29] S. Vashisth, H. Singh, A. K. Yadav and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," *Applied Optics*, vol. 53, no. 28, pp. 6472–6481, 2014.

[30] N. Wang and *et al.*, "A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images," in *International Symposium on Biometrics and Security Technologies (ISBAST'13)*, pp. 217–223, 2013.

[31] S. Yuan and *et al.*, "An optical authentication system based on encryption technique and multimodal biometrics," *Optics & Laser Technology*, vol. 54, pp. 120–127, 2013.

[32] G. Zhang, B. Javidi and J. Li, "Encrypted optical memory using double-random phase encoding," *Applied Optics*, vol. 36, no. 5, pp. 1054–1058, 1997.

[33] L. Zhang, L. Zhang and D. Zhang, "Fingerknuckleprint verification based on band-limited phase-only correlation," in *Computer Analysis of Images and Patterns*, pp. 141–148, 2009.

[34] W. Zhang, M. Zhang, B. Yang and T. Takagi, "Multibiometric based secure encryption, authentication scheme with fuzzy extractor," *International Journal of Network Security*, vol. 12, no. 1, pp. 50–57, 2011.

Biography

Eman Tarek. received her B.S. degree in 2012 in Department of information technology, Mansoura University, Egypt. She is currently pursuing here M.S. degree in information technology. Here current research interests include Pattern Recognition, Information Security, Biometrics.

Osama Ouda. received his B.S. in Computer Science from Mansoura University, Egypt, in 2000, his M.S. in Computer Science from Ain-Shams University, Egypt, in 2007, and his Ph.D. in Computer and Information Sciences from Chiba University, Japan, in 2011. From November 2013 to May 2014, he was a research fellow at iPRoBe laboratory, Michigan State University, East Lansing, USA. Currently, he is an assistant professor in the Department of Information Technology, Mansoura University, Egypt. Dr. Ouda is a member of IEEE since 2011. His research interests include information security,biometrics, image processing and machine learning.

Ahmed Atwan. received his B.S degree in 1988, his M.S. degree in 1998 and Ph.D degree in 2004, all in Department of Communications and Electronics Engineering, Mansoura University, Egypt. His current research interests include Networking, Expert Systems, Biometrics, and Machine Learning.

An Efficient Protocol for Privately Determining the Relationship Between Two Straight Lines

Ledi Fang[1], Shundong Li[1], Wenli Wang[2]
(Corresponding author: Shundong Li)
School of Computer Science, Shaanxi Normal University[1]
No. 620 Xi Chang'an Street, Xi'an 710119, China
(Email: shundong@snnu.edu.cn)
School of Mathematics and Information Science, Shaanxi Normal University[2]
(Received July 13, 2017; revised and accepted Oct. 22, 2017)

Abstract

Secure multiparty computation (SMC) is now a research focus in the international cryptographic community. SMC makes participants perform secure computation without revealing their own private data. In this paper, we discuss a secure computational geometry problem, that is, to privately determine whether two straight lines intersect. This is a basic and important SMC problem. Almost all protocols addressing this problem are applicable for integers, which limits their applications. So, we propose an efficient scheme for rational numbers. We proved that the protocol is secure under the semi-honest model by using the simulation paradigm. In addition, we propose a protocol which can be applied to space problems. This protocol can be used as a building block to construct new protocols to solve some space problems. Finally, we analyze the computational complexity and communication complexity of the protocol, and present an experimental result.

Keywords: Secure Multi-party Computation; Simulation Paradigm; Straight Line Intersection

1 Introduction

Secure Multiparty Computation (SMC) [3] was initially introduced by Yao as the millionaires' problem [16] in 1982 for two parties. Then Ben and Goldwasser [2] extended SMC to multiple parties and established the theoretical basis of SMC [5, 13]. The heart of SMC is that parties can cooperatively compute a function of their own private data without disclosing any private information. Hence, the paries are able to maximize their interests while protecting their data privacy.

Privacy-preserving computational geometry is a promising research area of SMC. It mainly focuses on protecting the security of computational geometry. Many privacy-preserving computational geometry problems have been studied, such as point-inclusion, intersection of two convex polygons, convex hulls. Du [1] introduced the problem of the intersection of two straight lines. Later, Luo [10] presented and solved the problem.

The relationship between two straight lines has significant application in practice. For instance, the spy of Country A observes activity an route L_1 while another spy in Country B observes an activity route L_2. They are willing to cooperate to figure out whether L_2 is relevant to L_1 and the result is helpful for both countries to understand the trend of the target's behaviors, such as some suspected terroristic organizations, the military dynamics of a dangerous country. However, neither A nor B wants to disclose its observation to each other because they don't believe each other. It is possible that Country B exploits the intelligence information of Country A (or sells it to the target) to expose the spy of Country A, resulting in the spy being persecuted. So the problem of the relationship between two straight lines is of great significance.

A number of scholars have proposed protocols for this problem. For example, Luo introduced and solved the problem of the intersection of two straight lines. The protocol is helpful, but it only works for integer points on the lines [10]. In our real life, we usually choose some rational points on the lines to meet the needs of numerous practical applications. So we propose an efficient protocol based on the plane geometry to solve this problem. Then we use the simulation paradigm to prove the security of the protocol. In addition, we propose a protocol which can be applied to some space problems. This protocol can be used as a building block to construct new protocols to solve some space problems. Finally, we present the computation and communication complexity of different protocols and show an experimental result.

2 Preliminaries

2.1 Security

Two-party Computation. Two-party computation is a random mapping process where a random input pair is mapped to a random output pair, which is represented below:

$$f : \{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1\}^* \times \{0,1\}^*$$

That is to say, for an arbitrary given input pair, the function will output a pair of random variables $(f_1(x,y), f_2(x,y))$. The function is denoted as

$$(x,y) \longrightarrow (f_1(x,y), f_2(x,y))$$

Semi-honest parties [8]. Our work assumes that all parties are semi-honest. loosely speaking, a semi-honest party is one that follows the protocol properly, except that it keeps a records of all its intermediate computations and might try to derive the other parties' private inputs from the record. Goldreich [4] proved that, given a protocol that privately computes functionality f in the semi-honest model, we can construct a protocol by introducing macros that force each party either to behave in the semi-honest manner or to be detected, by which case we can privately compute functionality f in the malicious model. The semi-honest model is not merely an important methodological locus but may also provide a good model for many settings. It suffices to prove that a protocol is secure in the semi-honest setting.

Privacy by simulation [8]. Intuitively, a protocol is private if what a party can efficiently compute by participating in the protocol can also be efficiently computed from its input and output only. This assumption is formalized by the simulation paradigm, which requires that a party's view in a protocol execution can be simulated by its input and output only. If so, the parties learn nothing from the protocol execution itself, and the protocol is secure.

Definition 1. *For a functionality f, π privately computes f if there exist probabilistic polynomial-time algorithms, denoted by S_1 and S_2 such that*

$$\{S_1(x, f_1(x,y)), f_2(x,y)\}_{x,y}$$

$$\stackrel{c}{\equiv} \{view_1^{\pi}(x,y), output_2^{\pi}(x,y)\}_{x,y} \quad (1)$$

and

$$\{f_1(x,y)), S_2(y,(x,y))\}_{x,y}$$

$$\stackrel{c}{\equiv} \{view_1^{\pi}(x,y), output_2^{\pi}(x,y)\}_{x,y} \quad (2)$$

where $\stackrel{c}{\equiv}$ denotes computational indistinguishability, $view_1^{\pi}(x,y)$ and $view_2^{\pi}(x,y)$, $output_1^{\pi}(x,y)$ and $output_2^{\pi}(x,y)$ are related random variables, defined as a function of the same random execution.

2.2 A Symmetric Cryptographic Solution to Determine Whether Two Numbers Are Equal

Li *et al.* [9] proposed a secure solution to determine whether two numbers are equal by using XOR operations. This cryptographic protocol is much more efficient than others because the computational complexity of symmetric encryption is much lower than that of public key encryption. We use this scheme as a basic module to design Protocol 3 in Section 3. Li's protocol is as follows:

Protocol 1: A symmetric cryptographic solution to determine whether two numbers are equal.

Inputs: Alice has a number a, Bob has a number b.

Output: Whether $a = b$.

Setup: Alice and Bob choose random numbers $r \in \{0,1\}^m$ and $s \in \{0,1\}^n (m, n > 64)$, respectively, and compute $c = a \oplus r$, $d = b \oplus s$. Then exchange c and d.

Encryption Process: Alice and Bob compute $a' = d \oplus r = b \oplus s \oplus r$, $a' = c \oplus s = a \oplus r \oplus s$, respectively. Then they use hash to compute $hash(a')$ and $hash(b')$, respectively. Finally, they exchange $hash(a')$ and $hash(b')$.

Decryption Process: Alice and Bob judge whether $hash(a') = hash(b')$. If it holds, then $a = b$; otherwise $a \neq b$.

2.3 Area of the Triangle In the Plane

There are three points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$ with rational coordinates. The area of the triangle constituted by these three points can be computed as follows:

$$S_{\triangle P_1 P_2 P_3} = \frac{1}{2}[y_1(x_3 - x_2) + x_1(y_2 - y_3) + x_2 y_3 - x_3 y_2] \quad (3)$$

If $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$ is in counterclockwise order, then the area value is positive; otherwise the area value is negative.

2.4 Protocol Based on the Formula for the Area of the Triangle In the Plane

Li *et al.* proposed a protocol [7] for securely computing the area of a triangle, but the protocol discloses the slope. Then they improved and developed the protocol [6]. We use this protocol as a basic module to design Protocol 3 in Section 3. The protocol is as follows:

Protocol 2: Securely compute Area of a Triangle in the Plane.

Inputs: Alice' s input is point $P_1(x_1, y_1)$, and Bob' s inputs are point $P_2(x_2, y_2)$ and point $P_3(x_3, y_3)$.

Output: $S_{\triangle P_1P_2P_3}$.

Setup: Paillier's homomorphic encryption scheme (G, E, D), Bob runs $G(\tau)$ (τ is the given security parameter) to generate a key pair (p_k, s_k).

Encryption Process:

Bob executes the following:

1) Computes $a = x_3 - x_2$, $b = y_2 - y_3$, $c = x_2y_3 - x_3y_2$. It is straightforward that the signs of a and b are different. We assume that $a > 0$, $b < 0$.
2) Chooses a random number r ($r \in Z_n^*$) such that $b_1 = b + r > 0$.
3) Uses the public key p_k to encrypt a and b_1, the results are denoted by $E(a)$ and $E(b_1)$, and then sends $E(a)$, $E(b_1)$, r and p_k to Alice.

Alice computes

$$\begin{aligned} E(S_1) &= E(ay_1 + b_1x_1) = E(a)^{y_1} \cdot E(b_1)^{x_1} \\ R &= rx_1 \end{aligned}$$

and then sends $E(S_1)$ to Bob.

Decryption Process:

Bob decrypts $E(S_1)$

$$S_1 = ay_1 + b_1x_1 = ay_1 + b_1x_1 + rx_1$$

and computes

$$S_2 = S_1 + c = ay_1 + b_1x_1 + c + rx_1$$

Bob sends S_2 to Alice.

Alice computes

$$S_{\triangle P_1P_2P_3} = \frac{1}{2}(S_2 - R) = \frac{1}{2}(ay_1 + b_1x_1 + c)$$

Alice tells Bob the result.

3 Determining the Relationship Between Two Straight Lines and Its Extension

In this section, we aim at solving the problem of privately determining the relationship between two straight lines. That is, Alice and Bob desire to determine the relationship between their own lines without disclosing the lines' information. This problem can be generalized as follows. Alice has $L_1 : y = k_1x + b_1$ and Bob has $L_2 : y = k_2x + b_2$. They want to know whether these two lines intersect. In addition, they want to know whether $L_1 // L_2$ or $L_1 \perp L_2$ without disclosing information about the lines. Many protocols have been put forward in recent years to solve this problem. Luo [10] put a scheme with high computational complexity. Yang [15] improved the protocol by using Paillier homomorphic encryption [14]. The Paillier public key encryption has additively homomorphic [11] property. Yang's protocol is of high computational complexity due to many modular exponentiation operations. Although Luo and Yang's protocols solved the problem, their protocols are only limited to the integer field. In real life, $k_1(k_2)$ or $b_1(b_2)$ are more likely to be rational numbers. The existing protocols are not applicable. So it's necessary to design a protocol to meet this requirement and we propose a protocol to solve this problem.

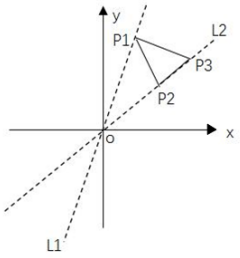


Figure 1: Two lines intersect

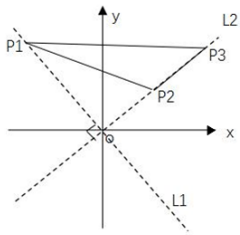


Figure 2: Two perpendicular lines

3.1 An Efficient Protocol for Determining the Relationship Between Two Straight Lines

Alice has a private line $L_1 : y = k_1x + b_1$ where k_1 and b_1 are rational numbers, Bob has a private line $L_2 : y = k_2x + b_2$ where k_2 and b_2 are also rational numbers. They can separately and secretly compare the slopes and intercepts. The two lines are parallel if they have the same slopes and different intercepts. They are coincident if they have the same slopes and intercepts. Otherwise, the two lines intersect or may be perpendicular.

In the latter situation, Alice and Bob separately shift L_1 and L_2 to go through the origin. Alice randomly chooses a point denoted by $P_1(x_1, y_1)$ on L_1, Bob randomly chooses two points denoted as $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$ on L_2. These three points constitute a triangle $\triangle P_1P_2P_3$. We denote the height of $\triangle P_1P_2P_3$ by h, the area of $\triangle P_1P_2P_3$ by $S_{\triangle P_1P_2P_3}$. $h = \frac{2S_{\triangle P_1P_2P_3}}{\overline{P_2P_3}}$. We determine whether $h = \overline{op_1}$ (See Figure 1 and Figure 2).

If $h = \overline{op_1}$, L_1 and L_2 are perpendicular.

If $h \neq \overline{op_1}$, L_1 and L_2 intersect.
In order to describe clearly, we define

$$P(L_1, L_2) = \begin{cases} 0, & L_1, L_2 \text{ intersect} \\ 1, & L_1, L_2 \text{ are parallel} \\ 2, & L_1, L_2 \text{ are coincident} \\ 3, & L_1, L_2 \text{ are perpendicular} \end{cases}$$

Protocol 3: An Efficient Protocol for Determining the Relationship between Two Straight Lines

Inputs: Alice' s private line $L_1 : y_1 = k_1 x + b_1$, Bob' s private line $L_2 : y_2 = k_2 x + b_2$.

Output: $P(L_1, L_2)$

Setup: Suppose that $k_1 = \frac{u_1}{v_1}$ where $\gcd(u_1, v_1) = 1$, and $k_2 = \frac{u_2}{v_2}$ where $\gcd(u_2, v_2) = 1$. Alice and Bob use Protocol 1 to compare whether $u_1 = u_2$, $v_1 = v_2$, respectively. If $u_1 = u_2$ and $v_1 = v_2$, then $k_1 = k_2$. Similarly, Alice and Bob determine whether $b_1 = b_2$. If $k_1 = k_2$ and $b_1 = b_2$, then L_1 and L_2 are coincident. Otherwise, Alice and Bob do the following.

Alice and Bob separately shift L_1 and L_2 to go through the origin. Alice randomly chooses a point $P_1(x_1, y_1)$ on L_1, and Bob randomly chooses two points denoted by $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$ on L_2. These three points constitute a triangle $\triangle P_1P_2P_3$.

Encryption Process: Alice and Bob use Protocol 2 to privately compute the area of $\triangle P_1P_2P_3$.

Decryption Process: Bob computes h, and Alice computes $\overline{op_1}$. Then they use protocol 1 to determine whether $h = \overline{op_1}$. If

$$h = \overline{op_1}$$

L_1 and L_2 are perpendicular. Otherwise, L_1 and L_2 intersect. Then they can get the result of $P(L_1, L_2)$.

Thus, it's important for us to use the idea, but almost all protocols used to address this problem only work for planes. This limits their applications. Thus, we propose an efficient protocol for spaces.

3.2 A Secure Computational Protocol for Triangle Area in Spaces

By the formula, the area of the triangle constituted by three rational points $P_1(x_1, y_1, z_1)$, $P_2(x_2, y_2, z_2)$ and $P_3(x_3, y_3, z_3)$ in spaces is as follows:

$$S_{\triangle P_1P_2P_3} = \frac{1}{2}\sqrt{\begin{vmatrix} y_1 & z_1 & 1 \\ y_2 & z_2 & 1 \\ y_3 & z_3 & 1 \end{vmatrix}^2 + \begin{vmatrix} z_1 & x_1 & 1 \\ z_2 & x_2 & 1 \\ z_3 & x_3 & 1 \end{vmatrix}^2 + \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}^2} \quad (4)$$

which yields:

$$\begin{aligned} S_{\triangle P_1P_2P_3} &= \frac{1}{2}\{[x_1(y_2 - y_3) + y_1(x_3 - x_2) + y_2x_3 - y_3x_2]^2 \\ &\quad + [y_1(z_2 - z_3) + z_1(y_3 - y_2) + y_2z_3 - y_3z_2]^2 \\ &\quad + [z_1(x_2 - x_3) + x_1(z_3 - z_2) + z_2x_3 - z_3x_2]^2\}^{\frac{1}{2}}. \end{aligned}$$

We design a protocol to securely computes the area of a space triangle, and it is shown as follows.

Protocol 4: An efficient protocol for computing the space triangle area

Inputs: Private rational points $P_1(x_1, y_1, z_1)$, $P_2(x_2, y_2, z_2)$ and $P_3(x_3, y_3, z_3)$, where Alice has P_1 and Bob has P_2, P_3.

Output: $S = \frac{1}{2}\{[x_1(y_2 - y_3) + y_1(x_3 - x_2) + y_2x_3 - y_3x_2]^2 + [y_1(z_2 - z_3) + z_1(y_3 - y_2) + y_2z_3 - y_3z_2]^2 + [z_1(x_2 - x_3) + x_1(z_3 - z_2) + z_2x_3 - z_3x_2]^2\}^{\frac{1}{2}}$

Encryption Process:

Bob does the following:

1) Randomly chooses a random number $k \in Z_n^*$. (k is accurate to three decimal places.)
2) Computes

$$\begin{aligned} a &= y_3 - y_2, b = x_3 - x_2, c = y_2x_3 - y_3x_2 \\ d &= z_3 - z_2, e = y_2z_3 - y_3z_2, f = z_2x_3 - z_3x_2 \end{aligned}$$

and constitutes vectors

$$A = ((-ak, bk), (-dk, ak), (-bk, dk))$$

3) Sends A to Alice.

Alice randomly chooses three random numbers r_1,r_2,$r_3 \in Z_n^*$, and computes

$$\begin{aligned} T_1 &= -akx_1 + bky_1 + r_1 \\ T_2 &= -dky_1 + akz_1 + r_2 \\ T_3 &= -bkz_1 + dkx_1 + r_3 \end{aligned}$$

Then Alice sends T_1, T_2, T_3 to Bob.

Bob computes

$$\begin{aligned} T_1' &= T_1 + kc \\ T_2' &= T_2 + ke \\ T_3' &= T_3 + kf \end{aligned}$$

and sends T_1', T_2', T_3' to Alice.

Alice computes

$$\begin{aligned} D_1 &= T_1' - r_1 \\ D_2 &= T_2' - r_2 \\ D_3 &= T_3' - r_3 \\ T &= D_1^2 + D_2^2 + D_3^2 \end{aligned}$$

and tells T to Bob.

Decryption Process: $S = \frac{1}{2k}T^{\frac{1}{2}} = \frac{1}{2}\{[x_1(y_2-y_3)+y_1(x_3-x_2)+y_2x_3-y_3x_2]^2+[y_1(z_2-z_3)+z_1(y_3-y_2)+y_2z_3-y_3z_2]^2+[z_1(x_2-x_3)+x_1(z_3-z_2)+z_2x_3-z_3x_2]^2\}^{\frac{1}{2}}$ and tells the result to Alice.

Correctness: By Formula (4), the area of $\triangle P_1P_2P_3$ can be computed from $P_1(x_1, y_1z_1)$, $P_2(x_2, y_2, z_2)$ and $P_3(x_3, y_3, z_3)$. So Protocol 4 is correct.

Privacy: In order to analyse the security, we check whether each party can obtain the others' private information by executing Protocol 4. A brief analysis of the privacy of Protocol 4 is given as follows.

According to Protocol 4, Alice are supposed to receive a, b, d that contain Bob's unknown variables: $x_2, x_3, y_2, y_3, z_2, z_3$. It is obvious that the six unknown variables cannot be derived from three equations. Therefore, Alice cannot obtain Bob's secret points.

Bob can only gain Alice's information from three equations as follows:

$$T_1 = -akx_1 + bky_1 + r_1$$

$$T_2 = -dky_1 + akz_1 + r_2$$

$$T_3 = -bkz_1 + dkx_1 + r_3$$

Because of the random numbers r_1, r_2, r_3 which Alice adds, it is impossible for Bob to obtain Alice's secret point the six unknown variables$(x_1, y_1, z_1, r_1, r_2, r_3)$ from the three equations. Therefore, Bob cannot obtain Alice's secret points. This demonstrates that protocol 4 is private.

Thus, they can securely compute the area of a triangle in the space.

3.3 Applications

As mentioned above, Protocol 4 can be used as a building block to construct new protocols to solve some space problems such as the problem of the intersection of a line and a plane. This problem is as follows:

Alice has a line $L : \frac{x-x_0}{X} = \frac{y-y_0}{Y} = \frac{z-z_0}{Z}$. Bob has a plane $\pi : Ax+By+Cz+D = 0$. They want to determine the relationship between the line and the plane without revealing their private data.

Firstly Bob finds out the line L_3 of the normal vector of the plane. They can separately shift L and L_3 to go through the origin, and use Protocol 4 to determine the relationship between L_3 and L. Thereby the relationship between the line and the plane is obtained.

In order to describe clearly, we define

$$P(L,\pi) = \begin{cases} 0, & L, \pi \text{ intersect} \\ 1, & L, \pi \text{ are parallel or coincident} \\ 2, & L, \pi \text{ are perpendicular} \end{cases}$$

Protocol 5: A Scheme for Determining the Relationship between a line and a plane.

Inputs: Alice' s private line $L : \frac{x-x_0}{X} = \frac{y-y_0}{Y} = \frac{z-z_0}{Z}$, Bob' s private plane $\pi : Ax + By + Cz + D = 0$.

Output: $P(L, \pi)$

Encryption Process:

Bob finds out the of normal vector L_3 of the plane. Then they separately shift L and L_3 to go through the origin. Bob randomly chooses two points $P_4(x_4, y_4, z_4)$ and $P_5(x_5, y_5, z_5)$ on L_3. Alice randomly chooses a point $P_6(x_6, y_6, z_6)$.

Decryption Process:

Alice and Bob use Protocol 4 to compute the area of $\triangle P_4P_5P_6$. And then they determine the relationship between L and L_3.

1) If L and L_3 are parallel or coincident , then L and π are perpendicular.
2) If L and L_3 intersect, then L and π intersect.
3) If L and L_3 are perpendicular, then L and π are parallel or L is in the π.

Similarly, we can utilize the idea to solve the problem of determining the relationship of two planes in spaces.

4 Security

In this section, we use the simulation paradigm to prove that Protocol 3 is secure.

Theorem 1. *Protocol 3 can securely determine the relationship of straight lines.*

Proof. Alice and Bob respectively construct two simulators, S_1 and S_2 which make Equations (1) and (2) hold.

In Protocol 3:

$$\begin{aligned} view_1^{\pi}(L_1, L_2) &= \{L_1, hash(\overline{k}), hash(\overline{b}), S_{\triangle}, \overline{op_1}, \\ &\quad hash(\overline{h}), P(L_1, L_2)\} \\ f_1(L_1, L_2) &= f_2(L_1, L_2) \\ &= output_1^{\pi}(L_1, L_2) \\ &= output_2^{\pi}(L_1, L_2) \\ &= P(L_1, L_2). \end{aligned}$$

L_1, L_2 are the inputs of Alice and Bob. Alice got $S_{\triangle}$ when Protocol 2 finished.

Bob sent $hash(\overline{k})$ and $hash(\overline{b})$ to the Alice when they comparing whether $k_1 = k_2$, $b_1 = b_2$. In addition, Bob sent $hash(\overline{h})$ to the Alice when they comparing whether $h = \overline{op_1}$.

Alice constructs S_1. S_1 performs the following simulation.

1) By $f(L_1, L_2)$, S_1 randomly chooses a line L_2' such that $P(L_1, L_2') = P(L_1, L_2)$. Suppose that $L_2' : y' = k_2'x + b_2'$.

2) Suppose that $k_2' = \frac{u_2'}{v_2'}$ where $\gcd(u_2', v_2') = 1$. S_1 compare whether $u_1 = u_2'$, $v_1 = v_2'$. Then S_1 randomly chooses two points $P_2'(x_2', y_2')$and $P_3'(x_3', y_3')$ on L_2'.

3) S_1 computes $S'_{\triangle} = \frac{1}{2}[y_1(x_3' - x_2') + x_1(y_2' - y_3') + x_2'y_3' - x_3'y_2']$.

Clearly, $S'_{\triangle} \neq 0$. Then S_1 computes h' and $\overline{op_1'}$. In addition, S_1 determine whether $h' = \overline{op_1'}$.

Let

$$S_1(L_1, f_1(L_1, L_2)) = \{L_1, hash(\overline{k}'), hash(\overline{b}'), S'_{\triangle}, \overline{op_1}, hash(\overline{h}'), P(L_1, L_2)\}.$$

Since the selected points are random points and Protocol 1 has been proved, then

$$hash(\overline{k}) \stackrel{c}{\equiv} hash(\overline{k}'),\ hash(\overline{b}) \stackrel{c}{\equiv} hash(\overline{b}')$$

$$S_{\triangle} \stackrel{c}{\equiv} S'_{\triangle},\ hash(\overline{h}) \stackrel{c}{\equiv} hash(\overline{h}')$$

thus,

$$\{S_1(L_1, P(L_1, L_2), f_1(L_1, L_2)), f_2(L_1, L_2)\}$$

$$\stackrel{c}{\equiv} \{view_1^{\pi}(L_1, L_2), output_2^{\pi}(L_1, L_2)\}$$

Similarly, the simulator such that Eq.(2) holds can be constructed analogously, thus,

$$\{f_1(L_1, L_2), S_2(L_2, f_2(L_1, L_2))\}$$

$$\stackrel{c}{\equiv} \{output_1^{\pi}(L_1, L_2), view_1^{\pi}(L_1, L_2)\}$$

This completes the proof of the theorem. □

5 Efficiency Analysis

5.1 Theoretical Analysis

Computational complexity . There are many protocols such as Luo's scheme and Yang's scheme [15] determining the relationship between two lines. Luo's scheme was put forward at first, then Yang greatly improved recently. So we compare our protocols with Luo's scheme and Yang's scheme.

Luo's [10] scheme uses the scalar product protocol [1] for n times. The scalar product protocol utilizes an efficient oblivious transfer [12]. Suppose that the security parameter is p. Every invocation of scalar product protocol needs to use 1-out-of-k oblivious transfer p times. It needs $\lg k$ 1-out-of-2 oblivious transfer for a 1-out-of-k oblivious transfer. Each 1-out-of-2 oblivious transfer needs two modular exponentiation operations at least.

Therefore, Luo's Scheme needs at least $2p \lg k$ modular exponentiation operations. In order to meet the security requirement, Luo's scheme requires $p > 5$ and $k > 8$. So, Luo's scheme requires 30 modular exponentiation operations at least.

Yang's scheme uses the Paillier homomorphic encryption. Yang's protocol 3 (Yang 3) encrypts 3 times and decrypts 6 times to determine the relationship between two straight lines. That is to say, it uses 12 modular exponentiation operations in total.

Our Protocol 3 uses XOR operations so it greatly reduces the computational complexity. Protocol 3 uses at most 8 modular exponentiation operations for computing the area of the triangle. In addition, our protocols can be utilized in rational field while Luo's scheme and Yang's scheme does not work in rational field.

Communication Complexity. Communication complexity, i.e. communication rounds, is an important factor to evaluate secure multiparty computation solutions. Luo's scheme needs p rounds. Yang's scheme requires 2 round communications. Our protocols also require 2 round communications. Table 1 summarizes the comparison.

5.2 Simulation Result

In this section, we present an experimental result in terms of efficiency. Since Yang's scheme is much more efficient than Luo's scheme, we only compare our protocols with Yang's Scheme.

Experimental Settings: All the experiments are conducted on an HP PC with 3.30 GHz Intel Core i5-6600 processor with 8 GB RAM running a 64-bit Windows 10 Enterprise. The program code is written in Java.

Time Complexity Analysis: Our protocols can be used in the rational field. Supposed that Alice selects a point (16.5,13.2) on her line and Bob chooses two points (14.4,10.8) and (9.6,7.2) on his line. We run the experiment for 10000 times and randomly pick up 10 sets of data and the result is shown in Figure 3. Yang's scheme does not work in rational field, so we choose some integers to test. We assume that in the Paillier homomorphic encryption scheme the two large primes p and q are 256 bits. Suppose that Alice selects a point (17,13) on her line and Bob chooses two points (11,8) and (10,7) on his line. We run the experiment for 10000 times and randomly pick up 10 sets of data and the result is shown in Figure 3.

Table 1: Comparison of the computational and communication complexity

	Luo's scheme	Yang 3	Protocol 3
Computational Complexity	$2p \lg k$	12	8
Communication Complexity	p	2	2

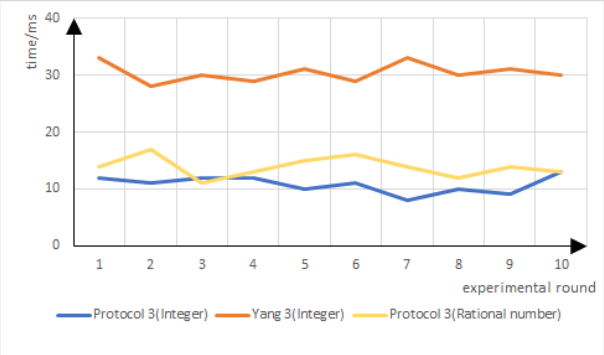


Figure 3: The comparison of Protocol 3 and Yang 3

The results of this experiment validate that our protocols are more efficient.

6 Conclusion

In this paper, we proposed an efficient protocol to privately determine the relationship between two straight lines. The protocol improves the efficiency by utilizing XOR operations and the idea of computing the area of a triangle in the planes. Also, we presented a protocol to compute the area of a triangle in the spaces. In addition, the two protocols can be used in rational field. Then we utilized simulation paradigm to prove the security and did experiment to show the efficiency of Protocol 3. In the future, We will discuss the problem of the relationship between two straight lines in the malicious model.

References

[1] M. J. Atallah, W. L. Du, "Secure multi-party computational geometry," in *Algorithms and Data Structures, Springer Berlin Heidelberg*, pp. 165–179, 2001.

[2] M. Ben-Or, S. Goldwasser, A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pp. 1–10,1988.

[3] W. L. Du, M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in *ACM Proceedings of the 2001 workshop on New security paradigms*, pp. 13–22, 2001.

[4] O. Goldreich, *Foundations of Cryptography: Basic Applications*, Cambridge University Press, London, 2004.

[5] S. N. Kumar, "Review on network security and cryptography," *International Transaction of Electrical and Computer Engineers System*, vol. 3, no. 1, pp. 1–11, 2015.

[6] S. D. Li, Y. M. Guo, S. F. Zhou, J. W. Dou, D. S. Wang, "Efficient protocols for the general millionaires' problem," *Chinese Journal of Electronics*, vol. 24, no. 4, pp. 598–604, 2015.

[7] S. D. Li, D. S. Wang, Y. Q. Dai, "Efficient secure multiparty computational geometry," *Chinese Journal of Electronics*, vol. 19, no. 2, pp. 324–328, 2010.

[8] S. D. Li, D. S. Wang, Y. Q. Dai, P. Luo, "Symmetric cryptographic solution to Yaos millionaires' problem and an evaluation of secure multiparty computations," *Information Sciences*, vol. 178, no. 1, pp. 244–255, 2008.

[9] S. D. Li, X. L. Yang, X. J. Zuo, S. F. Zhou, J. Kang, X. Liu, "Privacy protecting similitude determination for Graphics Similarity," *Chinese Journal of Electronics*, vol. 45, no. 9, pp. 2184–2189, 2017.

[10] Y. L. Luo, L. S. Huang, W. W. Jing, W. J. Xu, "Privacy protection in the relative position determination for two spatial geometric objects," *Computer Research and Development*, vol. 43, no. 3, pp. 410–416, 2006.

[11] Y. L. Luo, L. S. Huang, W. Yang, W. J. Xu, "An efficient protocol for private comparison problem," *Chinese Journal of Electronics*, vol. 18, no. 2, pp. 205–209, 2009.

[12] M. Naor, B. Pinkas, "Oblivious transfer and polynomial evaluation," in *ACM Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, pp. 245–254, 1999.

[13] R. Sharma, "Review paper on cryptography," *International Journal of Research*, vol. 2, no. 5, pp. 141–142, 2015.

[14] J. H. Wu, P. Zhang, X. B. Shi, "Research of MA protection based on addition-multiplication homomorphism and composite function technology," *Journal of Chinese Computer Systems*, vol. 33, no. 10, pp. 2223–2226, 2012.

[15] X. L. Yang, S. D. Li, X. J. Zuo, "Secure multi-party geometry computation," *Journal of Cryptologic Research*, vol. 3, no. 1, pp. 33–41, 2016.

[16] A. Yao, "Protocols for secure computations," in *IEEE Proceeding of the 23th IEEE Annual Symposium on Foundations of Computer Science*, pp. 160–164, 1982.

Biography

Ledi Fang was born in 1993. She is currently pursuing the M.S. degree with School of Computer Science in Shaanxi Normal University. Her research interests focus on secure multi-party computation and information security.

Shundong Li was born in 1963. He received the Ph.D. degree in Department of computer science and technology from Xian JiaoTong University in 2003. He is now a Professor with School of Computer Science in Shaanxi Normal University. His research interests focus on modern cryptography and secure multi-party computation.

Wenli Wang was born in 1991. She is currently pursuing the M.S. degree with School of Mathematics and Information Science in Shaanxi Normal University. Her research interests focus on modern cryptography and applied mathematics.

A Provable Secure Identity-based Generalized Proxy Signcryption Scheme

Caixue Zhou, Yue Zhang, and Lingmin Wang
(Corresponding author: Caixue Zhou)

School of Information Science and Technology, Jiujiang University
551 Qianjin Donglu, Jiujiang 332005, China
(Email: charlesjjjx@126.com)

(Received July 8, 2017; revised and accepted Oct. 22, 2017)

Abstract

Generalized proxy signcryption (GPSC) can realize both proxy signature and proxy signcryption with only one key pair and one algorithm, which significantly improves the efficiency of a system with a large number of users, or with limited storage space, or whose functions may be changed. In this paper, we propose an identity-based GPSC scheme in the random oracle model by using bilinear pairings. Our scheme can perform public verification in proxy signcryption mode, resist proxy key exposure attacks, resist insider attacks and support self-delegation. What is more, it needs no secure channel between the original person and the proxy person. Under the adaptive chosen ciphertext, chosen identity and chosen warrant attacks, the confidentiality of our scheme can be reduced to the GBDH hard problem. Under the adaptive chosen message, chosen identity and chosen warrant attacks, the unforgeability of our scheme can be reduced to the GDH' hard problem. We compare our scheme in proxy signcryption mode with other identity-based proxy signcryption schemes that use bilinear pairings, and the results show that it is practical.

Keywords: Bilinear Pairing; Generalized Proxy Signcryption; Proxy Signature; Proxy Signcryption

1 Introduction

In the traditional public key cryptosystem [23], a user's public key is an arbitrary string. Therefore, it needs a trusted third party - certificate authority (CA) to issue a certificate to bind the public key with the user's identity. However, the cost of certificate management is considered to be very high.

The identity-based public key cryptosystem [24, 9] uses an e-mail address or a telephone number *etc.* to represent a user's public key, so there is no need for a public key certificate to bind the public key with the user's identity. In this way, the cost of public key management is greatly reduced.

Signcryption [17] can realize encryption and authentication in a single logic step in an efficient way, so it is very suitable for resource-constrained systems.

Proxy signature [4, 14, 10] allows a designated proxy signer to sign documents on behalf of the original signer when the latter was absent. When the documents must be kept secret, proxy signcryption [18, 16] can be used instead.

Proxy signature and proxy signcryption are two separate cryptographic primitives. If a person is designated by an original person to be both a proxy signer and a proxy signcrypter, he/she must use two algorithms and two key pairs to realize the two functions. If we can use only one algorithm and one key pair, that will save the storage space, simplify the key management and reduce the cost of changing system functions.

In 2016, by reference to the concept of generalized signcription [32], Zhou [31] introduced a new concept of generalized proxy signcryption, which can realize both proxy signature and proxy signcryption with only one key pair and one algorithm. The algorithm can work in two modes - proxy signature mode and proxy signcryption mode. If the receiver's identity is set to null, which is used as the input of the algorithm, the algorithm will run in proxy signature mode; else it will run in proxy signcryption mode. In the same paper, a concrete identity-based GPSC scheme in the standard model was also presented.

In this paper, we propose an identity-based GPSC scheme in the random oracle model by using bilinear pairings. Then, we prove the confidentiality of our scheme in proxy signcryption mode under the GBDH hard assumption and the unforgeability in proxy signature and proxy signcryption modes under the GDH' hard assumption. At last, we compare our scheme in proxy signcryption mode with other identity-based proxy signcryption schemes that use bilinear pairings, and the results show that our scheme is practical.

Our scheme has the following merits. First, it can be verified publicly in proxy signcryption mode. Public ver-

ification is very useful in the scenario where the firewall first verifies the validity of the ciphertexts and only allows valid ciphertexts to pass through to the receiver. It prevents the receiver from unnecessarily using their resources to decrypt the invalid ciphertexts. Second, our scheme can resist proxy key exposure attacks [20]. Proxy key is often used in a potentially hostile environment, where it can be easily exposed, but such exposure must not leak any information about the long term private key. Third, our scheme supports self-delegation. Through self-delegation, the user can avoid using the long term private key in some situations, reducing the exposure risk of long term private key. Fourth, there is no need for a secure channel between the original person and the proxy person, which reduces the cost of system implementation. Fifth, our scheme can resist insider attacks. An inside attacker refers to the original person, the proxy person or the receiver. Even with their own private keys, the inside attackers still cannot breach the security of the scheme. Sixth, our scheme is very suitable for a system whose functions may be changed. Consider the following scenario: Previously a system only had the proxy signature function. Due to some reasons, it needs to add the proxy signcryption function. If we use the traditional method, the system must be re-programmed and re-deployed, and everyone in the system will be given a new key pair for the added proxy signcryption function, which will increase the cost of key management and the storage space of the system. However, for our scheme, we only need to let it run in proxy signcrytion mode and the added function will be realized. In this case, the system does not need to be re-programmed and re-deployed, and the total number of keys remains the same. Thus, the cost of key management and the storage space are saved. Reducing the cost of key management is of great practical significance. It is just due to the costly key management that the traditional public key cryptosystem has not been widely applied.

Generalized proxy signcryption can have many practical applications. For example, a person delegates a mobile agent to buy some goods or services on the Internet for himself/herself. For some sensitive messages, the mobile agent can use proxy signcryption, while for others it can use proxy signature. As another example, a general manager of a company delegates his/her signing/signcryption rights to his/her secretary for a period of time when he/she is on vacation. For sensitive messages, the secretary can use proxy signcryption, and for others, she can use proxy signature. Both the mobile agent and the secretary only need to keep one key pair and use one algorithm in the above two examples.

1.1 Related Works

Generalized signcryption was first introduced by Han *et al.* [8] in 2006, in which encryption, signature and signcryption share one key pair and one algorithm for the purpose of saving the storage space of keys and programs, simplifying key management and deployment of the system, and reducing the time spent in verifying the keys. Following Han *et al.*'s work, Wang *et al.* [26] pointed out some security flaws in scheme [8] and improved it, and gave a security model for generalized signcryption scheme for the first time in 2007. Lal and Kushwah [13] first gave the security model of identity-based generalized signcryption and a concrete scheme in 2008. Yu *et al.* [29] pointed out that the security model introduced in scheme [13] is not complete, and gave a new security model and a concrete provably secure scheme in 2010. In the same year, Kushwah and Lal [12] simplified the security model introduced in scheme [29], and proposed a more efficient identity-based generalized signcryption scheme. Han and Gui [7] proposed a multi-receiver generalized signcryption scheme in 2009. Ji *et al.* [11] gave for the first time a certificateless generalized signcryption scheme and security model in 2010. In the same year, Kushwah and Lal [12] pointed out that scheme [11] is insecure and proposed a new scheme. Zhou *et al.* [32] proposed a new certificateless generalized signcryption scheme which is secure against the malicious-but-passive key generation center attacks [1] in 2014. Wei *et al.* [27] proposed an identity-based generalized signcryption scheme in the standard model and applied it in big data security in 2015. In the same year, Zhou [30] pointed out that the multi-receiver generalized signcryption scheme [7] is insecure and improved it and Han *et al.* [6] proposed a generalized signcryption scheme in the attribute-based setting. Shen *et al.* [21] proposed an identity-based generalized signcryption scheme in the standard model in 2017.

The rest of the paper is organized as follows. In Section 2, we introduce the concept of bilinear pairing and some complexity assumptions. In Section 3, we describe the formal definition and security model of GPSC. In Section 4, we propose an efficient identity-based GPSC scheme in the random oracle model. In Section 5, we discuss the security and efficiency of the proposed scheme. We conclude the paper in Section 6.

2 Preliminaries

2.1 Bilinear Pairing

Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of prime order q, and g be a generator of G_1. The map $e : G_1 \times G_1 \to G_2$ is said to be an admissible bilinear pairing if the following three conditions hold.

1) Bilinearity: for all $a, b \in Z_q$, $P, Q \in G_1$, we have $e(aP, bQ) = e(P, Q)^{ab}$.

2) Non-degeneracy: $e(g, g) \neq 1_{G_2}$.

3) Computability: for all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

2.2 Complexity Assumptions

1) Bilinear Diffie-Hellman (BDH) Problem: Given $(P, aP, bP, cP) \in G_1^4$ for unknown $a, b, c \in Z_q$, one must compute $e(P,P)^{abc}$. The advantage of any probabilistic polynomial time (PPT) algorithm A in solving the BDH problem in (G_1, G_2, e) is defined to be: $ADV_A^{BDH} = Pr[A(P, aP, bP, cP) = e(P,P)^{abc}, a, b, c \in Z_q]$. BDH assumption: For every PPT algorithm A, ADV_A^{BDH} is negligible.

2) Decisional Bilinear Diffie-Hellman (DBDH) Problem: Given $(P, aP, bP, cP, T) \in G_1^4 \times G_2$ for unknown $a, b, c \in Z_q$, one must decide whether $T = e(P,P)^{abc}$. The advantage of any PPT algorithm A in solving the DBDH problem in (G_1, G_2, e) is defined to be: $ADV_A^{DBDH} = Pr[A(P, aP, bP, cP, T) = 1, a, b, c \in Z_q] - Pr[A(P, aP, bP, cP, e(P,P)^{abc}) = 1, a, b, c \in Z_q]$. DBDH assumption: For every PPT algorithm A, ADV_A^{DBDH} is negligible.

3) Gap Bilinear Diffie-Hellman (GBDH) Problem [2]: Given $(P, aP, bP, cP) \in G_1^4$ for unknown $a, b, c \in Z_q$, one must compute $e(P,P)^{abc}$ with the help of a DBDH oracle. The advantage of any PPT algorithm A in solving the GBDH problem in (G_1, G_2, e) is defined to be: $ADV_A^{GBDH} = Pr[A^o(P, aP, bP, cP) = e(P,P)^{abc}, a, b, c \in Z_q]$, where o denotes a DBDH oracle. GBDH assumption: For every PPT algorithm A, ADV_A^{GBDH} is negligible.

4) Computational Diffie-Hellman (CDH) Problem: Given $(P, aP, bP) \in G_1^3$ for unknown $a, b \in Z_q$, one must compute abP. The advantage of any PPT algorithm A in solving the CDH problem in G_1 is defined to be: $ADV_A^{CDH} = Pr[A(P, aP, bP) = abP, a, b \in Z_q]$. CDH assumption: For every PPT algorithm A, ADV_A^{CDH} is negligible.

5) Gap Diffie-Hellman (GDH') Problem [2]: Given $(P, aP, bP) \in G_1^3$ for unknown $a, b \in Z_q$, one must compute abP with the help of a DBDH oracle. The advantage of any PPT algorithm A in solving the GDH' problem in (G_1, G_2, e) is defined to be: $ADV_A^{GDH'} = Pr[A^o(P, aP, bP) = abP, a, b \in Z_q]$, where o denotes a DBDH oracle. GDH' assumption: For every PPT algorithm A, $ADV_A^{GDH'}$ is negligible.

3 Formal Definition and Security Model of Identity-based Generalized Proxy Signcryption

3.1 Formal Definition

An identity-based GPSC scheme consists of the following six algorithms, involving the original person ID_A, the proxy person ID_P and the receiver ID_R (ID_R may be null):

1) $Setup(1^k)$: Given a security parameter 1^k, the private key generator (PKG) generates a master private key s and a common parameter $params$. $params$ are public to all. PKG keeps the private key s secret.

2) $Extraction(params, s, ID_i)$: On input $params$, the PKG uses s to generate a private key D_i for user ID_i, and then he/she sends it to the user securely.

3) $Delegation(params, D_A, m_w)$: On input $params$, an original person's private key D_A and a warrant m_w (which includes the delegation period, the identities of original person and proxy person and the types of delegated messages, *etc.*), the original person outputs a delegation σ and sends $\{\sigma, m_w\}$ to the proxy person ID_P.

4) $ProxyKey-generation(params, m_w, \sigma, D_P)$: On input $params$, a warrant m_w, a delegation σ and a proxy person's private key D_P, the proxy person produces a proxy key SK_P.

5) $GPSC(params, m, m_w, SK_P, ID_R)$: This algorithm has two modes: proxy signature mode and proxy signcryption mode.

   Proxy-signature mode: If the input to the receiver's identity ID_R is null, it will run in this mode. Other inputs are the message m, the $params$, the warrant m_w and the proxy key SK_P. The proxy signer produces a signature σ_P.

   Proxy-signcryption mode: If the input to the receiver's identity ID_R is not null, it will run in this mode. Other inputs are the message m, the $params$, the warrant m_w and the proxy key SK_P. The proxy signcrypter produces a ciphertext σ_P.

6) UN-GPSC: This algorithm also has two modes: proxy signature verification mode and proxy unsigncryption mode.

   Proxy-signature verification mode ($params$, m_w, σ_P, ID_R): If the input to the receiver's identity ID_R is null, it will run in this mode. Any person can verify the validity of the proxy signature σ_P. If it is correct, the proxy signature will be accepted.

   Proxy-unsigncrytion mode ($params$, m_w, σ_P, ID_R, D_R): If the input to the receiver's identity ID_R is not null, it will run in this mode. The receiver ID_R uses his/her private key D_R to recover the message m or an invalid symbol $\perp$.

For consistency, we require if $\sigma_P = GPSC(params, m, m_w, SK_P, ID_R)$, then $UN-GPSC(params, m_w, \sigma_P)$ = true when ID_R is null or $UN-GPSC(params, m_w, \sigma_P, ID_R, D_R) = m$ when ID_R is not null.

3.2 Security Model of Identity-based Generalized Proxy Signcryption

When the scheme run in proxy signcryption mode, it has confidentiality security. The following security model [31]

considers proxy key exposure attacks, insider attacks and self-delegation.

Definition 1. *(confidentiality, proxy signcryption mode) An identity-based GPSC scheme is semantically secure against the adaptive chosen ciphertext, chosen identity and chosen warrant attacks (IND-IB-GPSC-CCA for short) in proxy signcryption mode if no PPT adversary A has a non-negligible advantage in the following game:*

Setup: *The challenger C runs the setup algorithm to generate a master private key s and a common parameter params. C gives params to A and keeps s secret.*

Phase 1: *A can make the following polynomially bounded number of queries.*

1) *Extraction queries: A produces an identity ID_i. C runs the extraction algorithm to produce a D_i and returns it to A.*
2) *Delegation queries: A produces a warrant m_w, a proxy identity ID_P and an original identity ID_A. C runs the delegation algorithm to produce a σ and returns (σ, m_w) to A. Here the delegation may be a self-delegation, i.e., the identity ID_P may be equal to the identity ID_A.*
3) *ProxyKey queries: A produces a proxy identity ID_P. C runs the proxy key generation algorithm to produce a SK_P and returns it to A.*
4) *GPSC queries: A produces a message m, a warrant m_w, an original identity ID_A, a proxy identity ID_P and a receiver's identity ID_R. Here if ID_R is null, it is equal to a proxy signature query or else it is equal to a proxy signcryption query. C runs the GPSC algorithm to produce a signature or a ciphertext σ_P to A.*
5) *UN-GPSC queries: A produces a σ_P, a warrant m_w, an original identity ID_A, a proxy identity ID_P and a receiver's identity ID_R. Here if ID_R is null, it is equal to a proxy signature verification query or else it is equal to a proxy un-signcryption query. If it is a proxy signature verification query, C runs the UN-GPSC algorithm to return true or false to A. If it is a proxy un-signcryption query, C runs the UN-GPSC algorithm to return the plaintext m or an invalid symbol $\perp$ to A.*

Challenge: *The attacker A selects two different messages m_0, m_1 with equal length, a warrant m_w^*, and three challenge identities ID_A^*, ID_P^* and ID_R^* (ID_R^* must not be null). Here A has not made the extraction query to identity ID_R^*. C randomly selects a bit $b \in \{0,1\}$, computes the m_b's proxy signcryption ciphertext σ_P^* on $(m_w^*, ID_A^*, ID_P^*, ID_R^*)$, and gives it to A.*

Phase 2: *The attacker A can adaptively make a series of queries as in the Phase 1, but he/she cannot make extraction query of identity ID_R^* nor can he/she make proxy un-signcryption query to σ_P^* under $(m_w^*, ID_A^*, ID_P^*, ID_R^*)$.*

Guess: *When the attacker A wants to end the game, he/she must give his/her guess $b' \in \{0,1\}$. If $b' = b$, he/she wins the game.*

The advantage of the adversary A is defined as: $Adv^{IND-IB-GPSC-CCA}(A) := 2Pr[b' = b] - 1$.

Note 1. *The attacker A is allowed to make a query about the private key of the original person or the proxy person in the Challenge stage, but these inside attackers cannot breach the security of the scheme.*

When the scheme run in proxy signature mode or proxy signcryption mode, it has unforgeability security. In the following security model [31], it considers proxy key exposure attacks, insider attacks and self-delegation.

Definition 2. *(unforgeability, both modes) An identity-based GPSC scheme is existentially unforgeable against the adaptive chosen message, chosen identity and chosen warrant attacks (EUF-IB-GPSC-CMA for short) in proxy signature mode or proxy signcryption mode if no PPT adversary A has a non-negligible advantage in the following game:*

Setup: *Same as in the confidentiality game.*

Attack: *Same as in the confidentiality game.*

Forgery: *If any one of the following events occurs, A wins the game.*

1) *The attacker A outputs a forged delegation σ^* on (ID_A^*, ID_P^*, m_w^*). He/she has not made the delegation query of (ID_A^*, ID_P^*, m_w^*) or extraction query of ID_A^*, and σ^* can pass the delegation verification. Here the identity ID_P^* may be equal to the identity ID_A^* (it means self-delegation).*
2) *The attacker A pretends to be a proxy person ID_P^* to output a forged ciphertext σ_P^* (which may be a proxy signature or proxy signcryption) on (ID_A^*, ID_R^*, m_w^*). The ciphertext σ_P^* is not the output of GPSC query, A has not made extraction query or proxy key query of ID_P^*, and σ_P^* can pass the validation of UN-GPSC.*

   Note 2. *The attacker A is allowed to make a query about the private key of the original person or the receiver (if ID_R^* is not null) in the Forgery stage, but these inside attackers cannot breach the security of the scheme.*

3) *The attacker A pretends to be an original person ID_A^* to output a forged ciphertext σ_P^* (which may be a proxy signature or proxy signcryption)*

on (ID_P^*, ID_R^*, m_w^*). The ciphertext σ_P^* is not the output of GPSC query. A does not make the delegation query with (ID_A^*, ID_P^*, m_w^*), the extraction query with ID_A^* or the proxy key query with ID_P^*, and σ_P^* can pass the validation of UN-GPSC.

Note 3. *The attacker A is allowed to make a query about the private key of the proxy person or the receiver (if ID_R^* is not null) in the Forgery stage, but these inside attackers cannot breach the security of the scheme.*

A's advantage is its probability of victory.

Note 4. *In the above Forgery stage, ID_R^* may be null. If ID_R^* is null, it runs in proxy-signature mode or else it runs in proxy-signcryption mode. So the two modes share the same game.*

4 An Identity-based Generalized Proxy Signcryption Scheme

Based on Yoon *et al.*'s [28] identity-based signature scheme, we give out our identity-based GPSC scheme.

4.1 The Concrete Scheme

Setup: Given a security parameter k, the PKG chooses an additive cyclic group G_1, a multiplicative cyclic group G_2, a generator P of G_1, a bilinear pairing $e : G_1 \times G_1 \to G_2$ and four secure hash functions $H_1 : \{0,1\}^* \to G_1^*$, $H_2, H_4 : \{0,1\}^* \to Z_q^*$, $H_3 : \{0,1\}^* \to \{0,1\}^m$. m represents the bit length of a message. G_1 and G_2 have the same prime order q. The PKG randomly chooses $s \in Z_q^*$ as the master private key, and computes $P_{pub} = sP$ as the master public key. Let $ID \in \{0,1\}^*$ be an identity of a user. The PKG defines a function $f(ID)$: If $ID \in null$ then $f(ID) = 0$; else $f(ID) = 1$. The PKG publishes the system public parameters as $\{e, G_1, G_2, P, P_{pub}, m, H_1, H_2, H_3, H_4, f\}$, and keeps the master private key s secret.

Extraction: Given an identity ID_i of a user i, the PKG computes the user's private key as $D_i = sH_1(ID_i) = sQ_i$.

Delegation: The original person ID_A first generates a warrant m_w, which records the identities and public keys of original person and proxy person, the type and scope of messages, the time period and so on. ID_A randomly selects $k_A \in Z_q^*$, and computes $R_A = k_A \cdot P$, $h_A = H_2(m_w, R_A)$ and $V_A = h_A D_A + k_A Q_A$. The delegation is $\sigma = (m_w, R_A, V_A)$. ID_A transmits $\sigma = (m_w, R_A, V_A)$ to ID_P publicly. ID_P can verify it through the equation $e(V_A, P) = e(Q_A, h_A P_{pub} + R_A)$. If σ is valid, ID_P accepts it; else σ is re-produced.

Proxy-Key Generation: ID_P randomly selects $k_P \in Z_q^*$, and computes $R_P = k_P \cdot P$, $h_P = H_2(m_w, R_P)$ and $V_P = h_P D_P + k_P Q_P$. At last, the proxy key is $SK_P = V_P + V_A$.

GPSC: Let $M \in \{0,1\}^m$ and $tag \in \{0,1\}$. The proxy person ID_P first computes $f(ID_R)$. If $f(ID_R) = 0$ then $tag = 0$; else $tag = 1$. ID_P randomly selects $t \in Z_q^*$, and computes $R = tP$, $T = e(P_{pub}, Q_R)^{t \cdot tag}$, $h_3 = tag \cdot H_3(R, T, ID_P, Q_P, ID_A, Q_A)$, $C = M \oplus h_3$, $h_4 = H_4(m_w, C, R, ID_R, Q_R)$ and $X = h_4 \cdot SK_P + t(Q_A + Q_P)$. At last, the ciphertext is $\sigma_P = (m_w, R, C, X, R_A, R_P, tag)$.

UN-GPSC:

1) $tag = 0$. $\sigma_P = (m_w, R, C = M, X, R_A, R_P, tag)$ is a proxy signature. Anyone can compute $h_A = H_2(m_w, R_A)$, $h_P = H_2(m_w, R_P)$ and $h_4 = H_4(m_w, C, R, null, null)$, and then verifies the equation $e(X, P) = e(Q_P, h_4 h_P P_{pub} + h_4 R_P + R) e(Q_A, h_4 h_A P_{pub} + h_4 R_A + R)$. If it holds true, ID_P accepts it; else he/she rejects it.

2) $tag = 1$. $\sigma_P = (m_w, R, C, X, R_A, R_P, tag)$ is a proxy signcryption. ID_R can compute $h_A = H_2(m_w, R_A)$, $h_P = H_2(m_w, R_P)$ and $h_4 = H_4(m_w, C, R, ID_R, Q_R)$, and then verifies the equation $e(X, P) = e(Q_P, h_4 h_P P_{pub} + h_4 R_P + R) e(Q_A, h_4 h_A P_{pub} + h_4 R_A + R)$. If it does not hold true, ID_P rejects it; else he/she accepts it and recovers the message $M = C \oplus H_3(R, e(R, D_R), ID_P, Q_P, ID_A, Q_A)$.

4.2 Adaptation

The scheme is an adaptive one and able to switch to two different modes according to the receivers identity ID_R. If the input to the receiver's identity ID_R is null, it will work in proxy signature mode or else it will work in proxy signcryption mode. So the two modes share the same algorithm, so we can use the same key pair to proxy-sign or proxy-signcrypt documents.

5 Analysis of the Proposed Scheme

5.1 Correctness

$$\begin{aligned} e(X,P) &= e(h_4 \cdot SK_P + t(Q_A+Q_P), P) \\ &= e(h_4 \cdot (h_P D_P + k_P Q_P + h_A D_A + k_A Q_A) \\ &\quad + t(Q_A+Q_P), P) \\ &= e(Q_P, h_4 h_P P_{pub} + h_4 R_P + R) e(Q_A, h_4 h_A P_{pub} \\ &\quad + h_4 R_A + R) \\ T &= e(P_{pub}, Q_R)^t \\ &= e(tP, sQ_R) \\ &= e(R, D_R). \end{aligned}$$

5.2 Semantic Security

Theorem 1. *In the random oracle model, if there is a PPT attacker A with a non-negligible advantage ε against the IND-IB-GPSC-CCA security of our scheme running in proxy signcryption mode in time T and performing at most q_E extraction queries, q_{SK_P} proxy key queries, q_{DE} delegation queries, q_{GPSC} GPSC queries, $q_{UN-GPSC}$ UN-GPSC queries, q_{H_1} H_1 queries, q_{H_2} H_2 queries, q_{H_3} H_3 queries and q_{H_4} H_4 queries, then the GBDH problem can be solved with probability $\varepsilon' \geq \varepsilon \cdot 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k)$ in time $T' \leq T + O((q_{GPSC} + q_{UN-GPSC} + q_E + q_{SK_P} + q_{DE}) \cdot t_m + q_{GPSC} \cdot t_e + (q_{GPSC} + q_{UN-GPSC}) \cdot t_p)$, where t_m, t_e and t_p represent the time for a scalar multiplication on G_1, an exponentiation on G_2 and a pairing operation, respectively.*

Proof. Our proof is partially similar to scheme [2]. Challenger C is given $(P, aP, bP, cP) \in G_1^4$ for random $a, b, c \in Z_q^*$. C does not know the values of a, b and c, and is asked to compute $e(P,P)^{abc}$ with the help of a DBDH oracle. To utilize adversary A, challenger C will simulate all the oracles defined in Definition 1. C maintains four lists L_1, L_2, L_3 and L_4, which are initially empty. We assume all queries in the following are distinct and A will ask for $H_1(ID)$ before ID is used in any other queries. In the beginning, C gives the system parameters *params* to A with $P_{pub} = aP$ and he/she randomly selects a number $\theta \in \{1, 2, ..., q_{H_1}\}$.

H_1 queries: On the i-th query ID, if $i \neq \theta$, C randomly selects $x \in Z_q^*$ and repeats the process until x is not in list L_1 and sets $Q_{ID} = xP$. Then C stores (i, ID, x) in list L_1 and returns Q_{ID} to A. Otherwise, C stores $(\theta, ID, -)$ in list L_1 and returns $Q_\theta = bP$ to A.

H_2 queries: A supplies an item (m_w, R_{ID}). C randomly selects $h_2 \in Z_q^*$ and repeats the process until h_2 is not in list L_2. C stores the item (m_w, R_{ID}, h_2) in list L_2, and returns h_2 to A.

H_4 queries: A supplies an item (m_w, C, R, ID_R, Q_R). C randomly selects h_4 and repeats the process until h_4 is not in list L_4. C stores the item $(m_w, C, R, ID_R, Q_R, h_4)$ in list L_4, and returns h_4 to A.

H_3 queries: A supplies an item (R, T, ID_P, Q_P, ID_A, Q_A). C does the following.

1) C checks if the DBDH oracle returns 1 when queried with the tuple (aP, bP, cP, T). If it does, C returns T and stops.
2) Otherwise, C goes through list L_3 with entries $(R, *, ID_P, Q_P, ID_A, Q_A, h_3)$, so that for different values of h_3, the DBDH oracle returns 1 when queried on the tuple (aP, bP, cP, T). If such a tuple exists, C returns h_3 and replaces the symbol * with T.
3) Otherwise, C randomly selects $h_3 \in \{0,1\}^m$ and repeats the process until h_3 is not in list L_3. C stores the item $(R, T, ID_P, Q_P, ID_A, Q_A, h_3)$ in list L_3, and returns h_3 to A.

Extraction queries: A supplies an identity ID. C searches in list L_1 on ID and obtains (i, ID, x). If $i = \theta$, then C outputs failure and aborts. Otherwise, C returns $x(aP)$.

Delegation queries: A produces a warrant m_w, a proxy identity ID_P and an original identity ID_A.

1) $ID_A \neq ID_\theta$. C runs the delegation algorithm as normal because C can get the private key of ID_A.
2) $ID_A = ID_\theta$. C produces the delegation as follows.
   a. Randomly selects $k, h_A \in Z_q^*$ and computes $V_A = kQ_A$ and $R_A = kP - h_A P_{pub}$.
   b. Saves the item (m_w, R_A, h_A) to list L_2. If a collision occurs in list L_2, C repeats the Step (a).
   c. Outputs the delegation $\sigma = (m_w, R_A, V_A)$ to ID_P.

Here the delegation may be a self-delegation, *i.e.*, the identity ID_P may be equal to the identity ID_A.

Proxy-Key queries: A produces a warrant m_w, a proxy identity ID_P and an original identity ID_A. C first runs delegation query to get V_A.

1) $ID_P \neq ID_\theta$. C runs the proxy-key algorithm as normal because C can get the private key of ID_P.
2) $ID_P = ID_\theta$. C produces the proxy-key as follows.
   a. Randomly selects $k, h_P \in Z_q^*$ and computes $V_P = kQ_P$ and $R_P = kP - h_P P_{pub}$.
   b. Saves the item (m_w, R_P, h_P) to list L_2. If a collision occurs in list L_2, C repeats the Step (a).

c. Outputs the proxy-key $SK_P = V_P + V_A$.

GPSC queries: A produces a message m, a warrant m_w, an original identity ID_A, a proxy identity ID_P and a receiver's identity ID_R. Here if ID_R is null, it is equal to a proxy signature query or else it is equal to a proxy signcryption query. C first makes a proxy-key query to get ID_P's proxy key, then runs the GPSC algorithm as normal to produce a signature or a ciphertext σ_P to A.

UN-GPSC queries: A produces a σ_P, a warrant m_w, an original identity ID_A, a proxy identity ID_P and a receiver's identity ID_R. If ID_R is null, it is equal to a proxy signature verification query or else it is equal to a proxy un-signcryption query. If it is a proxy signature verification query, it just needs public parameters. If it is a proxy un-signcryption query, we consider two cases:

1) $ID_R \neq ID_\theta$. C runs the UN-GPSC algorithm as normal because C can get the private key of ID_R.
2) $ID_R = ID_\theta$. C first runs the verification part of the UN-GPSC algorithm, which just needs public parameters. If the verification does not succeed, C returns $\perp$. Otherwise, it means the verification of the UN-GPSC algorithm holds true. In this situation, C checks if a tuple $(R, T, ID_P, Q_P, ID_A, Q_A, h_3)$ exists in list L_3, so that for some T, the DBDH oracle returns 1 when queried on (aP, bP, R, T). If such a tuple exists, C recovers the message m using the hash value h_3. Otherwise, C randomly selects $h_3 \in \{0,1\}^m$ and repeats the process until h_3 is not in list L_3. C stores the item $(R, *, ID_P, Q_P, ID_A, Q_A)$ in list L_3 and recovers the message m using the hash value h_3. The symbol * denotes an unknown value of pairing.

At last, attacker A selects two different messages M_0, M_1 with equal length, a warrant m_w^*, and three challenge identities ID_A^*, ID_P^* and ID_R^* (ID_R^* must not be null). If $ID_R^* \neq ID_\theta$, C outputs failure and aborts; otherwise C proceeds to construct a challenge as follows. C selects a random $b \in \{0,1\}$ and a random hash $h_3^* \in \{0,1\}^m$, and sets $R^* = cP$ and $C^* = h_3^* \oplus M_b$. Then C makes a delegation query to get (R_A^*, V_A^*), makes a proxy-key query to get (R_P^*, SK_P^*), makes H_4 query on the tuple $(m_w^*, C^*, R^*, ID_R^*, Q_R^* = bP)$ to get h_4^* and computes $X^* = h_4^* \cdot SK_P^* + (x_A^* + x_P^*)(cP)$ $(Q_A^* = x_A^* P, Q_P^* = x_P^* P, x_A^*, x_P^*$ can be obtained from list $L_1)$. At last, the challenge ciphertext is $\sigma_P^* = (m_w^*, R^*, C^*, X^*, R_A^*, R_P^*, tag = 1)$.

In the second stage of the confidentiality game, A can adaptively make a series of queries like before with the restrictions as in Definition 1. At last, A must give his/her guess. A cannot find out that σ_P^* is not a valid ciphertext unless he/she asks for the hash value of $H_3(R^* = cP, T = e(P,P)^{abc}, ID_P^*, Q_P^*, ID_A^*, Q_A^*)$. If this happens, C will solve the GDBH problem due to the first step of H_3 oracle.

Now, we assess the probability of success. In the Challenge stage, the probability that $ID_R^* = ID_\theta$ is $1/q_{H_1}$. The probability of A querying the private key of ID_θ is $1/q_{H_1}$. In the UN-GPSC queries, the probability of C rejecting a valid ciphertext does not exceed $q_{UN-GPSC}/2^k$.

The time complexity of C depends on the scalar multiplication on G_1, the exponentiation on G_2 and pairing operations needed in all the above queries. The extraction queries, delegation queries and proxy-key queries need $O(1)$ scalar multiplications on G_1. The GPSC queries need $O(1)$ scalar multiplications on G_1, $O(1)$ exponentiation on G_2 and $O(1)$ pairings. The UN-GRSC queries need $O(1)$ scalar multiplications on G_1 and $O(1)$ pairings. □

5.3 Unforgeability

Theorem 2. *In the random oracle model, if there is a PPT attacker A with a non-negligible advantage against the EUF-IB-GPSC-CMA security of our scheme running in proxy signature mode or proxy signcryption mode in polynomial time and performing at most q_E extraction queries, q_{SK_P} proxy key queries, q_{DE} delegation queries, q_{GPSC} GPSC queries, $q_{UN-GPSC}$ UN-GPSC queries, q_{H_1} H_1 queries, q_{H_2} H_2 queries, q_{H_3} H_3 queries and q_{H_4} H_4 queries, then the GDH′ problem can be solved with a non-negligible advantage in a polynomial time.*

This theorem follows from Lemmas 1, 2 and 3.

Lemma 1. *If A can forge a delegation of our scheme with a non-negligible advantage $\varepsilon \geq 10(q_{H_1}+q_{DE})(q_{DE}+1)/2^k$ in polynomial time t, then the GDH′ problem can be solved with probability $\varepsilon' \geq 1/9 \cdot 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k)$ in time $t' \leq 23q_{H_2}(t + (q_{GPSC} + 4q_{UN-GPSC})t_e)/\varepsilon$, where t_e represents the time for a pairing operation.*

Lemma 2. *If A can pretend to be a proxy person to forge our scheme (which may be a proxy signature or proxy signcryption) with a non-negligible advantage ε in polynomial time t, then the GDH′ problem can be solved with probability $\varepsilon' \geq 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k) \cdot (\varepsilon^3/(q_{H_2} + q_{H_4})^6 - 3/2^k)\varepsilon$ in time $t' \leq 2t + (q_{GPSC} + 4q_{UN-GPSC})t_e$, where t_e represents the time for a pairing operation.*

Lemma 3. *If A can pretend to be an original person to forge our scheme (which may be a proxy signature or proxy signcryption) with a non-negligible advantage ε in polynomial time t, then the GDH′ problem can be solved with probability $\varepsilon' \geq 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k) \cdot (\varepsilon^3/(q_{H_2} + q_{H_4})^6 - 3/2^k)\varepsilon$ in time $t' \leq 2t + (q_{GPSC} + 4q_{UN-GPSC})t_e$, where t_e represents the time for a pairing operation.*

Proof. (Lemma 1) Suppose challenger C is given $(P, aP, bP) \in G_1^3$ for random $a, b \in Z_q^*$. C does not know

the values of a and b, and is asked to compute abP with the help of a DBDH oracle. To utilize adversary A, challenger C will simulate all the oracles defined in Definition 2. C maintains four lists L_1, L_2, L_3 and L_4, which are initially empty. We assume all queries in the following are distinct and A will ask for $H_1(ID)$ before ID is used in any other queries. In the beginning, C gives the system parameters $params$ to A with $P_{pub} = aP$ and randomly selects a number $\theta \in \{1, 2, ..., q_{H_1}\}$.

The H_1, H_2, H_4, extraction, delegation, proxy-key, GPSC and UN-GPSC queries are the same as in Theorem 1.

H_3 **queries:** A supplies an item $(R, T, ID_P, Q_P, ID_A, Q_A)$. C does the following.

1) C goes through list L_3 with entries $(R, *, ID_P, Q_P, ID_A, Q_A, h_3)$, so that for different values of h_3, the DBDH oracle returns 1 when queried on the tuple (aP, bP, R, T). If such a tuple exists, C returns h_3 and replaces the symbol * with T.
2) Otherwise, C randomly selects $h_3 \in \{0,1\}^m$ and repeats the process until h_3 is not in list L_3. C stores the item $(R, T, ID_P, Q_P, ID_A, Q_A, h_3)$ in list L_3, and returns h_3 to A.

At last, attacker A outputs a forged delegation σ^* on (ID_A^*, ID_P^*, m_w^*). He/she does not make delegation query with $(ID_A^*, ID_P^*, m_w^*, \sigma^*)$ or extraction query with ID_A^*, and σ^* can pass the delegation verification. Here the identity ID_P^* may be equal to the identity ID_A^* (it means self-delegation). If $ID_A^* \neq ID_\theta$, C outputs failure and stops. Otherwise, we suppose the forged delegation is $\sigma^* = (m_w^*, R_A^*, V_A^*)$. According to the forking lemma [19], we can get two valid delegations $\sigma^* = (m_w^*, R_A^*, V_A^*)$ and $\sigma' = (m_w^*, R_A', V_A')$, so that $V_A^* = h_A^* D_A^* + k_A^* Q_A^*$, $V_A' = h_A' D_A^* + k_A^* Q_A^*$ and $h_A^* = H_2^*(m_w^*, R_A^*) \neq h_A' = H_2'(m_w^*, R_A^*)$. Therefore we can get $V_A^* - V_A' = (h_A^* - h_A')D_A^* = (h_A^* - h_A') \cdot abP$ and $abP = (V_A^* - V_A')(h_A^* - h_A')^{-1}$.

Now, we assess the probability of success. In the forgery stage, the probability that $ID_A^* = ID_\theta$ is $1/q_{H_1}$. The probability of A querying the private key of ID_θ is $1/q_{H_1}$. In the UN-GPSC queries, the probability of C rejecting a valid ciphertext does not exceed $q_{UN-GPSC}/2^k$. Combined with the forking lemma, the probability of C success is $\varepsilon' \geq 1/9 \cdot 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k)$.

In terms of the time complexity, GPSC needs one pairing operation and UN-GPSC needs four pairing operations. Combined with the forking lemma, the running time of C is $t' \leq 23 q_{H_2}(t + (q_{GPSC} + 4q_{UN-GPSC})t_e)/\varepsilon$. □

Proof. (Lemma 2) Suppose challenger C is given $(P, aP, bP) \in G_1^3$ for random $a, b \in Z_q^*$. C does not know the values of a and b, and is asked to compute abP with the help of a DBDH oracle. To utilize adversary A, challenger C will simulate all the oracles defined in Definition 2. C maintains four lists L_1, L_2, L_3 and L_4, which are initially empty. We assume all queries in the following are distinct and A will ask for $H_1(ID)$ before ID is used in any other queries. In the beginning, C gives the system parameters $params$ to A with $P_{pub} = aP$ and randomly selects a number $\theta \in \{1, 2, ..., q_{H_1}\}$.

The H_1, H_2, H_3, H_4, extraction, delegation, proxy-key, GPSC and UN-GPSC queries are the same as in Lemma 1.

At last, attacker A pretends to be a proxy person ID_P^* to output a forged ciphertext σ_P^* (which may be a proxy signature or proxy signcryption) on $(ID_A^*, ID_R^*, m^*, m_w^*)$. The ciphertext σ_P^* is not the output of a GPSC query. A does not make extraction query or proxy key query on ID_P^*, and σ_P^* can pass the validation of UN-GPSC. If $ID_P^* \neq ID_\theta$, C outputs failure and stops. Otherwise, we suppose the forged ciphertext is $\sigma_P^* = (m_w^*, R^*, C^*, X^*, R_A^*, R_P^*, tag)$. According to the multiple-forking lemma [3], with the same inputs and different oracle instance to H_2 and H_4, we can get 4 forged signatures

$$\begin{aligned}
\sigma_P^{(1)} &= (m^*, R^*, X^{(1)}, R_A^*, R_P^*),\\
\sigma_P^{(2)} &= (m^*, R^*, X^{(2)}, R_A^*, R_P^*),\\
\sigma_P^{(3)} &= (m^*, R^*, X^{(3)}, R_A^*, R_P^*),\\
\sigma_P^{(4)} &= (m^*, R^*, X^{(4)}, R_A^*, R_P^*).
\end{aligned}$$

Let $h_P^{(1)}$ and $h_P^{(2)}$ be two different hash values of H_2, and $h_4^{(1)}$, $h_4^{(2)}$, $h_4^{(3)}$ and $h_4^{(4)}$ be four different hash values of H_4. We have

$$\begin{aligned}
X^{(1)} &= h_4^{(1)} \cdot (h_P^{(1)} D_P + k_P Q_P + h_A D_A + k_A Q_A) + t(Q_A + Q_P),\\
X^{(2)} &= h_4^{(2)} \cdot (h_P^{(1)} D_P + k_P Q_P + h_A D_A + k_A Q_A) + t(Q_A + Q_P),\\
X^{(3)} &= h_4^{(3)} \cdot (h_P^{(2)} D_P + k_P Q_P + h_A D_A + k_A Q_A) + t(Q_A + Q_P),\\
X^{(4)} &= h_4^{(4)} \cdot (h_P^{(2)} D_P + k_P Q_P + h_A D_A + k_A Q_A) + t(Q_A + Q_P).
\end{aligned}$$

Thus, we have

$$\begin{aligned}
&((X^{(1)} - X^{(2)})(h_4^{(1)} - h_4^{(2)})^{-1} - (X^{(3)} - X^{(4)})(h_4^{(3)}\\
&-h_4^{(4)})^{-1})(h_P^{(1)} - h_P^{(2)})^{-1} = abP.
\end{aligned}$$

Now, we assess the probability of success. In the forgery stage, the probability that $ID_P^* = ID_\theta$ is $1/q_{H_1}$. The probability of A querying the private key of ID_θ is $1/q_{H_1}$. In the UN-GPSC queries, the probability of C rejecting a valid ciphertext does not exceed $q_{UN-GPSC}/2^k$. Combined with the multiple-forking lemma, the probability of C success is $\varepsilon' \geq 1/q_{H_1} \cdot (1 - 1/q_{H_1}) \cdot (1 - q_{UN-GPSC}/2^k) \cdot (\varepsilon^3/(q_{H_2} + q_{H_4})^6 - 3/2^k)\varepsilon$.

In terms of the time complexity, GPSC needs one pairing operation and UN-GPSC needs four pairing operations. Combined with the multiple-forking lemma, the running time of C is $t' \leq 2t + (q_{GPSC} + 4q_{UN-GPSC})t_e$. □

Proof. (Lemma 3) The proof is similar to that of Lemma 2. □

5.4 Comparison of Performance

We compare our scheme running in proxy signcryption mode with other identity-based proxy signcryption schemes that use bilinear pairings, which include Li *et al.*'s scheme [15], Duan *et al.*'s scheme [5], Wang *et al.*'s scheme [25] and Tian *et al.*'s scheme [22]. The comparison results are listed in Table 1 and Table 2. The pairing computations that can be pre-computed are not included in Table 1. P, M and E represent a pairing computation, a scalar multiplication on G_1 and an exponentiation on G_2, respectively. From Table 1, we can see that scheme [15] and [5] need 8 and 7 pairing computations in the proxy un-signcryption stage, respectively. Therefore, the computational costs of these two schemes are higher than those of the other schemes, indicating they are inefficient. Scheme [25] is the most efficient one in all stages, but it is vulnerable to the proxy key exposure attacks. Once the proxy key is exposed in scheme [25], the original person can compute the private key of the proxy person. Scheme [22] needs 4 pairing computations in the delegation stage, and thus the cost greatly exceeds those of the others, indicating it is inefficient. About the ciphertext size, our scheme is slightly longer. In general, our scheme is one of the efficient schemes.

6 Conclusions

Generalized proxy signcryption can realize both proxy signature and proxy signcryption with only one key pair and one algorithm, which significantly improves the efficiency of a system with a large number of users, or with limited storage space or whose functions may be changed. In this paper, we propose an identity-based GPSC scheme in the random oracle model by using bilinear pairings. Our scheme can perform public verification in proxy signcryption mode, resist proxy key exposure attacks, resist insider attacks and supports self-delegation. What is more, it needs no secure channel between the original person and the proxy person. Under the adaptive chosen ciphertext, chosen identity and chosen warrant attacks, the confidentiality of our scheme can be reduced to the GBDH hard problem. Under the adaptive chosen message, chosen identity and chosen warrant attacks, the unforgeability of our scheme can be reduced to the GDH' hard problem. Through performance evaluation, our scheme is found to be practical.

Acknowledgments

This work was supported by the National Natural Science Foundation of China [grant numbers 61462048, 61562047, 61662039]. We express our thanks to Ms. Yan Di, who checked our manuscript.

References

[1] M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wang, and G. M. Yang, "Malicious kgc attacks in certificateless cryptography," in *Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security (ASIACCS'07)*, pp. 302–311, Mar. 2007.

[2] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pp. 369–372, Mar. 2008.

[3] A. Boldyreva, A. Palacio, and B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," *Cryptology ePrint Archive*, vol. 25, no. 1, pp. 57V115, Jan. 2012.

[4] L. Z. Deng, H. W. Huang, and Y. Y. Qu, "Identity based proxy signature from rsa without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229–235, 2017.

[5] S. S. Duan, Z. F. Cao, and Y. Zhou, "Secure delegation-by-warrant id-based proxy signcryption scheme," in *Computational Intelligence and Security, International Conference (CIS'05)*, pp. 445–450, Dec. 2005.

[6] Y. L. Han, Y. C. Bai, D. Y. Fang, and X. Y. Yang, "The new attribute-based generalized signcryption scheme," in *Intelligent Computation in Big Data Era - International Conference of Young Computer Scientists, Engineers and Educators (ICYCSEE'15)*, pp. 353–360, Jan. 2015.

[7] Y. L. Han and X. L. Gui, "Adaptive secure multicast in wireless networks," *International Journal of Communication Systems*, vol. 22, no. 9, pp. 1213–1239, 2009.

[8] Y. L. Han, X. Y. Yang, P. Wei, Y. M. Wang, and Y. P. Hu, "Ecgsc: Elliptic curve based generalized signcryption," in *Ubiquitous Intelligence and Computing, Third International Conference (UIC'06)*, pp. 956–965, Sep. 2006.

[9] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[10] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of Proxy Signature Based on Elliptic Curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[11] H. F. Ji, W. B. Han, and L. Zhao, "Certificateless generalized signcryption," *Cryptology ePrint Archive*, no. 33, pp. 962-967, 2012.

[12] P. Kushwah and S. Lal, "Efficient generalized signcryption schemes," *Cryptology ePrint Archive*, 2010. (`http://eprint.iacr.org/2010/346`)

[13] S. Lal and P. Kushwah, "Id based generalized signcryption," *Cryptology ePrint Archive*, 2008. (`http://eprint.iacr.org/2008/084`)

Table 1: Comparison of computational costs

Schemes	Dele	Dele-Veri	P-Signcrypt	P-UnSigncrypt
[15]	3M	3P+E	P+2M+2E	8P+4E
[5]	2M	3P	P+2M+2E	7P+2E
[25]	2M	2P+M	P+2M+E	3P+M
[22]	4P+5M+2E	2P	P+2M+2E	4P+2E
Ours	3M	2P+M	P+3M+E	4P+4M

Table 2: Comparison of communication overhead

Schemes	CipherText-Size
[15]	$2\|G_1\| + \|q\| + \|m\| + \|m_w\|$
[5]	$3\|G_1\| + \|q\| + \|m_w\|$
[25]	$3\|G_1\| + 2\|ID\| + \|m\| + \|m_w\|$
[22]	$\|G_1\| + \|q\| + \|m\| + \|m_w\|$
Ours	$4\|G_1\| + \|m\| + \|m_w\|$

[14] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[15] X. X. Li and K. F. Chen, "Identity based proxy-signcryption scheme from pairings," in *2004 IEEE International Conference on Services Computing (SCC'04)*, pp. 494–497, Sep. 2004.

[16] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[17] Y. Ming and Y. M. Wang, "Cryptanalysis of an identity based signcryption scheme in the standard model," *International Journal of Network Security*, vol. 18, no. 1, pp. 165–171, 2016.

[18] C. H. Pan, S. P. Li, Q. H. Zhu, C. Z. Wang, and M. W. Zhang, "Notes on proxy signcryption and multi-proxy signature schemes," *International Journal of Network Security*, vol. 17, no. 1, pp. 29–33, 2015.

[19] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, p. 361-396, 2000.

[20] J. C. N. Schuldt, K. Matsuura, and K. G. Paterson, "Proxy signatures secure against proxy key exposure," in *11th International Workshop on Practice and Theory in Public-Key Cryptography (PKC'08)*, pp. 141–161, Mar. 2008.

[21] X. Q. Shen, M. Yang, and J. Feng, "Identity based generalized signcryption scheme in the standard model," *Entropy*, vol. 19, no. 3, Article Number 121, 2017.

[22] X. X. Tian, J. P. Xu, H. J. Li, Y. Peng, and A. Q. Zhang, "Secure id-based proxy signcryption scheme with designated proxy signcrypter," in *2009 International Conference on Multimedia Information Networking and Security (MINES'09)*, pp. 351–355, Nov. 2009.

[23] S. Vollala, B. S. Begum, A. D. Joshi, and N. Ramasubramanian, "High-radix modular exponentiation for hardware implementation of public-key cryptography," in *Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST'16)*, pp. 346–350, Dec. 2016.

[24] F. Wang, C. C. Chang, C. L. Lin, and S. C. Chang, "Secure and efficient identity-based proxy multi-signature using cubic residues," *International Journal of Network Security*, vol. 18, no. 1, pp. 90–98, 2016.

[25] Q. Wang and Z. F. Cao, "Efficient id-based proxy signature and proxy signcryption form bilinear pairings," in *Computational Intelligence and Security, International Conference, Part II (CIS'05)*, pp. 167–172, Dec. 2005.

[26] X. A. Wang, X. Y. Yang, and Y. L. Han, "Provable secure generalized signcryption," *Cryptology ePrint Archive*, 2007. (`http://eprint.iacr.org/2007/173`)

[27] G. Y. Wei, J. Shao, Y. Xiang, P. P. Zhu, and R. X. Lu, "Obtain confidentiality or/and authenticity in big data by id-based generalized signcryption," *Information Sciences*, vol. 318, pp. 111–122, 2015.

[28] H. J. Yoon, J. H. Cheon, and Y. D. Kim, "Batch verifications with id-based signatures," in *7th International Conference of Information Security and Cryptology (ICISC'04)*, pp. 233–248, Dec. 2004.

[29] G. Yu, X. X. Ma, Y. Shen, and W. B. Han, "Provable secure identity based generalized signcryption scheme," *Theoretical Compute Science*, vol. 411, no. 40-42, pp. 3614–3624, 2010.

[30] C. X. Zhou, "An improved multi-receiver generalized signcryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 340–350, 2015.

[31] C. X. Zhou, "Identity based generalized proxy signcryption scheme," *Information Technology and Control*, vol. 45, no. 1, pp. 13–26, 2016.

[32] C. X. Zhou, W. Zhou, and X. W. Dong, "Provable certificateless generalized signcryption scheme," *Designs, Codes and Cryptography*, vol. 71, no. 2, pp. 331–346, 2014.

Biography

Caixue Zhou received BS degree in Computer Science Department from Fudan University in 1988, Shanghai, China and MS degree in Space College of Beijing University of Aeronautics and Astronautics in 1991, Beijing, China. He is an Associate Professor in the School of Information Science and Technology, Jiujiang University, Jiujiang, China since 2007. He is a member of the CCF (China Computer Federation) and a member of CACR(Chinese Association for Cryptologic Research). His research interests include applied cryptography, security of computer networks.

Yue Zhang received BS degree in College of Computer Science from Chongqing University in 2004, Chongqing, China and MS degree in School of Computer Science and Technology from Huazhong University of Science and Technology in 2008, Wuhan, China. She is a lecturer in the School of Information Science and Technology, Jiujiang University, JiuJiang, China since 2007. Her research interests include applied cryptography, network and information security.

Lingmin Wang received BS degree in computer science and technology from Shenyang Normal University in 2003, Shenyang, China and MS degree in School of Computer Science and Technology from Huazhong University of Science and Technology in 2009, Wuhan,China. She is a lecturer in the School of Information Science and Technology, Jiujiang University, Jiujiang, China since 2007. She is a member of the CCF(China Computer Federation). Her research interest includes security of computer networks.

Cryptanalysis of Two Strongly Unforgeable Identity-based Signatures in the Standard Model

Wenjie Yang[1,2], Min-Rong Chen[2], and Guo-Qiang Zeng[3]
(Corresponding author: Min-Rong Chen)
College of Cyber Security, College of Information Science and Technology, Jinan University[1]
School of Computer, South China Normal University[2]
Guangzhou 510631, China
(Email: mrongchen@126.com)
National-Local Joint Engineering Laboratory of Digitalize Electrical Design Technology, Wenzhou University[3]
(Received July 14, 2017; revised and accepted Oct. 22, 2017)

Abstract

The strong unforgeability of digital signature means that no attacker can forge a valid signature on a message, even given some previous signatures on the message, which has been widely accepted as a common security requirement. Recently, Tsai *et al.* and Hung *et al.* presented an efficient identity-based signature scheme and a revocable identity-based signature scheme, respectively. Meanwhile, they all claimed that their scheme is strongly unforgeable against chosen message attacks. In this paper, we point out that the two schemes cannot meet the requirements of strong unforgeability by giving some concrete attacks and briefly analyze the reasons why the provably-secure schemes are insecure following their security model.

Keywords: Cryptanalysis; Identity-Based Signature; Strong Unforgeability

1 Introduction

To simplify the complicated certificate management in traditional public key systems, Shamir [11] introduced the concept of identity-based public key cryptography (IB-PKC). In IB-PKC settings, an entity's public key is some unique public information such as ID card, email address, while the corresponding private key are directly derived by the private key generator (PKG) from these public identity information. Moreover, the author addressed the first identity-based signature (IBS) scheme. Since then, a few classic IBS schemes [3, 5] were presented in random oracles following Shamir's idea.

As shown in [2], however, a security proof in random oracles can only serve as a heuristic argument and does not necessarily imply the security in the real implementation. It arises interest to construct a IBS scheme provably secure without random oracles. Until 2006, the first practical IBS scheme provably secure in the standard model was presented in [9]. Unfortunately, it does not cover the strong unforgeability [1] which is needed in a variety of applications. Afterwards, lots of improved IBS schemes were proposed to meet the requirements of strong unfrogeability in the standard model [7, 8, 10].

Recently, Tsai *et al.* [12] analyzed the existing strongly unforgeable IBS schemes without using random oracles and proposed an efficient and practical IBS scheme with short signature that is secure without random oracles. In the same year, Hung *et al.* [4] introduced a revocable identity-based signature (RIBS) scheme in the standard model. They all claimed that their (R)IBS scheme is strongly unforgeable against chosen message attacks.

In this paper, we first illustrate that Tsai *et al.*'s IBS scheme cannot meet the requirements of strong unforgeability by giving some concrete attacks. Then, we demonstrate that an attacker can easily discover the difference between simulated signatures and real signatures by interacting with the challenger. Finally, we show that Hung *et al.*'s RIBS scheme is actually based on Tsai *et al.*'s IBS scheme and can give some similar cryptanalysis according to the same ideas.

The rest of this paper is organized as follows. Section 2 gives some preliminaries. In Section 3, we review Tsai *et al.*'s IBS scheme and cryptanalyze its security. In Section 4, we look back Hung *et al.*'s RIBS scheme and briefly do some cryptanalysis on it. Finally, the conclusion is given in Section 5.

2 Preliminaries

2.1 Bilinear Groups and Complexity Assumption

Bilinear groups: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of same prime order p and g be a gen-

erator of $\mathbb{G}_1$. The bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ has the following properties [6,13]:

- Bilinearity: $\forall g, h \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_p^*$, we have $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$;
- Non-degenracy: $\hat{e}(g, g) \neq 1_{\mathbb{G}_2}$ for $1_{\mathbb{G}_2}$ denotes the identity element of $\mathbb{G}_2$;
- Computability: There exists an efficient algorithm to compute $\hat{e}(g, h)$.

Computational Diffie-Hellman (CDH) Assumption: Let $(\mathbb{G}_1, \mathbb{G}_2, p, \hat{e})$ be a description of the bilinear group of prime order p. g is a generator of subgroup $\mathbb{G}_1$. The CDH assumption is that if the challenge tuple $D = ((\mathbb{G}_1, \mathbb{G}_2, p, \hat{e}), g, g^a, g^b)$ is given, no probabilistic polynomial time (PPT) algorithm $\mathcal{A}$ can output $g^{ab} \in \mathbb{G}_1$ with more than a negligible advantage. The advantage of $\mathcal{A}$ is defined as $\mathbf{Adv}_{\mathcal{A}}^{CDH}(\lambda) = Pr[\mathcal{A}(D) = g^{ab}]$ where the probability is taken over random choices of $a, b \in \mathbb{Z}_p$.

2.2 Collision Resistant Hash (CRH) Assumption

Let $H_k : \{0,1\}^* \to \{0,1\}^n$ be a collision-resistant hash family of functions, where n is a fixed length and k is an index. We say that the $(\epsilon, t)-$CRH assumption holds if no polynomial time adversary $\mathcal{A}$ running in time at most t can break the collision resistance of H_k with probability ϵ. Here, the successful probability of the adversary $\mathcal{A}$ is presented as $Pr[\mathcal{A}(k) = (m_0, m_1) : m_0 \neq m_1, H_k(m_0) = H_k(m_1)]$, where the probability is over the random choice consumed by the adversary $\mathcal{A}$.

2.3 Frameworks and Security Notions

Identity-Based Signature (IBS) Scheme consists of four polynomial-time algorithms as follows:

Setup. Given a security parameter κ, this algorithm produces a master secret key msk and the corresponding public parameters $params$. Then $params$ are published and msk is kept by itself.

Extract. Given a user's identity ID, the public parameters $params$ and the master secret key msk, this algorithm computes a private key D_{ID} for ID, which is transmitted to the user ID through a secure channel.

Sign. Given a private key D_{ID} of a user ID and a message m, this algorithm running by the user ID generates and outputs a signature σ of ID on m.

Verify. Given a user's identity ID, a message m and a signature σ, a verifier checks the validity of σ. More precisely, the algorithm outputs 1 if accepted, or 0 if rejected.

Strong Unforgeability for Identity-Based Signature Here, we denote by $\mathcal{O}_E$ an oracle simulating the algorithm *Extract*, and by $\mathcal{O}_S$ an oracle simulating the algorithm *Sign*. Strong unforgeability under an adaptive chosen-message attack is defined using the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

Setup: $\mathcal{C}$ picks a security parameter κ and runs the algorithm *Setup*. It keeps the master secret key msk to itself and gives $\mathcal{A}$ the resulting parameters $params$.

Extract queries: $\mathcal{A}$ adaptively asks for the private key of any identity ID_i. To each extraction query of ID_i, $\mathcal{C}$ responds by running $\mathcal{O}_E$ to generate the private key D_{ID_i} of ID_i and forwarding D_{ID_i} to $\mathcal{A}$.

Signing queries: $\mathcal{A}$ adaptively asks for the signature of any identity ID_i on any message m_i. To each signing query of ID_i on M_i, $\mathcal{C}$ responds by running $\mathcal{O}_S$ to generate a signature σ, and sending σ to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs (ID^*, m^*, σ^*) and wins if the followings hold:

1) σ^* is a valid signature of ID^* on m^*;
2) ID^* is not queried during extract queries;
3) (ID^*, m^*, σ^*) is not queried during the sign queries.

We define $\mathbf{Adv}_{\mathcal{A}}$ to be the probability that $\mathcal{A}$ wins the above game, taken over all coin toss of $\mathcal{C}$ and $\mathcal{A}$. In this paper, $\mathcal{A}$ is said to $(t, q_e, q_s, \varepsilon)$-strongly break an identity-based signature (IBS) scheme if $\mathcal{A}$ runs in time at most t, makes at most q_e *extract* queries, at most q_s *signing* queries, and $\mathbf{Adv}_{\mathcal{A}}$ is at least ε. An IBS scheme is $(t, q_e, q_s, \varepsilon)$-strongly existential unforgeable under an adaptive chosen message attack if no adversary $(t, q_e, q_s, \varepsilon)$-strongly breaks it.

Revocable Identity-Based Signature (RIBS) Scheme consists of five polynomial-time algorithms as follows.

Setup. Given a security parameter κ and the total number z of all periods, this algorithm outputs a master secret key msk and the corresponding public parameters $params$. Then $params$ are published and msk is kept by the PKG.

Initial key extract. Given an identity ID, the public parameters $params$ and the master secret key msk, this algorithm outputs the initial key D_{ID} which is transmitted to the user ID through a secure channel.

Time key update. Given an identity ID, a time period t, the public parameters $params$ and the master secret key msk, this algorithm outputs the time key T_{ID} which is transmitted to the user through a public channel. The user can combine the initial key D_{ID} and the time key T_{ID} to obtain the full private key $S_{ID,t}$.

Sign. Given an identity ID, the corresponding private key $S_{ID,t}$, a time period t and a message m, this algorithm outputs a signature σ of ID on m in t.

Verify. Given an identity ID, a message m and a signature σ, a verifier checks the validity of σ in the period t. More precisely, the algorithm outputs 1 if accepted, or 0 if rejected.

Strong Unforgeability for Revocable Identity-Based Signature Here, we denote by $\mathcal{O}_E$ an oracle simulating the algorithm *Initial key extract*, by $\mathcal{O}_T$ an oracle simulating the algorithm *Time key update*, and by $\mathcal{O}_S$ an oracle simulating the algorithm *Sign*. Strong unforgeability under an adaptive chosen-message attack is defined using the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

Setup: $\mathcal{C}$ picks a security parameter κ and runs the algorithm *Setup*. It keeps the master secret key msk to itself and gives $\mathcal{A}$ the resulting parameters *params*.

Extract queries: $\mathcal{A}$ adaptively asks for the initial key of any identity ID. To each extraction query of ID, $\mathcal{C}$ responds by running $\mathcal{O}_E$ to generate the initial key D_{ID} and forwarding D_{ID} to $\mathcal{A}$.

Update queries: $\mathcal{A}$ adaptively asks for the time key of any identity ID in period t. To each update query of ID, $\mathcal{C}$ responds by running $\mathcal{O}_T$ to generate the time key T_{ID} and forwarding T_{ID} to $\mathcal{A}$.

Signing queries: $\mathcal{A}$ adaptively asks for the signature of any identity ID on any message m in period t. To each signing query, $\mathcal{C}$ responds by running $\mathcal{O}_S$ to generate a signature σ and sending σ to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs $(ID^*, m^*, t^*, \sigma^*)$ and wins if the following holds:

1) σ^* is a valid signature of ID^* on m^* in t^*;
2) σ^* has not been outputted in the signing queries on (ID^*, m^*, t^*);
3) Either ID^* or (ID^*, t^*) has not appeared in the extract queries or the update queries, respectively.

The adversary $\mathcal{A}$'s advantage is defined as the probability that $\mathcal{A}$ wins the above game. In addition, to simplify the security analysis, we consider two types of adversaries, namely, outside adversary and inside adversary (or revoked user). Note that if the adversary is an outsider, it is allowed to issue all queries in the above game except for the initial key extract query on the target identity ID^*. If the adversary is an insider, it is allowed to issue all queries in the above game except for the time key update query on (ID^*, t^*).

3 Tsai *et al.*'s IBS Scheme

3.1 Review of Tsai *et al.*'s Scheme

The strongly unforgeable identity-based signature scheme [12] is specified by the following four algorithms.

Setup. Given a security parameter κ, the PKG chooses two groups $\mathbb{G}_1$, $\mathbb{G}_2$ of sufficiently large prime order $p > 2^\kappa$, a generator g of $\mathbb{G}_1$ and an admissible bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. The PKG sets three collision resistant hash functions, namely, $H_1 : \{0,1\}^* \to \{0,1\}^m$, H_2 and $H_3 : \{0,1\}^* \to \{0,1\}^n$, where m and n are fixed lengths. We assume $p > 2^m$ and $p > 2^n$ so that the hash outputs can be viewed as the elements of $\mathbb{Z}_p$. The PKG chooses two random values $u', w' \in \mathbb{G}_1$ as well as two vectors $\vec{u} = (u_i)$ of length m and $\vec{w} = (w_j)$ of length n, where u_i, $w_j \in \mathbb{G}_1$ for $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$. The PKG then chooses a secret random value $\alpha \in \mathbb{Z}_p^*$ and sets $g_1 = g^\alpha \in \mathbb{G}_1$. Finally, the PKG randomly chooses $g_2 \in \mathbb{G}_2$ and sets the master secret key $msk = g_2^\alpha$ and the public parameters $params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, u', \vec{u}, w', \vec{w})$.

Extract. Given a user's identity $ID \in \{0,1\}^*$, the PKG sets $v = H_1(ID)$. Here, $v = (v_1, v_2, ..., v_m)$ is a bit string of length m. Let $U \subset \{1, 2, ..., m\}$ be the set of index i such that $v_i = 1$, for $i = 1, 2, ..., m$. The PKG chooses a random value $r_v \in \mathbb{Z}_p^*$ and computes the user's private key $D_{ID} = (D_1, D_2) = (g_2^\alpha (u' \prod_{i \in U} u_i)^{r_v}, g^{r_v})$. The PKG transmits D_{ID} to the user via a secure channel.

Sign. Given a message $m \in \{0,1\}^*$, let $vm = H_2(m)$ be a bit string of length n and let vm_j denote the jth bit of vm. Let $W \subset \{1, 2, ..., n\}$ be the set of index j such that $vm_j = 1$, for $j = 1, 2, ..., n$. The signer with identity ID chooses a random number $r_m \in \mathbb{Z}_p^*$ and then computes $h = H_3(m \| g^{r_m})$. The signer uses her/his private key $D_{ID} = (D_1, D_2)$ to create a signature on the message m by $\sigma = (D_1^h (w' \prod_{j \in W} w_j)^{r_m}, D_2^h, g^{r_m})$.

Verify. Given a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ of a signer ID on a message m, a verifier can compute $h = H_3(m \| \sigma_3)$ to validate the signature tuple by the equation

$$\hat{e}(\sigma_1, g) \stackrel{?}{=} \hat{e}(g_1, g_2)^h \hat{e}(u' \prod_{i \in U} u_i, \sigma_2) \hat{e}(w' \prod_{i \in W} w_i, \sigma_3).$$

The algorithm outputs "accept" if the above equation holds, and "reject" otherwise.

3.2 A Concrete Attack

Now, we shall in detail show how an attacker $\mathcal{A}$ forges a new signature σ' for a previously signed message m by interacting with the challenger $\mathcal{C}$ according to the security model [12].

1) $\mathcal{C}$ takes a security parameter κ and runs the *Setup* algorithm to produce a master secret key $msk = g_2^{\alpha}$ and public parameters $params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, u', \vec{u}, w', \vec{w})$. $\mathcal{C}$ then gives $params$ to $\mathcal{A}$ and keeps msk by itself.

2) Given any user's identity ID and any message m, $\mathcal{C}$ runs the *Sign* algorithms in Tsai *et al.*'s scheme and produces the corresponding signature σ for m under ID. The signature's concrete forms are as follows, where $h = H_3(m\|g^{r_m})$.

$$\begin{aligned}\sigma &= (\sigma_1, \sigma_2, \sigma_3)\\ &= (D_1^h(w'\prod_{j\in W} w_j)^{r_m}, D_2^h, g^{r_m})\\ &= ((g_2^{\alpha}(u'\prod_{i\in U} u_i)^{r_v})^h(w'\prod_{j\in W} w_j)^{r_m}, g^{r_v h}, g^{r_m})\end{aligned}$$

3) $\mathcal{A}$ picks $r'_v \in_R \mathbb{Z}_p^*$ and computes a new signature σ' for m under ID with $\sigma'_1 = \sigma_1((u'\prod_{i\in U} u_i)^{r'_v})^h = (g_2^{\alpha}(u'\prod_{i\in U} u_i)^{r_v+r'_v})^h(w'\prod_{j\in W} w_j)^{r_m}$, $\sigma'_2 = \sigma_2 g^{r'_v h} = g^{(r_v+r'_v)h}$ and $\sigma'_3 = \sigma_3$, where $h = H_3(m\|g^{r_m})$.

It is clear that σ' is a new valid signature for m on ID since

$$\begin{aligned}&\hat{e}(\sigma'_1, g)\\ =\ &\hat{e}((g_2^{\alpha}(u'\prod_{i\in U} u_i)^{r_v+r'_v})^h(w'\prod_{j\in W} w_j)^{r_m}, g)\\ =\ &\hat{e}((g_2^{\alpha})^h, g)\hat{e}(((u'\prod_{i\in U} u_i)^{r_v+r'_v})^h, g)\hat{e}((w'\prod_{j\in W} w_j)^{r_m}, g)\\ =\ &\hat{e}(g_1, g_2)^h\hat{e}(u'\prod_{i\in U} u_i, \sigma'_2)\hat{e}(w'\prod_{i\in W} w_i, \sigma'_3).\end{aligned}$$

Thus, the scheme fails to satisfy the requirement of strong unforgeability.

3.3 Flaws in the Security Proof

It is well known that a provably-secure cryptographic scheme should resist all attacks under the appropriate adversarial model. Then, why is Tsai *et al.*'s IBS scheme which is strictly proven under their security model not secure? In fact, there exist some fatal flaws in Tsai *et al.*'s security proof as follows.

• *Signing query*(ID, m). Upon receiving the query along with (ID, m), the challenger $\mathcal{C}$ sets $v = H_1(ID)$ and $vm = H_2(m)$.

Case 1. If $F(v) \neq 0 \bmod l_v$, the challenger $\mathcal{C}$ can construct the private key for $v = H_1(ID)$ as in the extract query, and then use the Signing algorithm to respond a signature σ on m.

Case 2. If $F(v) = 0 \bmod l_v$ and $K(vm) = 0 \bmod l_m$, the challenger $\mathcal{C}$ reports failure and terminates. Otherwise, if $F(v) = 0 \bmod l_v$ and $K(vm) \neq 0 \bmod l_m$, the challenger $\mathcal{C}$ chooses two random values $r_v, r_m \in \mathbb{Z}_p^*$ and then computes $h = H_3(m\|g^{r_m})$ to generate the simulated signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, where $\sigma_3 = g_1^{\frac{-h}{K(vm)}} \cdot g^{r_m}$.

From the above descriptions, we notice that if $F(v) = 0 \bmod l_v$ (where $v = H_1(ID)$), $\mathcal{C}$ cannot respond a valid signature σ on message m under the identity ID since $H_3(m\|g^{r_m}) \neq H_3(m\|\sigma_3)$. That is to say, an adversary can easily distinguish the distribution of simulated signatures from that of real signatures by making some signing queries under the target identity ID^* and message m^*. Therefore, the security argument of Tsai *et al.*'s IBS scheme did not work out exactly as their simulated game definition.

4 Hung *et al.*'s RIBS Scheme

4.1 Review of Hung et al.'s Scheme

Here, we review the strongly secure revocable identity-based signature scheme [4] by the five algorithms below.

Setup. Given a security parameter κ and the total number z of all periods, the PKG chooses two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of sufficiently large prime order $p > 2^{\kappa}$. Let g be a generator of $\mathbb{G}_1$ and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be an admissible map. The PKG sets the master secret key and the public parameters by running the following tasks.

1) Pick two secret values $\alpha, \beta \in Z_p^*$ at random and compute $g_1 = g^{\alpha+\beta} \in \mathbb{G}_1$. Select a random $g_2 \in \mathbb{G}_1$ and compute g_2^{α} and g_2^{β}.
2) Set four collision resistant hash functions $H_1 : \{0,1\}^* \to \{0,1\}^{n_u}$, $H_2 : \{0,1\}^* \to \{0,1\}^{n_t}$, $H_3, H_4 : \{0,1\}^* \to \{0,1\}^{n_m}$, where n_u, n_t and n_m are fixed lengths.
3) Choose three random values $u', t', w' \in \mathbb{G}_1$ and three vectors $\vec{U} = (u_i)$, $\vec{T} = (t_j)$, $\vec{W} = (w_k)$, where $u_i, t_j, w_k \in \mathbb{G}_1$ for $i = 1, 2, ..., n_u$, $j = 1, 2, ..., n_t$ and $k = 1, 2, ..., n_m$.
4) Finally, the PKG sets the master secret key $msk = (g_2^{\alpha}, g_2^{\beta})$ and the public parameters $params$= ($\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$, g, g_1, g_2, H_1, H_2, H_3, H_4, u', $\vec{U}$, t', $\vec{T}$, w', $\vec{W}$).

Initial key extract. Given a user's identity $ID \in \{0,1\}^*$, the PKG sets $vu = H_1(ID)$. Here, $vu = (vu_1, vu_2, ..., vu_{n_u})$ is a bit string of length n_u. Let $U \subset \{1, 2, ..., n_u\}$ be the set of indices i such that $vu_i = 1$, for $i = 1, 2, ..., n_u$. The PKG chooses a random value $r_u \in \mathbb{Z}_p^*$ and computes the user's private key $D_{ID} = (D_1, D_2) = (g_2^{\alpha}(u'\prod_{i\in U} u_i)^{r_u}, g^{r_u})$. The PKG transmits D_{ID} to the user via a secure channel.

Time key update. Given a user's identity $ID \in \{0,1\}^*$ and a period t, the PKG sets $vt = H_2(ID, t)$. Here,

$vt = (vt_1, vt_2, ..., vt_{n_t})$ is a bit string of length n_t. Let $T \subset \{1, 2, ..., n_t\}$ be the set of indices j such that $vt_j = 1$, for $j = 1, 2, ..., n_t$. The PKG chooses a random value $r_t \in \mathbb{Z}_p^*$ and computes the user's private key $T_{ID} = (T_1, T_2) = (g_2^{\beta}(t' \prod_{j \in T} t_j)^{r_t}, g^{r_t})$. The PKG sends T_{ID} to the user via a public channel. Upon receiving T_{ID}, the user combines it with his/her initial secret key $D_{ID} = (D_1, D_2)$ to obtain the signing key $S_{ID,t}$ =(S_1, S_2, S_3)=(D_1T_1, D_2, T_2)= $(g^{\alpha+\beta}(u' \prod_{i \in U} u_i)^{r_u}(t' \prod_{j \in T} t_j)^{r_t}, g^{r_u}, g^{r_t})$.

Sign. For a period t, given a non-revoked user's identity $ID \in \{0,1\}^*$, a message $m \in \{0,1\}^*$, the user first computes a string $vm = H_3(m)$ of length n_m. Let vm_k denote the k-th bit of the string vm and let $W \subset \{1, 2, ..., n_m\}$ be the set of indices k such that $vm_k = 1$ for $k = 1, 2, ..., n_m$. Then the user chooses a random number $r_m \in Z_p^*$ and computes g^{r_m} and $h = H_4(m \| g^{r_m})$. Finally, the user generates a signature σ on the message m as follows:

$$\begin{aligned}\sigma &= (\sigma_1, \sigma_2, \sigma_3, \sigma_4)\\ &= (S_1^h(w' \prod_{k \in W} w_k)^{r_m}, S_2^h, S_3^h, g^{r_m})\\ &= (g_2^{(\alpha+\beta)h}(u' \prod_{i \in U} u_i)^{r_u h}(t' \prod_{j \in T} t_j)^{r_t h}(w' \prod_{k \in W} w_k)^{r_m},\\ &\quad g^{r_u h}, g^{r_t h}, g^{r_m}),\end{aligned}$$

where (S_1, S_2, S_3) is the signing key $S_{ID,t}$ obtained above.

Verify. Given a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ of a signer ID on a message m in a period t, a verifier can compute $h = H_4(m \| \sigma_4)$ to validate the signature tuple by the following equation

$$\begin{aligned}\hat{e}(\sigma_1, g) \stackrel{?}{=}\ & \hat{e}(g_1, g_2)^h \hat{e}(u' \prod_{i \in U} u_i, \sigma_2) \cdot\\ & \hat{e}(t' \prod_{j \in T} t_j, \sigma_3) \hat{e}(w' \prod_{k \in W} w_k, \sigma_4).\end{aligned}$$

The algorithm outputs "accept" if the above equation holds, and "reject" otherwise.

4.2 Some Concrete Attacks

In fact, Hung *et al.*'s RIBS scheme is based on Tsai *et al.*'s IBS scheme. Thus, we can easily give a similar cryptanalysis according to the same ideas in Subsection 3.2. Here, we shall show how an attacker $\mathcal{A}$ forges a new signature σ' for a previously signed message m by interacting with the challenger $\mathcal{C}$ under the security model defined in [4].

1) $\mathcal{C}$ takes a security parameter κ and runs the *Setup* algorithm to produce the master secret key $msk = (g_2^{\alpha}, g_2^{\beta})$ and the public parameters $params$= ($\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$, g, g_1, g_2, H_1, H_2, H_3, H_4, u', $\vec{U}$, t', $\vec{T}$, w', $\vec{W}$). $\mathcal{C}$ then gives $params$ to $\mathcal{A}$ and keeps msk by itself.

2) Given any user's identity ID, a period t and any message m, $\mathcal{C}$ runs the *Sign* algorithms in Hung *et al.*'s scheme and outputs the corresponding signature σ for m under ID in t. The signature's concrete forms are as follows, where $h = H_3(m \| g^{r_m})$.

$$\begin{aligned}\sigma &= (\sigma_1, \sigma_2, \sigma_3, \sigma_4)\\ &= (S_1^h(w' \prod_{k \in W} w_k)^{r_m}, S_2^h, S_3^h, g^{r_m})\\ &= (g_2^{(\alpha+\beta)h}(u' \prod_{i \in U} u_i)^{r_u h}(t' \prod_{j \in T} t_j)^{r_t h}(w' \prod_{k \in W} w_k)^{r_m},\\ &\quad g^{r_u h}, g^{r_t h}, g^{r_m})\end{aligned}$$

3) $\mathcal{A}$ picks two random values r'_u and r'_t from $\mathbb{Z}_p^*$ and forges a new signature σ' on m under ID in t as follows, where $h = H_3(m \| g^{r_m})$.

$$\begin{aligned}\sigma'_1 &= \sigma_1((u' \prod_{i \in U} u_i)^{r'_u})^h((t' \prod_{j \in T} t_j)^{r'_t})^h\\ &= (g_2^{\alpha+\beta}(u' \prod_{i \in U} u_i)^{r_u + r'_u}(t' \prod_{j \in T} t_j)^{r_t + r'_t})^h(w' \prod_{j \in W} w_j)^{r_m}\end{aligned}$$

$\sigma'_2 = \sigma_2 g^{r'_u h} = g^{(r_u + r'_u)h}$, $\sigma'_3 = \sigma_3 g^{r'_t h} = g^{(r_t + r'_t)h}$ and $\sigma'_4 = \sigma_4$.

It is clear that σ' is a new valid signature for m on ID in t since

$$\begin{aligned}&\hat{e}(\sigma'_1, g)\\ =\ & \hat{e}(g_2^{(\alpha+\beta)h}(u' \prod_{i \in U} u_i)^{(r_u + r'_u)h}(t' \prod_{j \in T} t_j)^{(r_t + r'_t)h}\\ & (w' \prod_{k \in W} w_k)^{r_m}, g)\\ =\ & \hat{e}(g_2^{(\alpha+\beta)h}, g)\hat{e}((u' \prod_{i \in U} u_i)^{(r_u + r'_u)h}, g) \cdot\\ & \hat{e}((t' \prod_{j \in T} t_j)^{(r_t + r'_t)h}, g)\hat{e}((w' \prod_{k \in W} w_k)^{r_m}, g)\\ =\ & \hat{e}(g_1, g_2)^h \hat{e}(u' \prod_{i \in U} u_i, \sigma'_2)\hat{e}(t' \prod_{j \in T} t_j, \sigma'_3)\hat{e}(w' \prod_{k \in W} w_k, \sigma'_4).\end{aligned}$$

Therefore, the RIBS scheme fails to meet the requirement of strong unforgeability under their security model. For more details about cause analysis, the interested readers are referred to Section 3.3.

5 Conclusion

Strong unforgeability has been widely accepted as a common security requirement for signature schemes. In this paper, we first reviewed two so-called strongly unforgeable identity-based signatures presented by Tsai *et al.* and Hung *et al.*, respectively. Then, we demonstrated that both of them are not strongly unforgeable by giving some concrete attacks. Finally, we illustrated that there exist some serious errors in their proving process.

Acknowledgements

The authors would like to thank Prof. Jian Weng for his helpful comments. This work was supported by National Science Foundation of China (Grant Nos. 61472165, 61373158 and 61732021), Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defence (Grant No. 2014B090904067), Guangdong Provincial Special Funds for Applied Technology Research and development and Transformation of Important Scientific and Technological Achieve (Grant No. 2016B010124009), the Zhuhai Top Discipline–Information Security, Guangzhou Key Laboratory of Data Security and Privacy Preserving, Guangdong Key Laboratory of Data Security and Privacy Preserving, Zhejiang Provincial Natural Science Foundation of China (Grant Nos. LY16F030011 and LZ16E050002).

References

[1] D. Boneh, E. Shen, and B. Waters, "Strongly unforgeable signatures based on computational diffiehellman," in *Proceedings of The nineth international Conference on Theory and Practice in Public Key Cryptography (PKC2006)*, pp. 229–240, June 2006.

[2] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, no. 35, 2004.

[3] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, 2017.

[4] Y. H. Hung, T. T. Tsai, Y. M. Tseng, and S. S. Huang, "Strongly secure revocable id-based signature without random oracles," *Information Technology and Control*, vol. 43, no. 3, 2014.

[5] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[6] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of Proxy Signature Based on Elliptic Curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[7] S. Kwon, "An identity-based strongly unforgeable signature without random oracles from bilinear pairings," *Information Sciences*, vol. 276, no. 32, pp. 1–9, 2014.

[8] Y. Ming and Y. M. Wang, "Cryptanalysis of an identity based signcryption scheme in the standard model," *International Journal of Network Security*, vol. 18, no. 1, pp. 165–171, 2016.

[9] K. G. Paterson and J. C. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Proceedings of The Eleventh Australasian Conference on Information Security and Privacy (ACISP'06)*, pp. 207–222, June 2006.

[10] C. Sato, T. Okamoto, and E. Okamoto, "Strongly unforgeable id-based signatures without random oracles," in *Proceedings of The Fifth International Conference on Information Security Practice and Experience (ISPEC'09)*, pp. 35–45, June 2009.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of The Fourth Annual International Cryptology Conference*, pp. 47–53, June 1984.

[12] T. T. Tsai, Y. M. Tseng, and S. S. Huang, "Efficient strongly unforgeable id-based signature without random oracles," *Informatica*, vol. 25, no. 3, pp. 505–521, 2014.

[13] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

Biography

Wenjie Yang is working toward his PhD degree in College of Cyber Security/College of Information Science and Technology, Jinan University at Guangzhou, P.R. China. His research interests focus on Cryptography and Information Security.

Min-Rong Chen received the B.S. degree and the M.S degree from South China University of Technology, Guangzhou, China, in 2000 and 2004, respectively, and the PhD degree from Shanghai Jiaotong University, Shanghai, China, in 2008. From 2008 to 2015, she was an Associate Professor with the College of Information Engineering, Shenzhen University, Shenzhen, China. She is currently an Associate Professor with the School of Computer, South China Normal University, Guangzhou, China. She has headed two national projects. She has authored or co-authored the book Extremal optimization: Fundamentals, algorithms, and applications (CRC press, 2016), over 30 journal and conference papers. She holds one patent. Her research interests include computational intelligence and information security.

Guo-Qiang Zeng received the B.S. degree in automation from China Jiliang University, Hangzhou, China, in 2006, and the PhD degree in control science and engineering from Zhejiang University, China, in 2011. From 2011 to 2014, he was a Lecturer with the Department of Electrical and Electronic Engineering, Wenzhou University, Wenzhou, China. Since 2015, he has been an Associate Professor with the National-Local Joint Engineering Laboratory of Digitalize Electrical Design Technology, Wenzhou University. He has headed three national and provincial projects. He has authored or co-authored the book Extremal optimization: Fundamentals, algorithms, and applications (CRC press, 2016), over 30 journal and conference papers, and over ten inventions. He holds seven patents. His research interests include computational intelligence and information security.

A High-efficiency Discrete Logarithm-based Multi-proxy Blind Signature Scheme via Elliptic Curve and Bilinear Mapping

Lin Teng and Hang Li
(Corresponding author: Hang Li)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: 1451541@qq.com)

(Received July 14, 2017; revised and accepted Oct. 22, 2017)

Abstract

Generally, multi-proxy blind signature scheme has been proposed to provide privacy protection. However, multi-proxy blind signature scheme requires their signatures of all the proxy signers. So there are some drawbacks about proxy signature. Proxy knows all the information of signers, it will lead to information leakage. Therefore, we propose a discrete logarithm-based multi-proxy blind signature scheme in this paper. The new scheme combines Elliptic curve, bilinear mapping and blind signature. Elliptic curve can avoid that a proxy signer is absent or makes mistakes causing unsuccessful signature. It enhances the robustness and fault tolerance. Meanwhile, blind idea makes proxy signers have no information about sensitive message. Bilinear mapping can reduce the computation time. Finally, the security analysis shows that this new scheme is with more flexibility and fault tolerance than traditional multi-proxy signature schemes. And it can be widely used in many real engineering applications.

Keywords: Blind Signature; Bilinear Mapping; Discrete Logarithm; Elliptic Curve; Multi-proxy Blind Signature Scheme

1 Introduction

Proxy signature means that a designated proxy signer can generate valid signatures on behalf of the original signer in an agent signature scheme [12, 13, 18]. It allows the original signer to delegate the signature to the proxy signer and generate an effective proxy signature. Proxy signature contains initialization process, authorization process, proxy signature generation process and proxy signature verification process. Traditional proxy signature schemes are easily attacked and sensitive information is leaked [7, 10, 16]. Then in order to meet the actual demand, some improved proxy signatures are proposed.

Xie *et al.* [26] proposed that in the system initialization phase, when each user's public key was certified by CA, the registering user must perform a challenge-response protocol or zero-knowledge protocol to convince CA that he knew the private key corresponding to his public key. Ma *et al.* [17] proposed a proxy signature-based re-authentication scheme for secure fast handoff in WMNs. To begin with, he designated the mesh portal (MPP) as the authenticator of the MH that initially accessed a certain mesh domain. After the successful initial association, the MH was authorized to obtain a temporal proxy delegation of the MPP for the preparation of handoff. Making use of the proxy delegation in handoff case, the MH could efficiently associate with a target MAP connecting to the MPP by performing the proposed re-authentication scheme, in which mutual authentication and pairwise master key (PMK) establishment were performed between the MH and the MAP in a three-way handshake procedure without involving any other parties.

A proxy signature scheme allowed a proxy signer to sign messages on behalf of an original signer within a given context. Most identity based proxy signature schemes currently known employ bilinear pairings. So an identity based proxy ring signature (IBPS) scheme from RSA without pairings was constructed, and the security was proved under the random oracle model [4]. Lan *et al.* [11] put forward a new security cloud storage data encryption scheme based on identity proxy re-encryption. This scheme could flexibility share data with other users security without fully trusted cloud. For the detailed structure, he used a strong unforgeable signature scheme to make the transmuted ciphertext had publicly verification combined identity-based encryption. Furthermore, the transformed ciphertext had chosen-ciphertext security under the standard model. Liu *et al.* [14] constructed the initial threshold proxy signature scheme independently, which is an improvement for proxy signature scheme.

In a (t, n) threshold proxy signature scheme, an original signer delegates his signature right to n proxy signers, in which cooperation of t proxy signers can produce a valid proxy signature. Then a lot of threshold proxy signature schemes are proposed [2, 8, 15, 22, 28, 29].

Through the above analysis, we make a summary on the type of proxy signature scheme.

1) Proxy multi-signature [27]. $m \to 1$, m original signers delegate the signature to one proxy signer.

2) Multi-proxy signature [19, 23]. $1 \to n$, an original signer delegates the signature authority to n proxy signers.

3) Multi-proxy multi-signature [3, 12]. $m \to n$, m original signers delegate the signature to n proxy signers. It is an extension of $m \to 1$ and $1 \to n$ applications and increases the flexibility of scheme.

The rest of this paper is organized as follows. Section 2 and Section 3 introduce Bilinear map and Elliptic curve respectively. the system model for wireless body area network. Section 3 outlines the proposed scheme to analyze detailed processes. Experience and security analysis are given in Section 4. Section 5 finally concludes the paper.

2 Bilinear Map

Supposing G_0 and G_1 are two $p - order$ multiplicative cyclic groups [5]. g is a generator of G_0 and e is a bilinear map, namely $e : G_0 \times G_0 \to G_1$, then for any $i, j, k \in G_0$ and $a, b \in Z_p$, the map e has the following properties [21]:

1) Bilinear: $e(i^a, j^b) = e(i, j)^{ab}$.

2) Non-degenerative: $e(g, g) \neq 1$.

3) Polymerizability: $e(i \cdot j, k) = e(i, k) \times e(j, k)$.

If the group operation is highly computable in G_0 and the map $e : G_0 \times G_0 \to G_1$, then the group is called bilinear. So map e is commutative: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

3 Elliptic Curve (ECC)

The elliptic curve crypto-system is currently known as the public key system, which provides the highest encryption intensity for each bit [1]. Assuming that q is a big prime number. F_q is the finite field of q. r is a prime number. Therefore, Elliptic curve EC of F_q is defined as,

$$y^2 = x^3 + ax + b.$$

Where $(4a^3 + 27b^2) mod q \neq 0$. Elliptic curve encryption algorithm is with small key length, high safety performance, little digital signature time. In the application of intelligent terminal, it has great potential development, such as PDA, mobile phones. In the network, ECC algorithm also ensures its real-time collaborative work. Higher sensitivity level data encrypted by ECC algorithm , the speed can satisfy the large amount data, and the high security can well protect the safety of the system.

4 New Multi-proxy Blind Signature Scheme

First, we give the parameters used in this paper as shown in Table 1.

Assuming that the discrete logarithm problem in Z_p is difficult. And proxy signers, less than t, are dishonestly, that is, they unfaithfully execute the protocol.

4.1 Signature Scheme Based on Bilinear Map

Supposing that G_1 is the additive group with generator P and q order. G_2 is the multiplicative group with q order. Bilinear map is defined as $e : G_1 \times G_1 \to G_2$. $H_1 : 0, 1^* \to Z_q$ and $H_2 : 0, 1^* \to G_1$ are two Hash functions.

Detailed signature scheme based on bilinear map is as follows.

1) Key generation algorithm.

   - Private key generation. Randomly selecting $s \in Z_q^*$ as system private key.
   - Public key generation. P_{pub} as system public key, where $(G_1, G_2, q, P, P_{pub}, H_2)$ are public parameters.

2) Signature algorithm. For $M \in 0, 1^*$, signer computes $P_M = H_2(M) \in G_1$, $S_M = sP_M$. So the signature of information M is S_M.

3) Verification process. Verifying equation $e(S_M, P) = e(H_2(M), P_{pub})$. If it is correctness, then user accepts signature.

4.2 Generation Phase of Proxy Certificate

Assuming that m original signers and n proxy signers hold consultation the message range and the validity period of proxy for the proxy signature, and then it forms the Proxy Agent signature protocol W (including the public key of all original signers and proxy signers).

1) U_i randomly selects $k_{U_i} = Z_q^*$, calculates $L_{U_i} = g^{k_{U_i}} \bmod p$, and sends it to other $m - 1$ original signers and proxy signers. Each p_j randomly selects $k_{p_j} \in Z_q^*$, calculates $L_{p_j} = g^{k_{p_j}} \bmod p$, and sends it to other $n - 1$ proxy signers and m original signers. Finally, all original signers and proxy signers compute and save $K = \prod_{i=1}^{m} L_{U_i} \prod_{j=1}^{n} L_{p_j} \bmod p$.

Table 1: Parameter explanation

Symbol	Definition
p, q	Prime number. Where q is large prime factor of $p-1$.
g	$g \in Z_p^*$, $g^q \equiv 1(modp)$.
$h(\cdot)$	A secure one-way hash function.
$\|\|$	Concatenation of bit strings.
t	The threshold value.
x_{u_i}	Private key of original signer.
U_i	Original signer.
$y_{u_i} = g^{x_{u_i}} \bmod p$	Public key of original signer.
$x_{p_j} \in Z_q^*$	The private key of proxy signer.
$p_j = (1, 2, \cdots, n)$	Proxy signer.
$y_{p_j} = g^{x_{p_j}} \bmod p$	Public key of proxy signer.
ID_j	The identity information.
U_I	The message owner.

2) U_i calculates $V_{U_i} = (h(W)x_{U_i} + k_{U_i}K) \bmod q$, sends it to other $m-1$ original signers and n proxy signers. Personal delegation certificate of U_i is (L_{U_i}, V_{U_i}). p_j calculates $V_{p_j} = (h(W)x_{p_j} + k_{p_j}K) \bmod q$, sends it to other $n-1$ proxy signers and m original signers, then delegation certificate of p_j is (L_{p_j}, V_{p_j}).

3) Each $\frac{U_i}{p_j}$ verifies the correctness of the $\frac{V_{U_i}}{V_{p_j}}$ by following formulas:

$$g^{V_{U_i}} = y_{U_i}^{h(W)} L_{U_i}^K \bmod p, i = 1, 2, \cdots, m.$$

$$g^{V_{p_j}} = y_{p_j}^{h(W)} L_{p_j}^K \bmod p, j = 1, 2, \cdots, n.$$

If V_{U_i} and V_{p_j} are correct, then each proxy signer p_j computes $V = (\sum_{i=1}^{m} V_{U_i} + \sum_{j=1}^{n} V_{p_j})$ to generate the delegation proxy certificate K, V.

4.3 Generation Phase of Proxy Signature Key

When signature enters into $i-th$ phase, U uses the signature private key $x_{U_{i-1}}$ of $(i-1)th$ phase to calculate the signature private key x_{U_i} of $i-th$ phase.

$$x_{U_i} = x_{U_{i-1}} \bmod n.$$

Each p_j randomly selects $n_j \in Z_q^*$ and $a_{je} \in Z_q^*$, calculates and broadcasts $N_j = g^{n_j} \bmod p$ and $g^{a_{je}} \bmod p$ to other proxy signers. It requires that the product of any t N_j of the proxy signers is unequal. Meanwhile, It constructs a polynomial $f_j(x) = \sum_{e=0}^{t-1} a_{je}x^e \bmod q$, to satisfy $a_{j0} = (x_{p_j} + n_j V)$. p_j calculates and sends the subsecret $f_j(ID_i) \bmod q$ for other $p_i (o = 1, 2, \cdots, n, i \neq j)$, Calculate and save $f_j(ID_j) \bmod q$.

4.4 Generation Phase of Proxy Signature

Set the message m will be generated according to the will of the original signer. In this algorithm, each proxy member D_i will produce a part proxy signature for m according to generated proxy key K_i. Then it appoints one agent member M to collect all the proxy signatures and get the final proxy signature scheme.

1) Each proxy member D_i randomly generates integer $k_{p_i} \in Z_q^*$, computes $r_{p_i} = e(p, p)^{k_{p_i}}$. And r_{p_i} is broadcast to other $l-1$ proxy members.

2) Each proxy member D_i calculates $r_p = \prod_{i=1}^{l} r_{p_i}$ and $c_p = H_1(m||r_p), U_{p_i} = c_p s_{p_i} + k_{p_i} p$. So the part proxy signature of each proxy member for m is binary array (c_p, U_{p_i}).

3) Each proxy member D_i sends U_{p_i} to assigned member M.

4) M puts each proxy member's proxy signature into equation $c_p = H_1(m|| \prod_{i-1}^{l} e(U_{p_i}, p)(eH_2(\xi), pK_0 + pK_i))^{-c_p}$.

When all the proxy signature verifications are passed. M calculates $U_p = \sum_{i=1}^{l} U_{p_i}$. So the proxy signature of each proxy member for m is quaternion array (m, c_p, U_{p_i}, ξ).

4.5 Proxy Signature Verification Phase

Generated delegation proxy certificate (K, V) can verify the the validity of final signature. Due to $Y = \prod_{i=1}^{n} y_{p_i} modp$ and $Q = \prod_{i=1}^{n} N_i \bmod p$ The verification is as follows:

$$g^V = K^K (\prod_{i=1}^{m} y_{U_i} \prod_{j=1}^{n} y_{p_j})^{h(W)} \bmod p.$$

$$g^S = (YQ^V N^N)^{B+h(M)h(W)} \bmod p.$$

5 New Scheme Analysis

5.1 Security analysis

1) The security of the certificate.

Theorem 1. *Under the discrete logarithmic problem (DLP) difficulty assumption, personal delegation certificate of* $U_i(L_{U_i}, V_{U_i})$*, personal proxy certificate* (L_{p_j}, V_{p_j}) *of* p_j *and delegation proxy certificate* (K, V) *are safe.*

Proof. Assuming that the attacker A counterfeits a certificate (L'_{U_1}, V'_{U_1}) of U_1, it needs to meet: $g^{V'_{U_1}} = y_{U_1}^{h(W)}(L'^{K'}_{U_1})$, $K' = L'_{U_1}\prod_{i=2}^{m} L_{U_i}\prod_{j=1}^{n} L_{p_j}$. Setting a known L'_{U_1}, through the above two formulas to solve V'_{U_1}, it needs to solve the discrete logarithm in Z_p, so personal delegation certificate of U_1 is safe. Similarly, certificate (L_{p_j}, V_{p_j}) of p_j is safe. □

Let A counterfeits a delegation proxy certificate (K', V'), which needs to satisfy: $g^{V'} = K'^{K'}(\prod_{i=1}^{m} y_{U_i}\prod_{j=1}^{n} y_{p_j})^{h(W)} modp$. Under the DLP difficulty assumption, (K, V) is security.

2) Unforgeability. There are two existence-unforgeabilities of proxy signature: existence authorization-unforgeability and proxy signature existence-unforgeability.

Theorem 2. *Under the DLP difficulty assumption, the final proxy signature cannot be forged.*

Proof. If A directly constructs B' and forges S, it needs to solve the discrete logarithm or first forge part signature S'_i. But we use the following explanation to verify that S'_i cannot be forged. If A randomly selects n_i and c_i. It uses $S'_i = (T_i c_i + n_i N)(B + \bar{M}h(W)) \bmod q$ to calculate S'_i, but when it computes $g^{S'_i}$, the process is very difficulty. It is also difficult to solve n_i and c_i by $N_i = g^{n_i} \bmod p$ and $C_i = g^{c_i}$ under the DLP difficulty assumption. To sum up, the new scheme satisfies unforgeability. □

3) Non-repudiation. The original signature group cannot deny authorization to proxy signature group. The delegation proxy certificate (K, V) satisfies $C_i = g^{c_i}$. And $C_i = g^{c_i}$ refers to the private key information of all the original signers, so the original signature group cannot deny the authorization.

Proxy signature group cannot deny the signature of message M. In the proxy signature key generation phase, p_j only constructs the polynomial $f_j(x)$ satisfying $a_{j0} = (x_{p_j} + n_j V) modq$ with its own private key, and verifies the public key y_{p_j} of p_j. And then it verifies the validity of the final signature. Therefore, the proxy signature group cannot deny its proxy signature.

4) Traceability. When a dispute occurring, the identity of the T proxy signers who actually participate in the signature can be identified according to the uniqueness of the N in the final signature, that is, the scheme is traceable for the actual identity of the signer involved.

5) Robustness. This new scheme adds a threshold proxy process in the proxy signature generation phase. Only t proxy signers can complete the signature. Therefore, when the several proxy signers cannot participate in the signature, it will not affect the implementation of this scheme. Namely, the scheme has good robustness and fault tolerance.

6) Blindness. U_I first uses the randomly number α and β to blind M as $\bar{M}$. Then it sends B and $\bar{M}$ to the member p_i in E, and p_i wants to acquire message M through $\bar{M} = (\alpha^{-1}h(M||B') + \beta) \bmod q$, that is impossible. Therefore, each p_i in E cannot obtain the specific content of its signed message. So the scheme is with blindness.

7) Unlinkability. When U_I publishes the final signature of M, even if all p_i reserve intermediate variable B_i in each signature process and combine them to calculate B. By $B' = (\alpha B + \alpha\beta h(W)) \bmod q$ and $\bar{M} = (\alpha^{-1}h(M||B') + \beta) \bmod q$ to solve blind factor α and β. But α and β are randomly selected, p_i still does not know the final signature corresponding to which intermediate variables B_i, thereby p_i cannot combine the final signature with the detailed information of signature process. They are independent. So the scheme satisfies the unlinkability and effectively protect the privacy message.

8) Preventing the abuse of signature privilege. In W, it clearly stipulates the message range of proxy signature and the proxy valid period, this can prevent the proxy signer abuse of their proxy right. Because the proxy private key contains the original signer and proxy signer's private key, it only can be used for proxy signatures, which ensures that the proxy private key cannot be used for other purposes other than generating valid proxy signatures.

5.2 Proof of Correctness

Theorem 3. *If the original signer and proxy signer strictly generate the correct parameters according to (1) and (2), the formula (1) and (2) can be verified.*

Proof. $g^{V_{U_i}} = g^{h(W)x_{U_i} + k_{U_i}K} = y_{U_i}^{h(W)} L_{U_i}^{K} modp$, that is, the formula (1) can be verified, and the same for formula (2). The original signer and proxy signer are established by verifying (1), (2) to confirm the security of their personal delegate certificate and personal proxy certificate. □

6 Experiment And Analysis

We make comparison experiments to demonstrate the performance of our new scheme with MSBQ [6], EMRP [24], QPBW [25] and ECCB [20] with MATLAB 2014b platform. Supposing that bilinear pairings in this scheme is $e : G \times G \to G_T$. G_T is bilinear target group. Table 2

Table 2: Performance comparison with different schemes

Stage	MSBQ	EMRP	QPBW	ECCB	New scheme
Encryption	$p + 3e_T + 5h$	$2p + 2e_T + 4e + 2h$	$3p + 2e_T + 3e + 2h$	$4p + 3e + 2h$	$3e$
Deryption	$3p + 2e_T + 4h$	$p + 3e_T + 3e + h$	$2p + 2e_T + 3h$	$3p + 4e_T + 3h$	$2e$

Table 3: Comparison results with different methods

Scheme	Blind signature scheme	Muilt-proxy muilt-signature scheme	Security	Threshold signature scheme
MSBQ	NO	NO	YES	YES
EMRP	YES	NO	NO	NO
QPBW	YES	NO	NO	NO
ECCB	NO	YES	NO	YES
New scheme	YES	YES	YES	YES

is the computation complexity with different schemes. Where symbols p, e_T, e and h denote bilinear pairings operation, exponential operation in G_T, exponential operation in G and Hash operation. Their coefficients are operation numbers. From the table, we can know that our new scheme needs the least operation time. In addition, it has the optimal encryption results.

Table 3 is the comparison result with different methods in terms of qualitative analysis.

7 Conclusion

In this paper, we propose a discrete logarithm-based multi-proxy blind signature scheme in this paper. The new scheme combines Elliptic curve, bilinear mapping and blind signature. It can meet indistinguishable against adaptively chosen-ciphertext attacks in random oracle model. We also give security proof and efficiency analysis in this paper. And comparison with other proxy re-encryption schemes shows that our scheme is with high efficiency, more flexibility and fault tolerance. In the future, we will study more advanced re-encryption schemes taking communication cost between authorized user and proxy into consideration.

References

[1] F. D. Aranha, R. Dahab, J. Pez, *et al.*, "Efficient implementation of elliptic curve cryptography in wireless sensors," *Advances in Mathematics of Communications*, vol. 4, no. 2, pp. 169-187, 2017.

[2] W. C. Chang, H. F. Li and S. L. Yin, "Mixed symmetric key and elliptic curve encryption scheme used for password authentication and update under unstable network environment," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 3, pp. 632-639, May 2017.

[3] H. Chen, Q. Xue, F. Li, *et al.*, "Multi-proxy multi-signature binding positioning protocol," *Security & Communication Networks*, vol. 9, no. 16, pp. 3868-3879, 2016.

[4] L. Deng, H. Huang, Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229-235, 2017.

[5] X. Fu, X. Nie, F. Li, "Outsource the ciphertext decryption of inner product predicate encryption scheme based on prime order bilinear map," *International Journal of Network Security*, vol. 19, no. 2, pp. 313-322, 2017.

[6] W. Guo, Z. J. Zhang, P. Y. Li, *et al.*, "Multi-proxy strong blind quantum signature scheme," *International Journal of Theoretical Physics*, vol. 55, no. 8, pp. 3524-3536, 2016.

[7] M. S. Hwang, C. C. Lee, S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102–115, 2013.

[8] M. S. Hwang, Iuon-Chung Lin, Eric Jui-Lin Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers", *Informatica*, vol. 11, no. 2, pp. 1-8, Apr. 2000.

[9] M. S. Hwang, S. F. Tzeng and S. F. Chiou, "A non-repudiable multi-proxy multi-signature scheme", *Innovative Computing, Information and Control Express Letters*, vol. 3, no. 3, pp. 259–264, 2009.

[10] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[11] C. Lan, H. Li, S. Yin, *et al.*, "A new security cloud storage data encryption scheme based on identity proxy re-encryption," *International Journal of Network Security*, vol. 19, 2017.

[12] C. C. Lee, T. C. Lin, S. F. Tzeng and M. S. Hwang, "Generalization of proxy signature based on factorization", *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 3, pp. 1039–1054, 2011.

[13] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[14] C. Y. Liu, A. H. Wen, L. C. Lin, *et al.*, "Proxy-protected signature secure against the undelegated

proxy signature attack," *Computers & Electrical Engineering*, vol. 33, no. 3, pp. 177-185, 2007.

[15] J. Liu, S. L. Yin, H. Li and L. Teng, " A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[16] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[17] C. Ma, K. Xue, P. Hong, "A proxy signature-based re-authentication scheme for secure fast handoff in wireless mesh networks," *International Journal of Network Security*, vol. 15, no. 2, pp. 122-132, 2013.

[18] G. Pointcheval, "Anonymous proxy signatures," *International Conference on Security and Cryptography for Networks, Springer Berlin Heidelberg*, pp. 201-217, 2008.

[19] A. R. Sahu, S. Padhye, "Provable secure identity-based multi-proxy signature scheme," *International Journal of Communication Systems*, vol. 28, no. 3, pp. 497-512, 2015.

[20] N. Tahat, E. E. Abdallah, "A proxy partially blind signature approach using elliptic curve cryptosystem," *International Journal of Mathematics in Operational Research*, vol. 8, no. 1, 87, 2017.

[21] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[22] S. F. Tzeng, M. S. Hwang, C. Y. Yang, "An improvement of nonrepudiable threshold proxy signature scheme with known signers", *Computers & Security*, vol. 23, no. 2, pp. 174-178, Apr. 2004.

[23] S. F. Tzeng, C. C. Lee, and M. S. Hwang, "A batch verification for multiple proxy signature", *Parallel Processing Letters*, vol. 21, no. 1, pp. 77–84, 2011.

[24] K. G. Verma, B. B. Singh, "Efficient message recovery proxy blind signature scheme from pairings," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 11, 2017.

[25] H. Wang, R. Shi, H. Zhong, *et al.*, "Quantum proxy blind signature based on W state," *Chinese Journal of Quantum Electronics*, 2016.

[26] Q. Xie, Y. X. Yu, "Cryptanalysis of two nonrepudiable threshold proxy signature schemes," *International Journal of Network Security*, vol. 3, no. 1, pp. 18-22, 2006.

[27] L. Yi, G. Bai, G. Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme," *Electronics Letters*, vol. 36, no. 6, pp. 527-528, 2000.

[28] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.

[29] S. L. Yin, H. Li, J. Liu, "A new provable secure certificateless aggregate signcryption scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, 2016.

Biography

Hang Li obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:1451541@qq.com.

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016. Now, she is a laboratory assistant in Software College, Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. Email:ysl352720214@163.com.

An Improved AES S-box Based on Fibonacci Numbers and Prime Factor

Kamsiah Mohamed[1], Fakariah Hani Hj Mohd Ali[1], Suriyani Ariffin[1], Nur Hafiza Zakaria[2] and Mohd Nazran Mohammed Pauzi[3]

(Corresponding author: Kamsiah Mohamed)

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA[1]
40450 Shah Alam,Selangor, Malaysia
Faculty of Science and Technology, University Sains Islam Malaysia[2]
71800 Nilai, Negeri Sembilan, Malaysia
Faculty of Engineering and Life Sciences, Universiti Selangor[3]
45600, Bestari Jaya, Selangor, Malaysia
(Email: kamsh@unisel.edu.my)

(Received Aug. 28, 2017; revised and accepted Dec. 18, 2017)

Abstract

This paper emphasises the study on ways of constructing the substitution boxes (S-boxes). To improve the strength of block cipher, a new proposed substitution box for symmetric key cryptography was designed based on Fibonacci numbers and prime factor. This new security approach was designed for better security of block ciphers. The level of security S-box was evaluated based on the cryptographic properties such as balance criteria, nonlinearity, correlation immunity, algebraic degree, transparency order, propagation, number of fixed points and opposite fixed points, algebraic immunity, robustness to differential cryptanalysis, signal to noise ratio (SNR) Differential Power Analysis (DPA) as well as confusion coefficient. The AES S-box and the new proposed S-box were analysed to verify the cryptographical security of the S-box. Result showed that the new proposed S-box using the Fibonacci numbers and prime factor possessed good cryptographic properties compared to the AES S-box.

Keywords: Block Cipher; Cryptography; Fibonacci; S-box

1 Introduction

Cryptography is an important part of information security that covers the investigation of algorithms and protocols for secure information. Within the advancement of technology, the design of cryptographic algorithm is often enhanced to ensure that information is secure. In terms of security, it is always a question of whether or not these algorithms are secure enough to protect information. Block ciphers are the most prominent and important elements to provide high level security. Generally, block cipher is a deterministic algorithm on fixed length group of bits known as blocks to transform a fixed length block of plaintext message blocks into cipher text blocks of the same length. Since 1970, block cipher design and analysis have been widely studied culminating in the selection of Rijndael [8] as the new Advanced Encryption Standard (AES) in 2001 [5]. Thus, a modern block cipher was designed based on the AES substitution box (called S-box) to substitute blocks of input bits to a set of output bits. S-box is a critical part of any block cipher that provides the primary source non-linear [12, 16].

This paper proposes a design of secure symmetric encryption S-box to improve the existing S-box. The design and characteristics of S-box in a block cipher are the central measures of resistance against all adequately high nonlinearities [9]. The confusion and diffusion properties are needed to build a strong encryption algorithm as suggested by [37]. However, there are some problems addressed in the process of the designing of a new S-box. The two sets of problems arise from the selection of an S-box before its cryptographic use can be considered secure. The first problem is related to the design (or search) of a good S-box while the second problem is in the verification of a given S-box as one cryptanalytic technique [2]. Hence, constructing secure S-boxes to use them in different cryptosystems for increasing their security is the current study problem [17]. S-box design is usually the most important task while designing a new cipher [7].

The design of the new S-box is an important concern in creating new and more secure cryptosystems [11]. The disadvantages of S-box design are the limitations that make it vulnerable and insecure [1, 18]. Currently, there are no algebraic procedures that can give the preferred and complete set of properties for an S-box [33]. Thus, there has been a lot of attention on redesigning, recre-

ating or renewing the design and implementation of the original AES S-box.

Based on previous studies, there are various techniques used to construct the standard AES S-box such as linear-transform and non-linear function [39], fractional linear transformation [19], branch numbers [36], affine transformation [6, 41] and the network RFWKIDEA32-1 [26]. In another study, it was shown that Fibonacci number can make secure communication from cryptanalysis attacks [35]. This technique can fulfil the requirements for communication such as capacity, security and robustness to secure data transmission over an open channel. Recent studies proved that the performance of encryption and decryption algorithm using Fibonacci number is faster than symmetric algorithms [38] and RSA algorithms [14]. These studies demonstrated that the performance of encryption and decryption algorithm can be increased using Fibonacci numbers. However, no study has addressed Fibonacci technique and prime factor to construct the AES S-box. In this paper, Fibonacci numbers and prime factor were used to improve the original AES S-box.

This paper is organized as follows: In Section 2, previous studies on Fibonacci numbers are reviewed. Section 3 briefly describes the AES S-box in cryptography, the Fibonacci numbers and prime factor. Comparison between the properties of Boolean functions of our new proposed S-box and the AES S-box is explained in Section 4. Finally, conclusion is presented in Section 5.

2 Review on Fibonacci Numbers

In the field of cryptography, numbers play an important role in different theoretical and practical applications. Cryptosystems rely on the assumption that a number of mathematical problems are computationally intractable since they cannot be solved in polynomial time [29]. The Fibonacci numbers are natural numbering system appropriate for the development of each living thing. Many studies have investigated on how Fibonacci sequence can be observed in the real world. These numbers occur everywhere in nature, ranging from the leaf arrangement in plants, the structure of DNA as well as various proportions in human face and structure of sea shells. One study has been conducted observing that the phyllotaxis of plants follows the Fibonacci sequence [28].

A study by [23] showed that the structure of DNA and its organization pattern is a fractal. Then, [31] discovered that the DNA gene-coding region sequences are strongly related to the Golden Ratio and Fibonacci/Lucas integer numbers. In another study, [3] examined the Fibonacci numbers can be seen in the structure of coronary arterial tree and that diseased atherosclerotic lesions in coronary arteries follow the Fibonacci distribution. Nevertheless, in computer science, the Fibonacci numbers act as a foundation for various algorithms that are widely applied. In a previous study, the Fibonacci numbers have been applied in the encryption and decryption algorithm to display encrypting message.

In another study [34], it was shown that the content of the original message were changed to the ciphertext by taking each character from the message and converting it based on the Fibonacci numbers. Based on these previous studies, understanding the role of the Fibonacci numbers may be a key to increase the performance of block cipher in cryptosystems.

3 AES S-box in Cryptography

Substitution is a nonlinear transformation that makes the confusion of bits. It is often considered as a look-up table, which uses several byte substitution transformations in the key expansion routine to perform a one-for-one substitution of a byte value. An $n \times m$ S-box is a mapping from n input bits to m output bits, $S : \{0,1\}^n \rightarrow \{0,1\}^m$. Basically, an S-box is a set of m single output Boolean functions combined in a fixed order. There are 2^n inputs and 2^m possible outputs for an $n \times m$ S-box. Generally, an $n \times m$ S-box, S, is represented as a matrix of size $2^{n \times m}$ for each m-bit entry. An $n \times m$ S-box is a bijective S-box where each input is mapped to a dissimilar output entry and all possible outputs are presented in the S-box.

In 2001, the National Institute of Standards and Technology (NIST) announced the AES as a new standard to replace the Data Encryption Standard (DES). This standard indicates that the Rijndael algorithm is generally utilized as a part of numerous cryptographic applications. It was designed to handle additional block sizes and key lengths 128, 192 and 256 bits. The 128 bits AES encrypted a 16 byte block using a 16 byte key of 10 encryption rounds. The value of each byte in the array is substituted according to a look-up table.

The Rijndael AES S-box is designed based on three transformations. The S-box is generated by determining multiplicative inverse for a given number in Galois Field GF(2^8) using the irreducible polynomial:

$$m(x) = x^8 + x^4 + x^3 + x^1.$$

The multiplicative inverse is then transformed as in Equation (1):

$$x'_i = x_i \oplus x_{(i+4)mod8} \oplus x_{(i+5)mod8} \oplus x_{(i+7)mod8} \oplus C_i. \quad (1)$$

Where x_i is the bit i of the byte and the column vector C_i is added with the value {63} or {01100011}. The affine transformation element of the Rijndael AES S-box can be expressed as shown in Figure 1.

This affine transformation is the sum of multiple rotations of the byte as a vector. Figure 2 shows the original AES S-box represented here with hexadecimal notation.

3.1 Construct AES S-box Using Fibonacci Numbers and Prime Factor

In this paper, the Fibonacci numbers and prime factor were applied to construct the AES S-box to propose a new S-box.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 1: Affine transformation of Rijndael AES S-box

AES S-BOX

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
01	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
02	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
03	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
04	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
05	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
06	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
07	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
08	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
09	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
0A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
0B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
0C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
0D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
0E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
0F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

INVERSE AES S-BOX

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
01	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
02	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
03	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
04	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
05	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
06	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
07	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
08	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
09	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
0A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
0B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
0C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
0D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
0E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
0F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure 2: The AES S-box

3.2 Fibonacci Numbers

In mathematics, the Fibonacci numbers or Fibonacci sequences are the numbers in the integer sequence of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610.... Based on the definition, the first two numbers in the Fibonacci sequence are 0 and 1, and each subsequent number is the sum of the previous two. In mathematical terms, the sequence F_n in Fibonacci numbers is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}. \tag{2}$$

With seed values

$$F_0 = 0, F_1 = 1. \tag{3}$$

The Fibonacci numbers were applied because they have a wide range of significant mathematical properties that make them very useful in computer science. Moreover, the Fibonacci numbers are efficiently computable. Based on this fact, the series can be generated efficiently. Any number can be written as the sum of unique Fibonacci numbers. The straightforwardness and beauty of Fibonacci numbers are persuaded to create matrix cryptosystems, which are helpful in securing information.

3.3 Prime Factor

The prime factor is the most remarkable and practical for cryptography. Many algorithms used in public-key cryptography contain various and critical security applications. Most of them are related to the fact that prime factorisation is unique. Prime factorisation is the finding of prime numbers that can be multiply together to make the original number. In a number of theories, prime factor is a positive integer where the prime numbers divide that integer exactly. For a prime factor p of n, the multiplicity of p is the largest exponent a for which pa divides n precisely. In this paper, the AES S-box was improved with the Fibonacci numbers and prime factor to make a strong and secure S-box against cryptanalysis attack.

The new proposed S-box was constructed by the following steps:

1) The multiplicative inverse in the finite field GF(2^8) was taken and the element {00} was mapped to itself.

2) The affine transformation was applied (over GF(2^8)).

3) Each byte in the S-box was assumed to comprise 8 bits labelled $[x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0]$.

4) XOR with the value {63} or {01100011} which is a byte of C_i.

5) Then XOR with the Fibonacci number.

6) XOR with the prime factor.

NEW S-BOX

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	45	4E	42	CB	52	56	FC	09	38	5E	12	C7	EE	92	4F
01	F3	BB	F0	44	C3	60	7E	C9	94	ED	9B	96	A5	9D	4B	F9
02	8E	C4	AA	1F	0F	06	CE	F5	0D	9C	DC	C8	48	E1	08	2C
03	3D	FE	1A	FA	21	AF	3C	A3	3E	2B	B9	DB	D2	1E	8B	4C
04	30	BA	15	23	22	57	63	99	6B	02	EF	8A	10	DA	16	BD
05	6A	E8	39	D4	19	C5	88	62	53	F2	87	00	73	75	61	F6
06	E9	D6	93	C2	7A	74	0A	BC	7C	C0	3B	46	69	05	A6	91
07	68	9A	79	B6	AB	A4	01	CC	85	8F	E3	18	29	C6	CA	EB
08	F4	35	2A	D5	66	AE	7D	2E	FD	9E	47	04	5D	64	20	4A
09	59	B8	76	E5	1B	13	A9	B1	7F	D7	81	2D	E7	67	32	E2
0A	D9	0B	03	33	70	3F	1D	65	FB	EA	95	5B	A8	AC	DD	40
0B	DE	F1	0E	54	B4	EC	77	90	55	6F	CD	D3	5C	43	97	31
0C	83	41	1C	17	25	9F	8D	FF	D1	E4	4D	26	72	84	B2	B3
0D	49	07	8C	5F	71	3A	CF	37	58	0C	6E	80	BF	F8	24	A7
0E	D8	C1	A1	28	50	E0	B7	AD	A2	27	BE	D0	F7	6C	11	E6
0F	B5	98	B0	34	86	DF	7B	51	78	A0	14	36	89	6D	82	2F

INVERSE S-BOX

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	5B	76	49	A2	8B	6D	25	D1	2E	08	66	A1	D9	28	B2	24
01	4C	EE	0B	95	FA	42	4E	C3	7B	54	32	94	C2	A6	3D	23
02	8E	34	44	43	DE	C4	CB	E9	E3	7C	82	39	2F	9B	87	FF
03	40	BF	9E	A3	F3	81	FB	D7	09	52	D5	6A	36	30	38	A5
04	AF	C1	03	BD	13	01	6B	8A	2C	D0	8F	1E	3F	CA	02	0F
05	E4	F7	05	58	B3	B8	06	45	D8	90	00	AB	BC	8C	0A	D3
06	15	5E	57	46	8D	A7	84	9D	70	6C	50	48	ED	FD	DA	B9
07	A4	D4	CC	5C	65	5D	92	B6	F8	72	64	F6	68	86	16	98
08	DB	9A	FE	C0	CD	78	F4	5A	56	FC	4B	3E	D2	C6	20	79
09	B7	6F	0E	62	18	AA	1B	BE	F1	47	71	1A	29	1D	89	C5
0A	F9	E2	E8	37	75	1C	6E	DF	AC	96	22	74	AD	E7	85	35
0B	F2	97	CE	CF	B4	F0	73	E6	91	3A	41	11	67	4F	EA	DC
0C	69	E1	63	14	21	55	7D	0C	2B	17	7E	04	77	BA	26	D6
0D	EB	C8	3C	BB	53	83	61	99	E0	A0	4D	3B	2A	AE	B0	F5
0E	E5	2D	9F	7A	C9	93	EF	9C	51	60	A9	7F	B5	19	0D	4A
0F	12	B1	59	10	80	27	5F	EC	DD	1F	33	A8	07	88	31	C7

Figure 3: Proposed S-box

The new equation of the Fibonacci numbers and prime factor is expressed as below.

$$x'_i = x_i \oplus x_{(i+4)mod8} \oplus x_{(i+5)mod8} \oplus x_{(i+7)mod8} \oplus C_i \oplus F_n \oplus P_i^{a_1}. \quad (4)$$

Based on the Equation (4), the proposed S-box generated is illustrated in Figure 3.

4 Analysis of S-boxes Properties

To ensure that the newly proposed S-box is secure, cryptographic tests were applied. In this paper, the AES S-box and the new proposed S-box were analysed using the S-box Evaluation Tool (SET). The SET is a tool utilised for analysing cryptographic properties of Boolean functions and S-boxes composing ANSI C code [32]. The quality of an S-box is determined based on cryptographic properties that must be considered in the designing and analysing of S-boxes.

The experiments were conducted on Ubuntu 16.04LTS operating system to test the cryptographic properties of S-boxes, which are balance criteria, nonlinearity, correlation immunity, algebraic degree, transparency order, propagation, number of fixed points and opposite fixed points, algebraic immunity, robustness to differential cryptanalysis, signal to noise ratio (SNR) Differential Power Analysis as well as confusion coefficient. Each property of S-boxes relates to a certain cryptographic attack.The results from the AES S-box and the new proposed S-box are depicted in Figure 4 and Figure 5.

Meanwhile, the explanation for the cryptographic properties of S-box is described as follows:

Balance: The most fundamental of all cryptographic properties desired to be presented by Boolean function is balance. For an $n \times m$, S-box is mapped from $GF(2^n)$ to $GF(2^m)$. If every value $\in GF(2^m)$ is mapped by an equal number of distinct input values, then the S-box is balanced. On the other hand, if an n-variable Boolean function whose Hamming weight is not equal to 2^{n-1}, it is called an unbalanced function [17].

Nonlinearity: One of the most important cryptographic properties of a Boolean function is nonlinearity. In fact, the nonlinearity of a n-variable Boolean function f represents a measure of the dissimilarity between f and the n-variable affine function a that f bears the closest bitwise similarity to be measured by the Hamming distance between f and a. $S : \{0,1\}^n \rightarrow \{0,1\}^m$ is defined as the least value of nonlinearity of all nonzero linear combination of n Boolean functions $f_i : \{0,1\} \rightarrow \{0,1\}, i = n-1, ?1, 0$ [17]. The nonlinearity of an S-box must be high to resist linear cryptanalysis. Without a nonlinear component, an attacker could express the input and output with a system of linear equations where the key bits are unknown.

The strength of S-box can be evaluated based on the nonlinearity criteria where the high nonlinearity is considered as cryptographically strong. Highly nonlinear functions were stimulated since algorithms close to linear are vulnerable to various approximation attacks [10]. The available limit of nonlinearity for 8×8 S-boxes is 100 [27].

An optimal value of nonlinearity is 120 [20]. Hence, the analysis of the nonlinearity must be high to resist linear cryptanalysis. Thus, the highest possible value of NL is $120 \leq NL \leq 100$.

Correlation Immunity: Correlation immunity is a property of Boolean functions that denotes the extent of independence between linear combinations of the in-

put bits and the output. An n-variable Boolean function, $f(x)$, which is mth-order correlation immune, is denoted $CL(m)$ if it is statistically independent of the subset of m input variables where $1 \leq m \leq n$. An n-variable boolean function, $f(x)$, which is mth-order correlation immune, is denoted by $CL(m)$, if, for every ω such that $1 \leq HW(\omega) \leq m, \hat{F}(\omega) = 0$. Thus, the higher the order of correlation immunity m, the more positions in $\hat{F}(\omega)$ must have the values of zero [40].

Algebraic Degree: The S-boxes should be the algebraic functions of higher degree to resist higher order differential attacks [22]. The algebraic degree of an S-box (similarly, a Boolean function) is desired to be as high as possible to resist a cryptanalytic attack known as lower order approximation [42].

Algebraic Immunity: Boolean functions with high algebraic immunity (AI) are vital to reduce the possibility of utilising algebraic attacks in breaking an encryption system. The algebraic immunity of an S-box depends on the number and type of linearly independent multivariate equations it satisfies [30].

Transparency Order: Transparency order is proposed as a parameter for the robustness of S-boxes to Differential Power Analysis (DPA): lower transparency order denoting more resistance. However, most cryptographically strong Boolean functions have been found to have high transparency order [24]. Also to prevent DPA attacks, transparency order of the S-box should be as low as possible.

Propagation Characteristic: An n-variable Boolean function $f(\bar{x})$ satisfies the propagation characteristics of degree k if $f(\bar{x})$ changes with a probability of half when $i, (1 \leq i \leq k)$ bits of $f(\bar{x})$ are complemented. Propagation characteristic is a Boolean function property that enables a function to achieve good diffusion by ensuring output uniformity [15,17].

Fixed(Fp)and Opposite Fixed Points(OFp): For an $n \times m$ S-box, a fixed point is defined as $f(x) = x$ where if an input x is given, the output is also x. An opposite fixed point is defined as $f(x) = \bar{x}$, where $\bar{x}$ denotes the bitwise complement of x. The number of Fp and OFp should be kept as low as possible to avoid leakage in any statistical cryptanalysis [21].

Robustness to Differential Cryptanalysis: Let $F = (f_1, f_2, ..., f_n)$ be an $n \times m$ S-box where f_i is a component function of S-box mapping $f_i = \{0,1\}^n \rightarrow \{0,1\}^m$. F is said to be robust against differential cryptanalysis [25].

Signal to Noise Ratio (SNR) Differential Power Analysis: The SNR of the DPA signal increases with the resistance against linear or differential cryptanalysis. When the SNR is bounded, the lower bound is reached by the poorest cryptographic S-boxes namely affine S-boxes. High quality cryptographic S-boxes are evaluated based on high SNR, which is close to the maximum bound [15]. A higher SNR values mean that the signal strength is stronger in relation to the noise levels.

Confusion Coefficient: The confusion coefficient property was defined with the intention to characterise the resistance of an S-box. Recently, [13] introduced confusion coefficient as a new property that relates to the DPA resistance of S-boxes. A high confusion coefficient indicates that the S-box output is very distinctive. Table 1 shows the comparison between the proposed S-box and the standard AES S-box. Based on the balance properties, findings suggest that both S-boxes are balanced. There is no exploitable bias where an attacker is unable to trivially approximate the functions or the output. In particular, a large imbalance may enable the Boolean function to be easily approximated by a constant function.

The confusion in a cipher system is measured through the nonlinear properties. Thus, the results indicate that the nonlinearity value of the standard AES S-box and the proposed S-box is high, achieving the optimal value to resist linear cryptanalysis attack. For correlation immunity, the results show that the AES S-box and the proposed S-box are zero independence between linear combinations of the input bits and the output. Meanwhile, the result for the algebraic degree properties shows that the proposed S-box has achieved high algebraic degree compared to the AES S - box. The AES S-box showed an algebraic degree 7, whereas the proposed S-box displayed an algebraic degree 8. Therefore, the proposed S-box will be more difficult to be attacked by algebraic attacks or higher-order differential cryptanalysis.

For algebraic immunity, the results demonstrated that the AES S-box and the proposed S-box is 4, which indicate that both S-boxes are secure from algebraic attack. For the transparency order properties, the proposed S-box was found to be smaller than the AES S-box, which means that the proposed S-box has better DPA resistance compared to the AES S-box. For propagation characteristic, the comparison of the PC(k) was satisfied by both S-boxes. While for the number of Fixed Points (Fp) and Opposite Fixed Points (OFp), the results showed that both S-boxes were satisfied. For robustness to differential cryptanalysis, the proposed S-box was seen to have higher resistance to DPA attacks than the AES S-box. The SNR (DPA) valued of the proposed S-box (9.8) was higher than the AES S-box (9.6). Thus, the proposed S-box has better resistance to DPA attacks in terms of SNR (DPA).

The last cryptographic property is confusion coefficient. From the results, the proposed S-box has a confusion coefficient variance of 0.1016 compared to the AES S-box, which is 0.1113. Hence, it was seen that the proposed S-box indicated a low confusion coefficient value to

```
Enter input dimension M
8
Enter output dimension N
8

Enter filename
File must be *.txt where values are tab separated.
Program assumes that the values are in lexicographical order.
./Aes1.txt

Calculations took 2848.12 miliseconds to run

Name of the file: ./Aes1.txt
Input size M is 8
Output size N is 8
S-box is balanced.
Nonlinearity is 112.
Corelation immunity is 0.
Absolute indicator is 32.
Sum of square indicator is 133120.
Algebraic degree is 7.
Algebraic immunity is 4.
Transparency order is 7.860.
Propagation characteristic is 0.
Strict Avalanche Criterion is not satisfied.
Number of fixed points is 0.
Number of opposite fixed points is 0.
Composite algebraic immunity is 4.
Robustness to differential cryptanalysis is 0.984.
Delta uniformity is 4.
SNR (DPA) (F) is 9.600.
Confusion coefficient variance is 0.111304.
```

Figure 4: Result for AES S-box

```
Enter input dimension M
8
Enter output dimension N
8

Enter filename
File must be *.txt where values are tab separated.
Program assumes that the values are in lexicographical order.
./NewSBox1.txt

Calculations took 2665.52 miliseconds to run

Name of the file: ./NewSBox1.txt
Input size M is 8
Output size N is 8
S-box is balanced.
Nonlinearity is 112.
Corelation immunity is 0.
Absolute indicator is 32.
Sum of square indicator is 133120.
Algebraic degree is 8.
Algebraic immunity is 4.
Transparency order is 7.859.
Propagation characteristic is 0.
Strict Avalanche Criterion is not satisfied.
Number of fixed points is 1.
Number of opposite fixed points is 0.
Composite algebraic immunity is 4.
Robustness to differential cryptanalysis is 0.981.
Delta uniformity is 4.
SNR (DPA) (F) is 9.887.
Confusion coefficient variance is 0.101562.
```

Figure 5: Result for the proposed S-box

make it harder for the side-channel attacks to attack the S-box.

As a conclusion, the proposed S-box has good cryptographic properties for algebraic degree, transparency order, robustness to differential cryptanalysis, SNR(DPA) and confusion coefficient than the AES S-box. Besides, the result of balance = 0, nonlinearity = 112, correlation immunity = 0, and algebraic immunity = 4 is similar to AES S-box.

According to [40], if an S-box satisfies these cryptographic properties, the S-box can be considered cryptographically secure. Therefore, it is important for every S-box to be evaluated based on cryptographic properties to resist linear attack, differential attack, algebraic attack and side channel attack.

5 Conclusions

In this paper, a new way to enhance the AES S-box has been explored using the Fibonacci numbers and prime factor approach to increase the security of S-box in a block cipher. The results showed that the values of several cryptography properties of the proposed S-box are similar with that of the existing S-box such as balance, nonlinearity, correlation immunity, algebraic immunity and propagation characteristic. Hence, the proposed S-box inherits all good cryptographic characteristics of the standard AES S-box. From the result, it was observed that the proposed S-box has a high algebraic degree, low transparency order, low robustness to differential cryptanalysis, high signal to noise ratio (SNR) differential power analysis and high confusion coefficient compared to the standard AES S-box. The experiments have shown that the new proposed S-box fulfilled the confusion and diffusion properties as described by [37].

The experimental results indicate that the proposed S-box has a high quality of cryptography properties. Therefore, the Fibonacci numbers and prime factor have made the proposed S-box to have more resistant to linear cryptanalysis attacks and differential cryptanalysis. As a result, this approach had increased the security level of S-box to achieve high quality cryptography properties. Future studies can be done by demonstrating of cache-timing attacks against the proposed S ?box as introduced by [4].

Timing attack is a type of side-channel attacks that allows an attacker to extract information based on the time taken to execute cryptographic algorithms. Since cryptographic systems generally work on the keys, hence, side-channel attacks have been developed to break a system. The size of the proposed S - box was analysed to see whether or not it leaks timing information during cache hits to determine its immunity against cache-timing attacks.

Table 1: Comparison of cryptographic properties between the AES S-box and the proposed S-box

Cryptographic Properties	**AES S-Box**	**Proposed S-Box**	**Range of Value (Parameter n)**	**Good Cryptographic Properties**
Balance	0	0	$n = 0$	No Exploitable Bias
Nonlinearity	112	112	$120 \geq n \geq 100$	High
Correlation Immunity	0	0	$n \leq 0$	Low
Algebraic Degree	7	8	$n \geq 10$	High
Algebraic Immunity	4	4	$n \leq 4$	Low
Transparency Order	7.860	7.859	$n < 7.8$	Low
Propagation Characteristic	0	0	$n \leq 0$	Low
Fixed (Fp) and Opposite Fixed points (OFp)	0,0	1,0	$n \leq 4$	Low
Robustness to Differential Cryptanalysis	0.984	0.981	$n < 0.98$	Low
Signal to Noise Ratio (SNR) Differential Power Analysis	9.600	9.887	$n > 0.98$	High
Confusion Coefficient	0.111	0.101	$n \leq 0$	Low

Acknowledgments

This research was supported by the Institute of Research Management and Innovation, Universiti Teknologi MARA (UiTM), Malaysia and registered under the research grant 600-IRMI/FRGS 5/3 (017/2017) by the Ministry of Education Malaysia. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *Journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[2] N. Ahmed, "Testing an S-box for cryptographic use," *International Journal of Computer and Electrical Engineering*, pp. 1–5.

[3] H. Ashrafian and T. Athanasiou, "Fibonacci series and coronary anatomy," *Heart, Lung and Circulation*, vol. 20, no. 7, pp. 483–484, 2011.

[4] D. J. Bernstein, "Cache-timing attacks on AES", 2005.

[5] C. Cid and R. Weinmann, *Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases. In Gröbner Bases, Coding, and Cryptography*, 2009.

[6] J. Cui, L. Huang, H. Zhong, C. Chang and W. Yang, "An Improved AES S-box and Its Performance Analysis," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 5, pp. 2291–2302, 2011.

[7] A. G. Czurylo, "Cryptographic Properties of Modified AES-like S-boxes," *Annales Universitatis Mariae Curie-Sklodowska Informatica*, vol. 11, no. 2, pp. 37–48, 2011.

[8] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*, 2013.

[9] A. Datta, D. Bhowmik and S. Sinha, "A Novel Technique for Analysing Confusion in S-boxes," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 11608–11615, 2016.

[10] O. Dunkelman and N. Keller, "A New Criterion for Nonlinearity of Block Ciphers," in *Cryptographers Track at the RSA Conference*, pp. 295–312, 2006.

[11] M. H. Dawson and S. E Tavares, "An Expanded Set of S-box Design Criteria Based on Information Theory and Its Relation to Differential-like Attacks," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 352–367, 1991.

[12] C. Easttom, *Creating Cryptographic S-Boxes: A Guideline for Designing Cryptographic S-boxes*, Feb. 25, 2018. (`https://pdfs.semanticscholar.org/7ae7/bcad617a7106afabc0ee7f29b16b6cadcb22.pdf`)

[13] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A Statistics-based Fundamental Model for Side-channel Attack Analysis," *IACR Cryptology ePrint Archive*, vol. 2014, pp. 152, 2014.

[14] N. G. Gonsalves, N. G. Bhat and K. K Tangod, "Performance Analysis of Secured Communication With Cryptography Using Fibonacci Series," *International Journal of Innovations In Engineering Research And Technology (IJIERT'17)*, vol. 4, no. 6, 2017.

[15] S. Guilley, P.E. Hoogvorst and R. Pacalet, "Differential power analysis model and some results," *Smart Card Research and Advanced Applications VI*, pp. 127–142, 2004.

[16] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4,"

International Journal of Electronics and Information Engineering, vol. 6, no. 2, pp. 59-71, 2017.

[17] I. Hussain and T. Shah, *Literature Survey on Nonlinear Components and Chaotic Nonlinear Components of Block Ciphers*, Dordrecht: Springer Science & Business Media, 2013.

[18] I. Hussain, T. Shah, M. Afzal and H. Mahmood, "Comparative analysis of S-boxes based on graphical SAC," *International Journal of Computer Applications*, vol. 2, no. 5, 2010.

[19] I. Hussain, T. Shah, M. A. Gondal and W. A. Khan, "Construction of Cryptographically Strong 8× 8 S-boxes," *World Applied Sciences Journal*, vol. 13, no. 11, pp. 2389–2395, 2011.

[20] I. Hussain, T. Shah, H. Mahmood and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Computing and Applications*, vol. 22, no. 6, pp. 1085–1093, 2013.

[21] H. Isa, N. Jamil and M. R. Z'aba, "S-box construction from non-permutation power functions," in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 46–53, 2013.

[22] L. R. Knudsen, "Truncated and Higher Order Differentials," in *International Workshop on Fast Software Encryption*, pp. 196–211, 1994.

[23] B. B. Mandelbrot, "The Fractal Geometry of Nature," *WH Freeman and Company New York, USA*, 1982.

[24] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, "Constrained Search for a Class of Good S-boxes with Improved DPA Resistivity," *IACR Cryptology ePrint Archive*.

[25] B. Mazumdar, D. Mukhopadhyay and I. Sengupta, "Design for security of block cipher S-boxes to resist differential power attacks," in *25th International Conference on VLSI Design (VLSID'12)*, pp. 113–118, 2012.

[26] A. Mersaid and T. Gulom, "The Encryption Algorithm AES-RFWKIDEA32-1 Based on Network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1–11, 2016.

[27] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in *Australasian Conference on Information Security and Privacy*, pp. 181–192, 1998.

[28] G. J. Mitchison, "Phyllotaxis and the Fibonacci Series," *Science*, vol. 196, no. 4287, pp. 270–275, 1977.

[29] M. H. Mohamed, Y. B. Mahdy and W. A. E. Shaban, "Confidential Algorithm for Golden Cryptography Using Haar Wavelet," in *International Journal of Computer Science and Information Security (IJCSIS'15)*, 2015.

[30] Y. Nawaz, K. C. Gupta, and G. Gong, "Algebraic immunity of S-boxes based on power mappings: analysis and construction," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4263–4273, 2009.

[31] J. C. Perez, "Chaos, DNA and Neuro-computers: A golden link: The hidden language of genes, global language and order in the human genome," *Speculations in Science and Technology*, vol. 14, no. 4, pp. 339–346, 1991.

[32] S. Picek, L. Batina, D. Jakobović, B. Ege and M. Golub, "S-box, SET, Match: A Toolbox for S-box Analysis," in *Workshop on Information Security Theory and Practice (WISTP)*, pp. 140–149, 2014.

[33] S. Picek, B. Ege, L. Batina, D.J. Jakobovic, L. Chmielewski and M. Golub, "On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box," in *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*, pp. 13–18, 2014.

[34] A. Q. Quazi, P. G. Maddikar and K. K Tangod, "A Survey on Secure E-mailing System with Cryptography Using Fibonacci Series," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 5, pp. 9911–9915, 2017.

[35] A. J. Raphael and V. Sundaram, "Secured Communication through Fibonacci Numbers and Unicode Symbols," *International Journal of Scientific & Engineering Research*, vol. 3, no. 4, pp. 2229–5518, 2012.

[36] P. C. Ruisanchez, "A New Algorithm to Construct S-boxes with High Diffusion," *International Journal of Soft Computing, Mathematics and Control (IJSCMC)*, vol. 4, no. 3, 2015.

[37] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[38] B. S. Tarle and G. L. Prajapati, "On The Information Security Using Fibonacci Series," in *Proceedings of the International Conference and & Workshop on Emerging Trends in Technology (ICWET'11)*, pp. 791–797, 2011.

[39] B. N. Tran, T. D. Nguyen and T. D. Tran, "A New S-box Structure to Increase Complexity of Algebraic Expression for Block Cipher Cryptosystems," in *International Conference on Computer Technology and Development(ICCTD'09)*, vol. 2, pp. 212–216, 2009.

[40] G. Z. Xiao and J. L. Massey, "A Spectral Characterization of Correlation-immune Combining Functions," *IEEE Transactions on information Theory*, vol. 34, no. 3, pp. 569–571, 1988.

[41] N. H. Zakaria, R. Mahmod, N. I. Udzir and Z. A. Zukarnain, "Enhancing Advanced Encryption Standard (AES) S-box Generation Using Affine Transformation," *Journal of Theoretical & Applied Information Technology*, vol. 72, no. 1, 2015.

[42] Y. Zheng and X. M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," in *Selected Areas in Cryptography (SAC'00)*, vol. 2012, pp. 262–274, 2000.

Biography

Kamsiah Mohamed received her Master degree in Software Engineering from Universiti Putra Malaysia (UPM). She is currently a Ph.D. candidate in Computer Science at Universiti Teknologi MARA (UiTM), Malaysia. Her research interest is Cryptography.

Fakariah Hani Hj Mohd Ali is a senior lecturer in the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Malaysia. She received her PhD degree in Network Security from the University Putra Malaysia (UPM). Her research interest includes Cryptography, Network Security and Big Data.

Suriyani Ariffin is a senior lecturer in the Faculty of Computer and Mathematical Sciences (UiTM), Malaysia. She received her PhD degree in Network Security from Universiti Putra Malaysia (UPM). Her research interest includes Cryptography and Network Security.

Nur Hafiza Zakaria is a lecturer in the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM). She received her PhD degree in Security in Computing from the Universiti Putra Malaysia (UPM). Her research interest includes Cryptography and Computer Security.

Mohd Nazran Mohammed Pauzi is a lecturer in the Faculty of Engineering and Life Sciences, Universiti Selangor (UNISEL), Malaysia. He is currently a Ph.D. candidate in Mathematics at Universiti Kebangsaan Malaysia (UKM). His research interest is Cryptography and Complex Analysis.

Research on the Security Protection of E-Commerce Information under the Background of Mobile Consumption

Yun Zhang
(Corresponding author: Yun Zhang)
Zhejiang Yuexiu University of Foreign Languages
No. 2801, Qunxian Middle Road, Shaoxing, Zhejiang, 31200, China
(Email: yunzhangzyu@126.com)
(Received May 31, 2018; revised and accepted Aug. 10, 2018)

Abstract

With the development of mobile network technology, mobile e-commerce is becoming mature, so opportunities and challenges are brought to businesses; therefore, the information security protection of mobile e-commerce is one of challenges. To strengthen the protection, X enterprise was taken as an example to conduct risk assessment in aspects of transactions, organization, data and third-party cooperation using the analytic hierarchy process and triangular fuzzy entropy. It was shown that the information security risk of the enterprise is overall low; transactions are the very common information leakage incident of the four aspects, and third-party cooperation is the safest. Finally, relevant suggestions of information safety protection were put forward based on the assessment results of the four aspects.

Keywords: Analytic Hierarchy Process; E-Commerce; Information Security; Triangular Fuzzy Entropy

1 Introduction

With the development of mobile network technology, mobile terminals have already popularized in people's life, which leads to a new business pattern, mobile e-commerce [1, 9]. At present, mobile e-commerce has features such as high openness, interoperability and no time limitation, so it has become the primary element of modern economic informatization. It can reduce costs, simplify processes and increase trade opportunities in trade activities. Despite the rapid development of e-commerce, the actual proportion of e-commerce in the whole economic trade volume is still very low, which is mainly caused by security problems [14]. As e-commerce does not need to be face to face, the personal privacy of consumer information is required, and the information of the seller or merchant is a trade secret. Therefore, the security of information is crucial in mobile e-commerce.

Zhang *et al.* [15] proposed a single electronic watermarking algorithm for six applications in e-commerce: graphics physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation and secure communication protection was verified with the effectiveness of the algorithm through simulation experiments. Jang *et al.* [7] studied the trust issues between smart phone and information security through empirical research based on users. Their purpose was to study the relationships among computer literacy, network literacy, knowledge of mobile phone virus and the trust (confidentiality, integrity, and availability) of information security management (ISM) principle of the smart phone users. It was shown that the network literacy had a positive effect on virus knowledge, but the computer literacy didn't have. Barai [5] analyzed the operation mode of e-commerce system to solve a security problem of database encryption, and introduced an encryption method based on symmetric and asymmetric encryption technology to overcome the single encryption technology of the traditional electricity system, and then the method was verified to be effective by simulation experiments. In the study, X enterprise was taken as an example to conduct risk assessment in aspects of transactions, organization, data and third-party cooperation using the analytic hierarchy process (AHP) and triangular fuzzy entropy (TFE), and then relevant suggestions were put forward based on the assessment results.

2 Concepts of Mobile E-Commerce

2.1 Mobile E-Commerce

Mobile e-commerce allows users to trade online through wireless networks. Customers can communicate with mer-

chants and visit the key business information any time through mobile terminals. As mobile terminals are used in information interaction, mobile e-commerce has characteristics of mobile terminals: mobility, convenience, positioning and real-time connection [14].

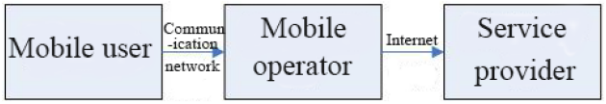


Figure 1: Mobile e-commerce implementation

Figure 1 is the implementation process of mobile e-commerce, and the whole process is simple. As long as the mobile operator opens corresponding wireless services to e-commerce participants on both sides, they can communicate online through the terminals and obtain transaction information anytime.

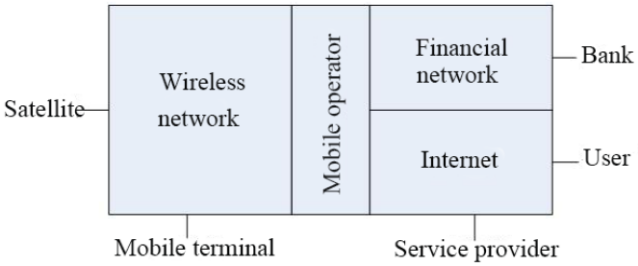


Figure 2: Mobile commerce frame

Figure 2 is a simplified mobile e-commerce frame [12]. Mobile e-commerce transaction is implemented based on Internet, Intranet and financial Intranet, and the transaction is finally implemented under the influence of wired network and infinite network. Mobile users can enjoy the services provided by merchants everywhere.

2.2 Security Problems Of Mobile E-Commerce

With the popularization of mobile terminals (mobile phones, iPads, *etc.*), the technology of mobile network has developed rapidly. Further, the business model has already changed before the relevant credit system, user privacy measures and policies are improved [3]. From the perspective of current development, many problems in mobile e-commerce still need to be solved [11]:

1) Hackers can get trade secrets or customer information illegally by breaking the business system of enterprises;
2) Information is destroyed by spreading viruses, for example, the bitcoin virus maliciously, and then blackmaillmg users;
3) The authority of the internal administrator of the business system is limited and not reasonable.

In order to solve the above problems, it is indispensable to establish a security system for mobile e-commerce. Figure 3 is a simple model of a security system.

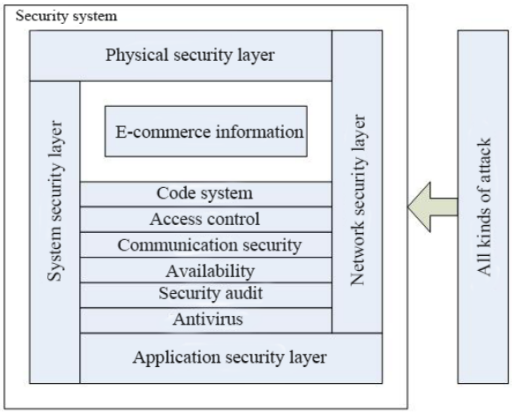


Figure 3: Security system model

It could be noted from the model [5] as shown in Figure 3 that the whole security system includes the application security layer, system security layer, network security layer and physical security layer, which realize the security protection of e-commerce information. The evaluation of security system is also part of security protection research, so this study researches the evaluation of e-commerce information security system to improve the security protection of e-commerce information

3 Evaluation Method of E-Commerce Information Security System

3.1 Analytic Hierarchy Process

AHP is one of multi-objective decision analysis methods [4], which combines qualitative with quantitative. It firstly divides a complex system into several subsystems, and then the subsystems into the target layer, criterion layer and indexes layer according to their characteristics, making the target analysis in order; security protection measures are provided based on the analysis results. The evaluation process includes system decomposition, security judgment and comprehensive judgment. The model of AHP [8] is shown in Figure 4.

3.2 Triangle Fuzzy Number

The mathematical formula of triangular fuzzy number [16] is:

$$\widetilde{N}(x) = \begin{cases} 0, & x \le a \\ \frac{x-a}{b-a}, & a < x \le b \\ \frac{c-x}{c-b}, & b < x \le c \\ 0, & x > c. \end{cases} \quad (1)$$

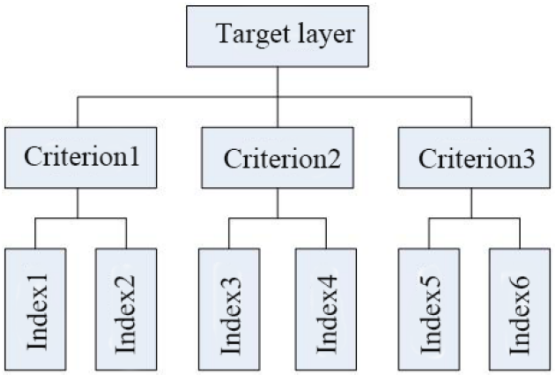


Figure 4: The hierarchical model

where $\widetilde{N}$ is the triangular fuzzy number, which is denoted as (a, b, c). The positive fuzzy number is only considered in the system risk assessment, so Equation (1), $\forall x < 0$, $\widetilde{N}(x) = 0$ also should be satisfied. In the evaluation, a represents the most pessimistic estimate, b represents the most likely estimate, and c is the most optimistic estimate.

3.3 The Entropy Weight Method

Entropy is a value that measures the uncertainty or information amount of the system. Its definition [6] is:

$$H = -\alpha \sum_{i=1}^{m} p_m \log p_i, \tag{2}$$

where H stands for the entropy of the system, and m stands for the status number, $0 \le p_i < 1$ and $\sum_{i=1}^{m} p_i = 1$. The entropy value of the system can be used to describe the degree of variation of the system; the greater the value, the greater the degree of variation and the less information. In this way, the entropy weight of i-th evaluation index in the system is defined as [10]:

$$\varepsilon_i = \frac{1 - H_i}{n - \sum_{i=1}^{n} H_i} \quad (i = 1, 2, \cdots, n), \tag{3}$$

where $0 \le \varepsilon_i \le 1$, $\sum_{i=1}^{n} \varepsilon_i = 1$. The effective information degree of an index in the system is expressed as entropy weight.

4 Case Analysis

4.1 Assessment of The Enterprise Profile

A Chinese enterprise X whose main business was mobile e-commerce and its existing information security protection level was evaluated. With the advent of mobile Internet, the enterprise X transformed its business and began to reduce the traditional electronic commerce to adapt to the development trend of the market, and then this enterprise used the model of online "brand + operation" to increase mobile electronic commerce activities which mainly included "boost business", "pull business" and "interactive business". As the business was related to the personal information of customers closely, it was crucial to protect the e-commerce information security, and some corresponding countermeasures should be put forward based on risk evaluation.

4.2 Evaluation Method

1) The information security protection risk of X enterprise was evaluated through questionnaire survey in aspects of organizational risk, data risk, transaction risk and third-party cooperation risk. A total of 200 questionnaires were randomly distributed in a ratio of 1:2:4 to middle-level leaders, grassroots cadres and ordinary employees, and the score of each index was between 0 and 100.

2) The results recorded after questionnaires were recycled, and a standardized matrix was constructed based on the score formula of positive and negative indicators [13], and standardized data was obtained. Then the entropy weight of each index was determined, referring to Equation (3).

3) Six experts were invited to evaluate the information security protection of enterprises, and the subjective evaluation matrix of experts could be obtained. The triangular fuzzy weight derived by the fuzzy synthesis matrix was obtained by the weight set of experts, and then the comprehensive weight of indicators was determined. The calculation formula of triangular fuzzy weight is:

$$\omega_i = \frac{\mu_i}{\sum_{i=1}^{n} \mu_i} \tag{4}$$

where μ_i stands for the weight vector of the i-th index in the triangular fuzzy set; the formula of comprehensive weight is:

$$\sigma_i = \theta \varepsilon_i + (1 - \theta)\omega_i, \tag{5}$$

where θ is the weight ratio of the objective preference coefficient, here $\theta = 0.4$.

4.3 Evaluation Results and Analysis

Table 1 shows the weight of each indicator and their results. It can be seen that the final evaluation of 13 indicators is:

$$D = [0.016\ 0.0329\ 0.0517\ 0.0661\ 0.0187\ 0.0245\ 0.0641\ 0.0496\ 0.0925\ 0.1103\ 0.0136\ 0.0374\ 0.0389]^T;$$

and the evaluation score of each criterion layer is $(1006, 1093, 0.3165, 0.0899)$.

Table 1: Weight of each indicator and evaluation results

Criterion layer	IL	EW	TFW	CW	AR
"Organization" risk (A1)	Financial Guarantee (A11)	0.0347	0.0474	0.0423	0.016
	Personnel Risk (A12)	0.0414	0.0564	0.0504	0.0329
	Safety Gear(A13)	0.108	0.0776	0.0898	0.0517
Data risk (A2)	Database Security (A21)	0.1066	0.096	0.1002	0.0661
	Information Encryption Security (A22)	0.0498	0.0547	0.0527	0.0187
	Integrity Strategy (A23)	0.0693	0.0445	0.0544	0.0245
"Transaction" Risk (A3)	Access Security (A31)	0.0895	0.1026	0.0974	0.0641
	Application Security (A32)	0.0856	0.0875	0.0867	0.0496
	Network Security (A33)	0.132	0.1143	0.1214	0.0925
	Terminal Security (A34)	0.1665	0.1142	0.1351	0.1103
Third-party "cooperation" risk (A4)	Risk of Relationship Weakening (A41)	0.0107	0.0475	0.0328	0.0136
	Contract Control Ability (A42)	0.0453	0.0828	0.0678	0.0374
	Partner Level(A43)	0.0606	0.0745	0.0689	0.0389

IL: Index Layer; EW: Entropy weight; TFW: Triangular Fuzzy Weight; CW: Comprehensive Weight; AR: Assessment Result.

Table 2 shows combined weight, assessment result and final risk value of each criterion layer. The final risk values are 0.0184 for A1, 0.0227 for A2, 0.1394 for A3, and 0.0152 for A4, and the total risk value of the security protection of e-commerce information of the whole enterprise is 0.1957. The risk degree of information security protection of the enterprise could be evaluated through the risk value calculated above. In general, the final risk value means high risk when it was larger than 0.7, and low risk when it was less than 0.3. The overall risk value of enterprise X was 0.1957, which means that the information security protection risk was low. The comparison suggested that the risk value of A3 was the highest, followed by A2, A1 and A4, showing that the most possible link of information security protection risk was the mobile transaction link, while the third party cooperation was relatively safe.

The comparison of different weights and evaluation results of indicators in the criterion layer are shown in Figure 5.

In terms of transaction risk, it was found from the comparison of transaction risk block that when the entropy weight is 0.1665, integrated weight is 0.1351, evaluation results are the highest, and the triangular fuzzy weights (0.1142) was relatively high, showing that the mobile terminal was most likely to affect the risk of information security protection in trading. Information leakage could cause a wide range of serious problems. The enterprise should pay real attention to the aspect of transaction risk.

In terms of data risk, the entropy value weight (0.1066), triangle fuzzy weight (0.096), integrated weight (0.1002) and evaluation results (0.0661) are much higher compared with the information encryption security and integrity strategy in Figure 5. The risk of database security is the highest so that the enterprise should pay real attention to database security. The integrated weights of the other

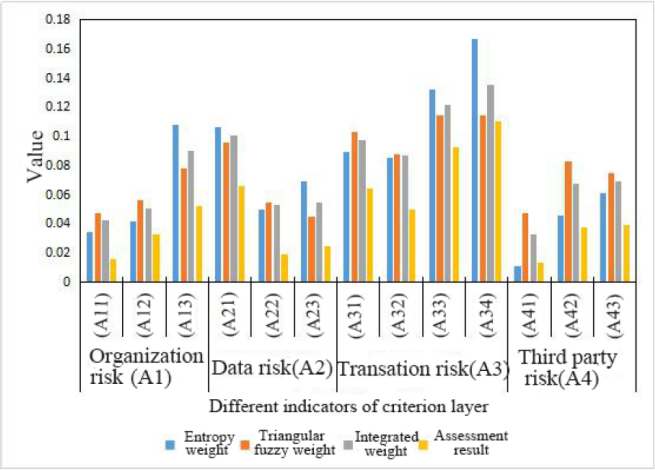


Figure 5: Comparison between weight and evaluation result of each indicator

Table 2: Evaluation results and final risk values of the criterion layer

Criterion layer	Combined weight	Assessment result	Final risk value
Organization risk (A1)	0.1825	0.1006	0.0184
Data risk (A2)	0.2073	0.1093	0.0227
Transaction (A3)	0.4406	0.3165	0.1394
Third-party cooperation risk (A4)	0.1695	0.0899	0.0152
Total	-	-	0.1957

two indicators are moderate. The evaluation results are relatively low, indicating that the loss and influence of enterprises are the least while accidents occurring because of the well protective measures. As the entropy weight and triangle fuzzy weight are paid attentions to by employees and experts at different degrees, the two weights are different, and the indicators paid less attentions to cause greater loss in the event of accidents.

In terms of organizational risk, the evaluation result of information security institutions is the largest, the risk of organizational personnel is the second, and financial security is the smallest as shown in Figure 5, and the integrated weight of financial security is relatively close to that of organizational personnel risk, 0.0423 vs. 0.0504, respectively, showing that the risk level between them is similar. While the evaluation result of financial security (0.016) is far lower than that of organizational personnel risk (0.0329), indicating that the enterprise pays enough attention to information security protection of financial security.

In terms of the third cooperation risk, the integrated weight of the level of the third-party cooperators, contract control, and weakened customer relationship risk are relatively low, 0.0689, 0.0678 and 0.0328, respectively as shown in Figure 5. The results of risk assessment are also low, indicating that the enterprise performs well in managing third-party cooperation, and for cooperators that have high of information, their risks of information security protection are less likely to happen.

4.4 Measures for Strengthening Information Security

Protection According to the assessment results and the analysis above, corresponding measures can be taken from several aspects of the criterion layer to improve the security protection of e-commerce information and reduce security risks under the background of mobile consumption.

1) In terms of organizational risk, the enterprise should strengthen the awareness of information security protection and regard it as the core content in the training of information security operation of employees. Moreover, it should strengthen employees' sense of belonging to improve the overall information literacy; according to the business arrangement and status, and requirements of information security, the enterprise should also formulate the framework of information security protection based on current management and protection technologies, keep up to date with the information security control system and focus on the implement of enterprises' supervision.

2) In terms of transaction risk, the enterprise should ensure the confidentiality and integrity of the information during the network communication transactions between the two parties, strengthen the management of relevant keys and the ability of resisting external attacks of the internal network, and strictly manage the use of employees' rights in the information network to minimize the risks of customers in communication transactions; in the meanwhile, the enterprise should also ensure the accuracy of identification in the interaction between mobile terminals and the network, and pay attention to technologies such as voice print recognition and fingerprint identification to help the enterprise improve the identification ability so to ensure the security and authenticity of data interaction.

3) In terms of data risk, databases should be encrypted effectively to prevent data theft caused by attacks in the internal system. Identification, recovery of lost data, isolation of physical storage devices, detection of network ports and data backup are all the encryption methods applied to databases, and the encryption of the physical level also needs the isolation of physical facilities and regular maintenance of equipment.

4) In terms of third-party cooperation, the enterprise should ensure the stability of the internal organization and the source of funds, strengthen the awareness of information security protection of employees and relevant security expertise, and select the third-party operators carefully to ensure that both parties have high levels of information management to ensure the information security protection in transactions.

5 Conclusion

In the study, security protection degree of e-commerce under the background of mobile consumption was evaluated by AHP and TFE. X enterprise was taken as an

example to conduct risk assessment in aspects of transactions, organization, data and third-party cooperation, and the results achieved are that the overall risk of the security protection of e-commerce information is low; the risk of transaction is the highest while the risk of the third-party operation is the lowest. The mobile terminal has the worst information security protection in the risk of transactions. The enterprise should pay more attention to information encryption and integrity strategy due to the lowest security protection of database. In the aspect of organization risk, the highest risk was the information security protection, and the enterprise performed well in managing third-party cooperation; cooperators have high levels of information, so their risks of information security protection are less likely to happen. In the end of the study, several suggestions were proposed for e-commerce information security protection.

References

[1] D. S. AbdElminaam, H. M. Abdul Kader, M. M. Hadhoud, S. M. El-Sayedr, "Increase the performance of mobile smartphones using partition and migration of mobile applications to cloud computing," *International Journal of Electronics and Information Engineering*, vol. 1, No. 1, pp. 34-44, 2014.

[2] O. I. Araoye, O. S. Adewale, B. K. Alese, *et al.*, "Developing a secured mobile-agent-based electronic commerce using crypto-steganography," *International Journal of Sciences*, vol. 4, no. 2, pp. 82–88, 2018.

[3] D. E. Asuquo, U. A. Umoh, "Analytic hierarchy process for QoS evaluation of mobile data networks," *International Journal of Computer Networks & Communications*, vol. 7, no. 6, pp. 125–137, 2015.

[4] J. F. Bai, X. Y. Wei, J. C. Yan, "Research on the selection of business-to-customer e-commerce logistics model based on analytic hierarchy process method," in *Proceedings of the 23rd International Conference on Industrial Engineering and Engineering Management*, pp. 11–15, 2016.

[5] D. K. Barai, I. S. Prabha, R. Srikanth, *et al.*, "Hypothecation of electronic commerce system with hybrid encryption methodology (HEM)," in *IEEE International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 2926–2929, 2016.

[6] F. Benedetto, G. Giunta, L. Mastroeni, "A maximum entropy method to assess the predictability of financial and commodity prices," *Digital Signal Processing*, vol. 46(C), pp. 19–31, 2015.

[7] Y. Jang, S. E. Chang, Y. Tsai, "Smartphone security: Understanding smart phone users' trust in information security management," *Security & Communication Networks*, vol. 7, no. 9, pp. 1313–1321, 2015.

[8] K. Katsaros, M. Dianati, Z. Sun, *et al.*, "An evaluation of routing in vehicular networks using analytic hierarchy process," *Wireless Communications & Mobile Computing*, vol. 16, no. 8, pp. 895–911, 2016.

[9] G. Lv, M. Gao, X. Ji, "Research on information security of electronic commerce logistics system," in *International Conference on Intelligent Computing*, pp. 600–611, 2016.

[10] C. Miao, M. Ding, "Social vulnerability assessment of geological hazards based on entropy method in Lushan earthquake-stricken area," *Arabian Journal of Geosciences*, vol. 8, no. 12, pp. 10241–10253, 2015.

[11] Y. Shi, J. Han, J. Li, *et al.*, "Identity-based undetachable digital signature for mobile agents in electronic commerce," *Soft Computing*, pp. 1–15, 2018.

[12] Y. Shi, J. Lin, G. Xiong, *et al.*, "Key-insulated undetachable digital signature scheme and solution for secure mobile agents in electronic commerce," *Mobile Information Systems*, vol. 2016(2), pp. 1–18, 2016.

[13] C. Singla, S. Kaushal, "Cloud path selection using fuzzy analytic hierarchy process for offloading in mobile cloud computing," in *IEEE International Conference on Recent Advances in Engineering & Computational Sciences*, pp. 1–5, 2016.

[14] D. Strzebicki, "The development of electronic commerce in agribusiness - The polish example," *Procedia Economics & Finance*, vol. 23, pp. 1314–1320, 2015.

[15] Q. Zhang, J. Zhu, X. Wang, *et al.*, "Monoecism algorithm in the application of e-commerce information security," *International Journal of Security & Its Applications*, vol. 9, no. 3, pp. 319–334, 2015.

[16] R. C. Zoie, "Cloud provider's services evaluation using triangular fuzzy numbers," in *IEEE International Conference on Control Systems and Computer Science*, pp. 123–128, 2017.

Biography

Yun Zhang, female, born in January 1978, graduated with a master's degree from the major of management science and engineering in Chongqing University of Posts and Telecommunications, China. Now she is a teacher in Zhejiang Yuexiu University of Foreign Languages, Shaoxing, Zhejiang, China. Her interests of research are E-commerce, mobile e-commerce and marketing.

A Conference Key Scheme Based on the Diffie-Hellman Key Exchange

Li-Chin Huang[1] and Min-Shiang Hwang[2,3]
(Corresponding author: Min-Shiang Hwang)
Department of Information Management, Executive Yuan, Taiwan (ROC)[1]
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University[3]
(Email: mshwang@nchu.edu.tw)
(Received May 31, 2018; revised and accepted Aug. 10, 2018)

Abstract

Secure group communication is becoming more and more important in internet. In order to provide a secure and reliable communication among the members of a conference over a public network, all group members must have the ability to establish a common secret key. We call this kind of the public key distribution system is a conference key distribution system (CKDS). Our protocol bases on the two-party Diffie-Hellman protocol to build intermediate keys from each subgroups gradually until the entire conference key is obtained. The process of forming the entire conference key will constructed a ripple structure which reduce the times of encryption and decryption than butterfly scheme key distribution systems. Our protocol promote the efficiency of a conference key distribution system.

Keywords: Conference Key; Key Authentication; Secure Group Communication

1 Introduction

A public key distribution system called public key distribution system (PKDS) is developed firstly [4]. However, this system provides only one pair of communication parties to share a particular pair of encryption and decryption keys [3, 9, 11, 13, 14, 21, 30]. The public key distribution system is applied in a conference key distribution system (CKDS) to permit any legitimate parties to share the same encryption and decryption keys. Hence, a conference key distribution system (CKDS) [2,29] is a scheme which generates a conference key and then spreads this key to all legitimate participants for establishing a secure communication.

Imgresson *et al.* [16] proposed a conference key distribution system (CKDS) without authentication on a ring network. For authenticate legitimate members using member's identification information (such as member's name and address) in cryptosystems, Shamir and Fiat proposed identify-based signature schemes [5], and Okamoto proposed an identity-based scheme [23]. An identity-based system applies to generating a conference key with authentication [23], called an identity-based conference key distribution system (ICKDS). Koyam and Ohta [17] applied Identity-based CKDS (ICKDS) on a ring network, complete graph network, and a star network. Many conference key schemes had been proposed for various enterprise organizations [1, 6–8, 15, 20, 25, 27, 31]. In this paper, we will propose a new hierarchical approach, the ripple scheme, to improve a conference key distribution.

The remaining of the paper is organized as follows. Section 2 gives a brief overview of the butterfly scheme. The proposed method is described in Section 3. Sections 4, 5, and 6 discuss the encryption and decryption cost, performance comparisons, and security analysis. Section 7 closes the paper with the conclusion.

2 Review of The Butterfly Scheme

In the butterfly scheme [26], the users generate a share keys for small subgroups, and furthermore these subgroups form larger subgroups and establish new subgroup keys by previous subgroup keys. These steps of key generation are repeated until the whole group constructs a share key for all users. The butterfly scheme is shown in Figure 1.

The initiation phase: Each user u_j chooses a random secret integer $\alpha_j \in Z_p^*$, where Z_p^* denotes the nonzero elements of the integers mod a prime p.

A conference key generation and distribution phase:

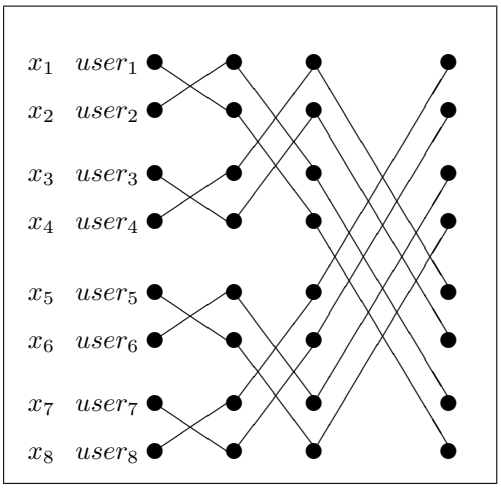


Figure 1: The butterfly scheme

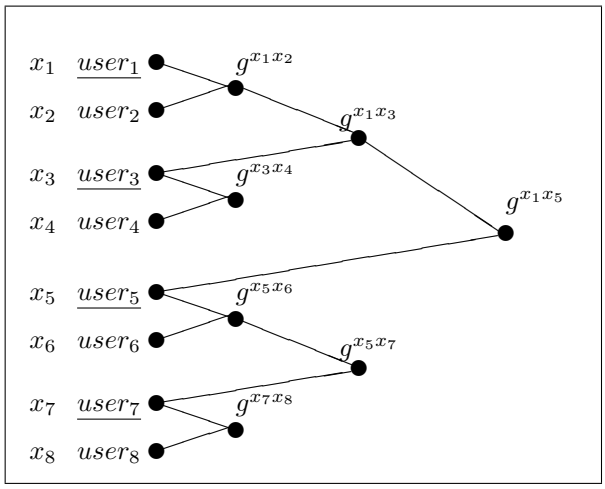


Figure 2: The Ripple scheme

1) In the first pairing, the members of a pair exchange $g^{x_j^0}$, where $x_j^0 = \alpha_j$. For example, u_1 sends $g^{x_1^0}$ to u_2, and u_2 sends $g^{x_2^0}$ to u_1. Then the users u_{2j-1} and u_{2j} compute $x_j^1 = g^{x_{2j-1}^0 x_{2j}^0} = g^{\alpha_{2j-1}\alpha_{2j}}$, where $x_j^1 \in Z_p^*$. Therefore, the members of a pair have established a conventional Diffie-Hellman key exchange.
2) In the second pairing, we may pair the pairs $u_j^1 = \{u_{2j-1}, u_{2j}\}$ into a second level of pairs. For Instance, $u_1^2 = \{u_1^1, u_2^1\}$, and a general rule $u_j^2 = \{u_{2j-1}^1, u_{2j}^1\}$. Consequently, the second level of pairings consists of 4 users in a pair. Each user u_{2j-1}^1 and u_{2j}^1 exchange $g^{x_{2j-1}^1}$ and $g^{x_{2j}^1}$. Every member in u_j^2 can compute $x_j^2 = g^{x_{2j-1}^1 x_2^1 j}$.
3) In the third pairing, consisting of 8 users may be formed. Each user u_{2j-1}^2 and u_{2j}^2 exchange $g^{x_{2j-1}^2}$ and $g^{x_{2j}^2}$. Then, every member in u_j^3 can compute $x_j^3 = g^{x_{2j-1}^2 x_{2j}^2}$. Reasoning from above the principle, we may produce a general rule, $u_j^k = \{u_{2j-1}^{k-1}, u_{2j}^{k-1}\}$ and $x_j^k = g^{x_{2j-1}^{k-1} x_{2j}^{k-1}}$.

3 The Proposed Scheme

We propose a different hierarchical approach to improve a conference key distribution. In our scheme, the users form keys for small subgroups using Diffie-Hellman scheme [4], and these subgroups act as single entities and chose a user as their manager to establish subgroup key that form larger subgroups and establish new keys using the manager's key chosen by in the previous subgroup keys. The process repeats until the entire group has formed a key that was shared by all members. For simplicity, we suppose the ripple scheme for establishing a group key for 8 users as shown in Figure 2. Our scheme describe as follow.

The initiation phase:

Each $user_i$ chooses a random secret integer $x_i \in Z_P^*$, $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$.

A conference key generation phase:

1) In the first round, the members of a pair exchange g^{x_i}, $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ to establish a conventional Diffie-Hellman key as their subgroup key (SK for short). Thus the users form keys for small subgroups, and these subgroups as single entities. For example, $user_1$ sends g^{x_1} to $user_2$, and $user_2$ sends g^{x_2} to $user_1$. Then, $user_1$ and $user_2$ establish a subgroup key $SK_{12} = g^{x_1x_2}$ mod p. Therefore, the $user_{2k-1}$ and $user_{2k}$ calculate a subgroup key $SK_{(2k-1)(2k)} = g^{(x_{2k-1})(x_{2k})}$ mod p , $k \in \{1, 2, 3, 4\}$, respectively.
2) In the second round, to form larger subgroups and establish new subgroup keys. The new subgroup key is formed by the manager's key which is selected from each subgroup. For example, $user_1$ and $user_2$ form a small subgroup which subgroup key SK_{12} is $g^{x_1x_2}$ mod p. And immediately they select a group manager $user_1$. As the same way, $user_3$ and $user_4$ get a small subgroup key $SK_{34} = g^{x_3x_4}$ mod p, and then select a group manager $user_3$. Afterwards, they take the manager's key g^{x_1} and g^{x_3} to form a larger subgroup key $SK_{1234} = g^{x_1x_3}$ mod p for $\{user_1, user_2, user_3, user_4\}$. Obviously, $\{user_5, user_6\}$ and $\{user_7, user_8\}$ can separately get $SK_{56} = g^{x_5x_6}$ mod p and $SK_{78} = g^{x_7x_8}$ mod p. They also select the manager $user_5$ and $user_7$ to from $SK_{5678} = g^{x_5x_7}$ mod p.

   Finally, the conference key $SK_{12345678} = g^{x_1x_5}$ mod p is formed by the manager $user_1$

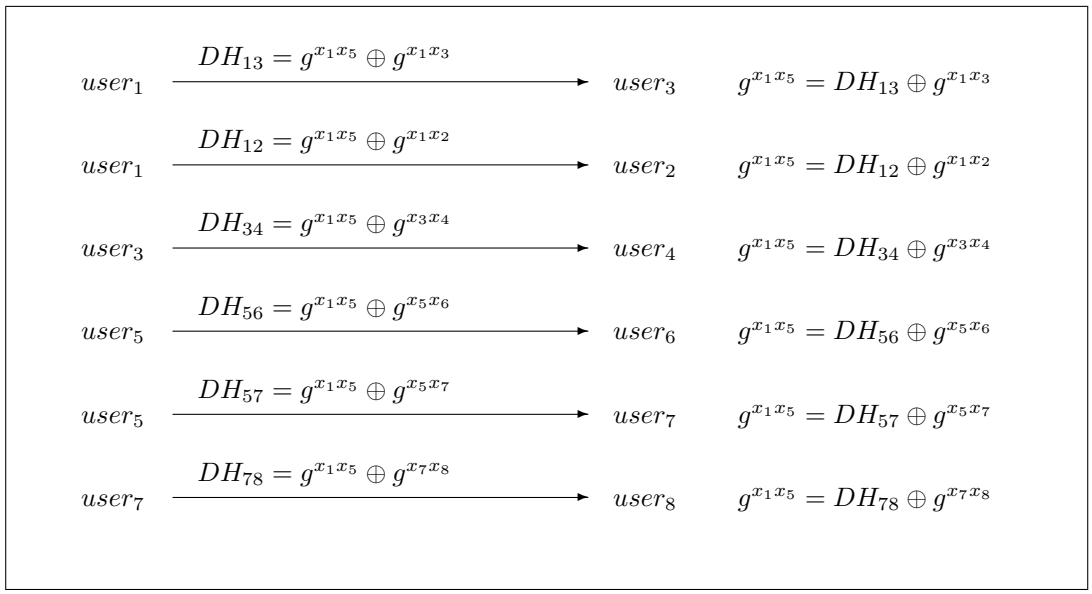


Figure 3: The conference key distributes to each member

and $user_5$ from $\{user_1, user_2, user_3, user_4\}$ and $\{user_5, user_6, user_7, user_8\}$.

The conference key distributes to each member phase:

The group manager $user_1$ and $user_5$ possess the conference key (for short CK).

1) $user_1$ send $DH_{13} = g^{x_1x_5} \bigoplus g^{x_1x_3}$ to $user_3$. As the same time, $user_1$ also sends $DH_{12} = g^{x_1x_5} \bigoplus g^{r_1r_2}$ to $user_2$.
2) $user_2$ gets the conference key $g^{x_1x_5}$ by computing $DH_{12} \bigoplus g^{x_1x_2}$.
3) $user_3$ gets the conference key $g^{x_1x_5}$ by $DH_{13} \bigoplus g^{x_1x_3}$. Then $DH_{34} = g^{x_1x_5} \bigoplus g^{x_3x_4}$ is computed by $user_3$ and sends it to $user_4$.
4) $user_4$ gets the conference key $g^{x_1x_5}$ by $DH_{34} \bigoplus g^{x_3x_4}$.
5) As the same way, $user_5$ send DH_{56} and DH_{57} to $user_6$ and $user_7$, respectively.
6) $user_6$ gets the conference key by $DH_{56} \bigoplus g^{x_5x_6}$.
7) $user_7$ gets the conference key by $DH_{57} \bigoplus g^{x_5x_7}$ and send DH_{76} to $user_8$.
8) $user_8$ gets the conference key by $DH_{78} \bigoplus g^{x_7x_8}$.

4 Encryption and Decryption Costs

As indicated in the previous section, our protocol is superior to the others with respect to exponentiation operations. With respect to conference key generation time, the total cost is 22 exponents and 12 XOR. We describe as follow.

The conference key generation phase:

Table 1 is the cost of the conference key generation phase.

1) **The first round:** Each $user_i$ and $user_{i-1}$ establishes a secret key $SK_{(2i-1)(2i)}$ based on Diffie-Hellman key exchange. There are 16 exponents in this round.
2) **The second round:** There are 2 exponentiation to form SK_{1234} secret key for $\{user_1, user_2, user_3, user_4\}$. As the same way, to construct SK_{5678} secret key requires 2 exponents.
3) **The third round:** To construct $SK_{12345678}$ (i.e. conference key) requires 2 exponents.

The conference key distributes to each member phase:

Figure 3 describes the conference key distributes to each member. Obviously, $user_i$ will generates $DH_{ij} = g^{x_1x_5} \oplus g^{x_ix_j}$ and send to $user_j$, the pair of $(i, j) \in \{(1, 3), (1, 2), (3, 4), (5, 6)\}$. Finally, $user_j$ get conference key $g^{x_1x_5}$.

Therefore, if n members require $n \times 2 + \sum_{i=1}^{log_2 n-1} \frac{1}{2i}$ exponents and $2log_2 n$ XOR to construct a conference key. In tree based conference key distribution systems require $2nlogn$. Our protocol is more efficient obviously.

5 Performance Comparison

In this section, we shall compare the computational complexity of our scheme with that of the butterfly scheme. To analyze the computational complexity, we first define the following notations.

Table 1: The Cost of the Conference Key Generation Phase

Round	Operation	Exponents per $user_i$	Times of exponents
1	$user_i$ compute g^{x_i} $i \in \{1,2,3,4,5,6,7,8\}$	$user_i$ $i \in \{1,2,3,4,5,6,7,8\}$	8
	$SK_{(2i-1)(2i)} = g^{(2x_i)(2i)}$ $i \in \{1,2,3,4,5,6,7,8\}$	$user_i$ $i \in \{1,2,3,4,5,6,7,8\}$	8
2	$SK_{1234} = g^{(x_1)(x_3)}$	$user_1$, $user_2$	2
	$SK_{5678} = g^{(x_5)(x_7)}$	$user_5$, $user_7$	2
3	$SK_{12345678} = g^{(x_1)(x_5)}$	$user_1$, $user_5$	2
Total			22

T_{MUL}: the time for computing modular multiplication.

T_{EXP}: the time for computing modular exponentiation.

T_{XOR}: the time for computing exclusive OR.

n: the number of participants in the conference.

In the conference key generation stage of our scheme, n members generate an entire conference key. Each member chooses a random secret key x_i and computes the corresponding public key g^{x_i}. Then, the members of a pair exchange their secret g^{x_i}, i $\in \{1, ..., n\}$ to construct a conventional Diffie-Hellman key as their subgroup key. Obviously, round 1 requires $2n \times T_{EXP}$. In the second Round, $\frac{n}{2}$ subgroup keys form larger subgroups by a convention Diffie-Hellman key, which require $\frac{n}{2} \times T_{EXP}$. As the same way, round i requires $\frac{n}{2^{i-1}} \times T_{EXP}$. Total computational complexity in this stage is required 3n-2n $\times (\frac{1}{2})^{(\log_2 n)} \times T_{EXP}$.

After generating the entire conference key (CK), each member enters the conference key distribution stage. $User_1$ computes $DH_{1,(\frac{n}{2^2}+1)} = CK \bigoplus g^{x_1 x_{\frac{n}{2^2}+1}}$ and send to $user_{(\frac{n}{2^2}+1)}$. Then $user_{(\frac{n}{2^2}+1)}$ obtains the conference key by $DH_{1,(\frac{n}{2^2}+1)} \bigoplus g^{x_1 x_{\frac{n}{2^2}+1}}$. As the same way, $user_{\frac{n}{2}+1}$ computes $DH_{(\frac{n}{2}+1),(\frac{n}{2}+\frac{n}{2^2}+1)} = CK \bigoplus g^{x_{\frac{n}{2}+\frac{n}{2^2}+1}}$ and send to $user_{(\frac{n}{2}+\frac{n}{2^2}+1)}$. $User_{(\frac{n}{2}+\frac{n}{2^2}+1)}$ also gets the conference key by $DH_{(\frac{n}{2}+1),(\frac{n}{2}+\frac{n}{2^2}+1)} \bigoplus g^{x_{\frac{n}{2}+\frac{n}{2^2}+1}}$. Therefore, round 1 requires $4 \times T_{XOR}$. The round 2 requires $8 \times T_{XOR}$ and round i requires $2^{(i+1)} \times T_{XOR}$. Total computation complexity in the key distribution stage is required $(2^{(\log_2 n)+1} - 4) \times T_{XOR}$.

In the computational complexity of the butterfly scheme, each user u_j chooses a random secret integer α_j and the members of a pair exchange x_j^0 to get the Diffie-Hellman key u_j^1 in the first round. Therefore, round 1 requires $2n \times T_{EXP}$. In the round 2, the members form $u_j^2 = \{u_{2J-1}^1, u_{2J}^1\}$ and require $n \times T_{EXP}$. The round i requires $n \times T_{EXP}$. Therefore, the butterfly scheme requires $n(\log_2 n + 1) \times T_{EXP}$.

According to Table 2, our scheme is more efficient than the butterfly scheme obviously.

6 Security

The security level of the proposed CKDS is based on Discrete Logarithmic Problem. Assume p is a large prime and g is a generator for Z_p^*. If b $\in X_p^*$ is publicly known, it is still hard to find the a such that b = g^a mod p. In our scheme, we extend two party Diffie-Hellman key exchange to construct a conference key, that is, two users such as $user_1$ (with private key x_1 and public key $b_1 = g^{x1}$ mod p) and $user_2$ (with private key x_2 and public key $b_2 = g^{x2}$ mod p) can calculate the shared key SK = g^{x1x2} mod p. Any user except $user_1$ and $user_2$ can not calculate SK even they know x_1 and x_2. Although the Diffie-Hellman key exchange exits a Man-in-Middle attack, many solutions [10, 12, 18, 22, 24, 28] are proposed to solve this problem.

7 Conclusions

In this paper, we show a different group key that the users produce a group key by the two-party Diffie-Hellman protocol. Our new scheme is more efficient than the butterfly scheme [26].

References

[1] T. Y. Chang and M. S. Hwang, "User-anonymous and short-term conference key distribution system via link-layer routing in mobile communications", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 144–158, 2011.

[2] T. Y. Chang, M. S. Hwang, W. P. Yang, "Cryptanalysis of the Tseng-Jan anonymous conference key distribution system without using a one-way hash function", *Information & Security: An International Journal*, vol. 15, no. 1, pp. 110–114, 2004.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol," *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

Table 2: Computational complexities of the butterfly scheme and our scheme

Round	Round 1	Round 2	...	Round i ($2 \le i \le \log_2 n$)	total
Our scheme					
key generation	$2n\times\ T_{EXP}$	$\frac{n}{2}\times\ T_{EXP}$	...	$\frac{n}{2^{i-1}}\times\ T_{EXP}$	3n-2n $\times(\frac{1}{2})^{(\log_2 n)}\times\ T_{EXP}$
key distribution	$4\times\ T_{XOR}$	$8\times T_{XOR}$	...	$2^{(i+1)}\times T_{XOR}$	$(2^{(\log_2 n)+1}-4)\times T_{XOR}$
The butterfly scheme	$2n\times\ T_{EXP}$	$n\times\ T_{EXP}$	...	$n\times\ T_{EXP}$	$[n(\log_2 n-1)+2n]\times T_{EXP}$ $= n(\log_2 n+1)\times\ T_{EXP}$

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[5] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proceedings of Crypto'86*, pp. 175–184, 1987.

[6] C. Guo, C. C. Chang, "A novel threshold conference-key agreement protocol based on generalized Chinese remainder theorem," *International Journal of Network Security*, vol. 17, no. 2, pp. 165-173, 2015.

[7] L. Harn, G. Gong, "Conference key establishment protocol using a multivariate polynomial and its applications," *Security and Communication Networks*, vol. 8, no. 9, pp. 1794–1800, 2015.

[8] C. L. Hsu, T. W. Lin, H. C. Lu, T. H. Chuang, Y. H. Chen, "Privacy-preserved conference key distribution protocol," in *12th International Conference on Digital Information Management*, pp. 127–132, 2018.

[9] M. S. Hwang, "Dynamic participation in a secure conference scheme for mobile communications", *IEEE Transactions on Vehicular Technology*, vol. 48, no. 5, pp. 1469–1474, Sept. 1999.

[10] M. S. Hwang, S. K. Chong, H. H. Ou, "On the security of an enhanced UMTS authentication and key agreement protocol," *European Transactions on Telecommunications*, vol. 22, no. 3, pp. 99–112, 2011.

[11] M. S. Hwang, C. W. Lin, and C. C. Lee, "An improved Yen-Joye's authenticated multiple-key agreement protocol," *Electronic Letters*, vol. 38, no. 23, pp. 1429–1431, 2002.

[12] M. S. Hwang, J. W. Lo, C. H. Liu, "Enhanced of key agreement protocols resistant to a denial-of-service attack," *Fundamenta Informaticae*, vol. 61, no. 3, pp. 389–398, 2004.

[13] M. S. Hwang, W. G. Tzeng, "A conference key distribution scheme in a totally-ordered hierarchy", *Lecture Notes in Computer Science*, vol. 2662, pp. 757–761, 2003.

[14] M. S. Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems", *IEEE Journal on Selected Areas in Communications*, vo1. 13, no. 2, 1995, pp. 416–420.

[15] T. Hyla, J. Pejaś, "A fault-tolerant authenticated key-conference agreement protocol with forward secrecy," *Lecture Notes in Computer Science*, vol. 9842, pp. 647–660, 2016.

[16] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. IT-28, September.

[17] K. Koyama and K. Ohta, "Identity-based conference key distribution system," in *Lecture Notes in Computer Science*, vol. 293, pp. 181–187, 1986.

[18] C. C. Lee, M. S. Hwang, and L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.

[19] C. C. Lee, T. C. Lin, M. S. Hwang, "A key agreement scheme for satellite communications," *Information Technology and Control*, vol. 39, no. 1, pp. 43–47, 2010.

[20] J. S. Lee, C. C. Chang, and K. J. Wei, "Provably secure conference key distribution mechanism preserving the forward and backward secrecy," *International Journal of Network Security*, vol. 15, no. 5, pp. 405–410, 2013.

[21] J. W. Lo, J. Z. Lee, M. S. Hwang, Y. P. Chu, "An improvement of a simple authenticated key agreement algorithm," *Journal of Internet Technology*, vol. 11, no. 7, pp. 997–1004, 2010.

[22] J. W. Lo, S. C. Lin, M. S. Hwang, "A parallel password-authenticated key exchange protocol for wireless environments," *Information Technology and Control*, vol. 39, no. 2, pp. 146–151, 2010.

[23] E. Okamoto, "Proposal for identity-based key distribution systems," *Electron. Letters*, vol. 22, pp. 1283–1284, 1986.

[24] H. H. Ou, M. S. Hwang and J. K. Jan, "A cocktail protocol with the authentication and key agreement on the UMTS," *Journal of Systems and Software*, vol. 83, no. 2, pp. 316–325, 2010.

[25] J. Ribeiro, G. Murta, S. Wehner, "Fully device-independent conference key agreement," *Source: Physical Review A*, vol. 97, no. 2, 2018.

[26] W. Trappe, Y. Wang, and K. J. R. Liu, "Group key agreement using divide-and-conquer strategies," in *Conference on Information Sciences and Systems*, 2001.

[27] C. Tselikis, C. Douligeris, S. Mitropoulos, N. Komninos, G. Tselikis, "Adaptation of a Conference Key Distribution System for the wireless ad hoc network,"

in *IEEE International Conference on Communications*, 2017.

[28] C. C. Yang, T. Y. Chang, M. S. Hwang, "Cryptanalysis of simple authenticated key agreement protocols," *IEICE Transactions on Foundations*, vol. E87-A, no. 8, pp. 2174–2176, 2004.

[29] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem", *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 141–145, May 2003.

[30] C. C. Yang, J. W. Li, M. S. Hwang, "A new mutual authentication and key exchange protocol with balanced computational power for wireless settings," *European Transactions on Telecommunications*, vol. 15, no. 2, pp. 91–99, 2004.

[31] C. N. Yang, J. M. Li, Y. S. Chou, "On the analysis of k-secure t-conference key distribution scheme," in *ACM 7th International Conference on Communication and Network Security*, pp. 91–95, 2017.

Biography

Li-Chin Huang received the B.S. in computer science from Providence University, Taiwan, in 1993 and M.S. in information management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001; and the Ph.D. degree in computer and information science from National Chung Hsing University (NCHU), Taiwan in 2001. Her current research interests include information security, cryptography, medical image, big data, and mobile communications.

Min-Shiang Hwang received B.S. in electronic engineering from National Taipei Institute of Technology, Taipei, Taiwan, in 1980; M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He also studied applied mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "electronic engineer" in 1988. He also passed National Telecommunication Special Examination in field "information engineering", qualified as the first class advanced technician in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories, Ministry of Transportation and Communications. He was also the Chairman of Department of Information Management, CYUT, Taiwan, during 1999-2002. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

Supervision and Investigation of Internet Fraud Crimes

Lei Zhang
(Corresponding author: Lei Zhang)
Railway Police College, Zhengzhou, Henan 450053, China
(Email: zhangleirpc@126.com)
(Received May 31, 2018; revised and accepted Aug. 10, 2018)

Abstract

The popularity of computers and the Internet in recent years facilitates people's life, but the Internet also provides a convenient crime platform for illegal elements. In order to detect and prevent Internet fraud accurately, Association Rules Mining was performed on the information in the samples of some Internet fraud cases using Apriori algorithm in this study. The attribute fields used for searching association rules are location of crime, scope of crime, time of crime, number of cases and degree of loss. Finally, it was found that the inherent rule is that Internet fraud in the suburban community will cause a higher loss. Moreover, several measures were put forward to prevent crimes.

Keywords: Apriori Algorithm; Data Mining; Internet Fraud; Supervision and Investigation

1 Introduction

With the maturity of Internet technology and the popularity of Internet terminals such as computers and mobile phones, the network has rapidly been integrated into our daily life [4]. The Internet has brought us a lot of convenience. Moreover, all aspects of the modern society cannot be separated from the Internet, for example, banking, traffic management and criminal investigation. However, in addition to bringing convenience to people's lives, it also provides a new space for criminals to commit crimes. As a virtual society, the network has many social characteristics; however, the information of users involved in network is unreal because of the virtual property of the network [16]. Criminals commit crimes, such as Internet fraud, by taking advantage of the virtual property of the network. Untrue information makes it very difficult to solve cases.

Many scholars have studied this aspect. Vlasselaer [15] proposed a method for detecting fraudulent credit card transactions on Internet stores. The method combined the characteristics of RFM based on customer transaction and the derived characteristics with the network characteristics of credit card holder and merchants to figure out the time-dependent suspicious score of each network object. The model combining two kinds of characteristics has good effect. Wu *et al.* [17] detected network identity fraud events on Facebook by analyzing the browsing behaviors of SNS users and found that the method could achieve a reasonable detection accuracy within a given observation time. Shen [10] carried out a deception detection experiment with three-stimulus guilty knowledge test paradigm under the simulated network fraud condition and put forward a multi-domain electroencephalography (EEG) signal processing method. The optimal subset was obtained using a genetic algorithm, and the linear discriminant analysis was used for classification. The results showed that the method was effective in detecting fraud under the simulated network fraud condition. In order to detect and prevent Internet fraud more accurately, this study performed association rule mining on the information in some Internet fraud case samples using the Apriori algorithm, and put forward the corresponding suggestions according to the rules.

2 Internet Fraud

2.1 Definition of Internet Fraud

With the rapid development of Internet technology, people's life has become more convenient, and has depended on the Internet more and more. Moreover, because of the non-face-to-face communication and anonymity on the Internet, it provides a hotbed for the new network crimes. Internet crime has emerged with the birth of the Internet. Although it emerged not too long ago, its harm to society is no less than that of traditional crimes. Internet fraud [7, 13] is a kind of Internet crimes. The crime of fraud is constantly changing with the development of the times and society, and the emergence of the network is a convenient tool for the illegal elements.

In general, Internet fraud is defined as the act of making up or concealing the facts through the network or

communication tools which rely on the Internet to achieve the illegal possession of a large amount of others' property, the word "Internet" has two connotations, Internet in broad sense and narrow sense. At present, there is no specialized classification of network fraud in China's criminal law [12]. The main reason is the wide range of network fraud. The content of fraud includes the categories of frauds described in the current criminal law, but it is difficult to be classified as a single category because of the use of the Internet [5].

2.2 Characteristics of Internet Fraud

The popularity of the Internet and computers has a profound impact on people's lives and also makes the network economy develop rapidly. The criminals also take the opportunity to implement fraudulent activities taking the advantage of network vulnerability. Based on the analysis of Internet fraud cases, the characteristics of Internet fraud are concluded as follows:

1) A wide range of crime objects [9]:
Traditional fraud is usually face to face; therefore, the victim of traditional fraud is often fixed, people in an age group or people who engage in some kind of job. However, after the emergence of network, fraudsters release false information regardless of cost and object via the Internet or the group chat function of communication tools such as QQ. It shows that the object of Internet fraud has changed from the single group to all netizens, i.e., the target of crime becomes more extensive.

2) Diversity of ways of crime:
As the Internet has been applied in different kinds of professional fields, people on the Internet engage in different kinds of works. Considering the wide range of crime object mentioned above, fraudsters may try to improve success rate by adopting different fraud means for different objects. Therefore, network fraud also has the feature of diversity. Moreover, the progress of network communication technology provides more network fraud tools for Internet fraud.

3) Professional crimes [2]:
In the early stage of the emergence of Internet fault, netizens were easy to be deceived by simple false information as they have not been familiar with it. However, with the increase of knowledge and the improvement of security awareness, the ability of netizens in identifying false information has also been improved. Fraudsters are more specialized in fabricating false information. Modern defrauders often have two skills: familiarity with the process of network business transactions and proficiency at computer programs.

4) Lowering trend of criminal age [8]:
The amount of information on the network is huge, but there is a lot of negative information. Young people who are shallow and immature and vulnerable to the temptation of bad information are more likely to commit crimes in pursuit of enjoyment. In recent years, the cases of Internet frauds in different regions show that the proportion of youngsters is increasing.

5) The concealment and continuity of fraud behaviors:
In Internet fraud, fraudsters only needs to send false information to victim, and the information sent through the network is not easy to be found. Therefore, the characteristics of fraudsters are difficult to know, and the backwardness of the network identity verification system makes virtual identity a protective umbrella of criminals. As for continuity, because the low implementation cost of Internet frau, it makes criminals feel less guilty.

6) Difficult evidence collection in detection process [14]:
Evidence collection is easy for traditional fraud because of the fixed objects and locations. However, for the network fraud, its concealment makes the crime process not easy to be found. Secondly, the dissemination and storage of its information is in the form of digital, which is very easy to be modified, hidden and deleted, and traces can be eliminated timely before exposure. In addition, because of the right to privacy of citizens, identity authentication on the network in the initial stage is very ambiguous, and most of the network identity information is not true. Once the criminals commit fraud with such an identity, the public security organs are difficult to collect evidences.

3 Apriori Algorithm

Apriori algorithm [3] put forward by Agrawal is used for searching the project relationship in database. It searches project relationship step by step and constantly repeats procedures of connection and pruning. Connection [6] means obtaining candidate set B_k by connecting frequent set M_k and M_{k-1}. Suppose $M_{k-1} = (m_1, m_2, \cdots, m_n)$, m_i, m_j, $(1 \le i \le n, 1 \le j \le n)$ are two elements of M_{k-1}, and $m_t[x]$ as the X-th item of m_t. Two elements in M_k and M_{k-1} can be connected, and moreover if m_i and m_j in M_{k-1} can be connected and $(m_i[m] = m_j[1]) \cap (m_i[2] = m_j[2]) \cap \cdots \cap (m_i[k-2] = m_j[k-2]) \cap (m_i[k-1] = m_j[k-1])$ when and only when the first $k-2$ element of the two elements are the same, then the result set generated after connection is $m_i[m]m_i[2] \cdots m_i[k-1]m_j[k-1]$. Pruning [11] means determining the count of each element in candidate set B_k through scanning database and eliminating elements with infrequent count. The remaining elements constitute a new frequent set M_k. The flow of Apriori algorithm [1] is shown in Figure 1.

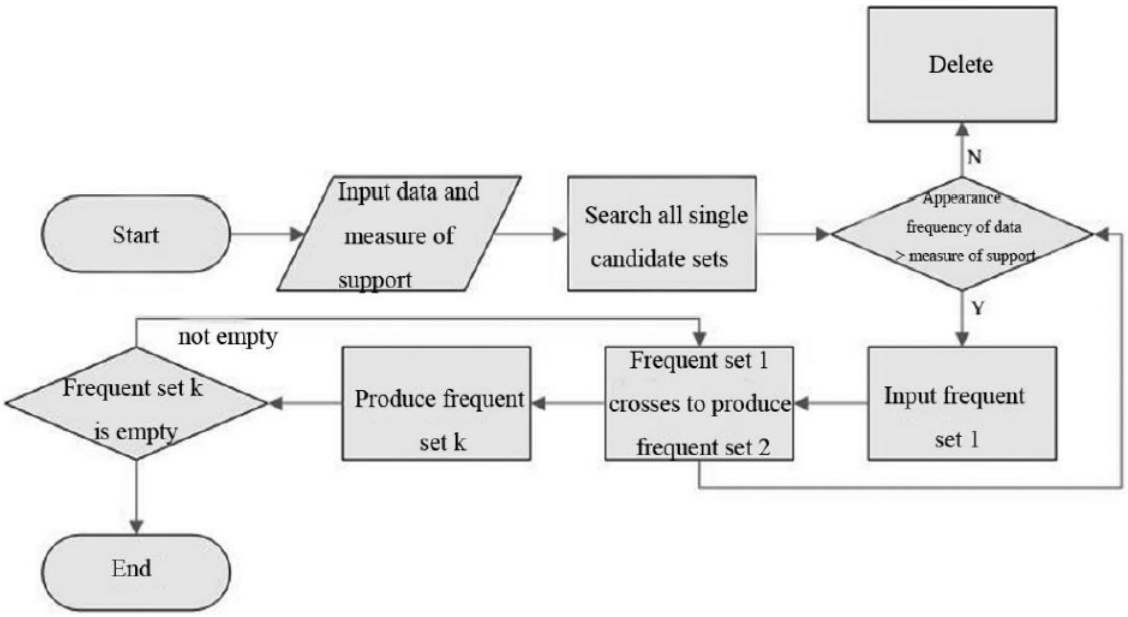


Figure 1: The flow of Apriori algorithm

4 Instance Analysis

With the continuous progress of information technology, the information processing of cases has been advanced. In the public security system, the functions of data processing have been relatively perfect, including recording, storage, classification-type query and static statistics of data, which greatly promote office efficiency, but it is difficult to make linking analysis of information between cases and explore the potential laws of cases. In order to deal with this problem and improve the detection rate of cases, Apriori algorithm was applied to search for information rules in cases.

4.1 Selection of Field

The information of network fraud cases in the database of the public security system was statistically analyzed, and the fields which appeared the most frequent were selected as the attribute values. After statistical analysis, crime scene, scope of crime, time of crime and number of criminals and degree of loss were selected as fields.

4.2 Data Preparation

The essential connection between different crimes and the law of committing crimes can be obtained through analyzing the information of cases. The information of some network fraud cases was selected from the case database of the public security department as the sample data according to the selected fields above. The content of the fields is shown in Table 1.

4.3 Establishment of Database

According to Table 1, the network fraud information was converted to the transaction database D. Crime scene was set as A; scope of crime was set as B; time of crime was set as C; scope of crime was set as D, and degree of loss was set as E. The subclassification was distinguished by number as shown in Table 2.

4.4 Data Mining

Association analysis was performed on the samples using Apriori algorithm, and the flow of the algorithm has been shown in the last section. In this study, the minimum support was set as 30%, the minimum confidence was set as 75%, and the measure of support was 3. Then the detailed data mining is as follows.

1) Candidate set B1 was obtained after performing scanning and statistics on Table 2 as shown in Figure 2.

2) The statistics of different item sets in Figure 2 were compared with measure of support; item sets whose statistics was smaller than 3 were deleted, and finally frequent set M1 was obtained as shown in Table 3.

   It could be found from Table 3 that C3, C4 and D1 were deleted, indicating that time of crime was at 16:00 22:00 and 22:00 4:00, and one criminal had a low association with the other information of the cases.

3) Item sets in frequent set M1 were combined in pairs, and then candidate set B2 was obtained as shown in Figure 3.

Table 1: The information of some network fraud cases

No.	Crime scene	Scope of crime	Time of crime	Number of criminals	Degree of loss
1	Residents community	Suburb	4:00-10:00	3	High
2	Bank	Suburb	22:00-4:00	2	Low
3	Bank	Urban area	16:00-22:00	1	High
4	Residents community	Suburb	10:00-16:00	2	High
5	Bank	Urban area	10:00-16:00	3	Low
6	Residents community	Urban area	10:00-16:00	3	Low
7	Residents community	Suburb	16:00-22:00	2	High
8	Residents community	Suburb	22:00-4:00	1	Low
9	Bank	Urban area	4:00-10:00	2	High
10	Residents community	Urban area	4:00-10:00	3	High

Table 2: Transaction database

No.	Crime scene	Scope of crime	Time of crime	Number of criminals	Degree of loss
1	A1	B1	C1	D3	E1
2	A2	B1	C4	D2	E2
3	A2	B2	C3	D1	E1
4	A1	B1	C2	D2	E1
5	A2	B2	C2	D3	E2
6	A1	B2	C2	D3	E2
7	A1	B1	C3	D2	E1
8	A1	B1	C4	D1	E2
9	A2	B2	C1	D2	E1
10	A1	B2	C1	D3	E1

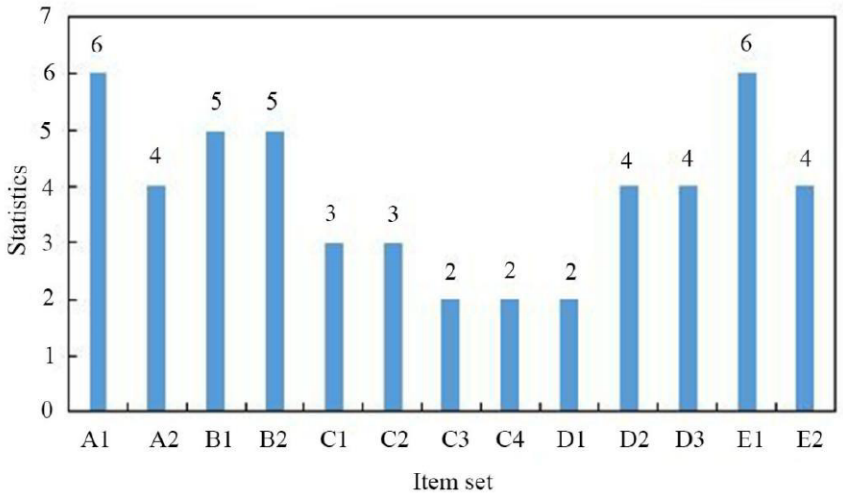


Figure 2: Candidate set B1

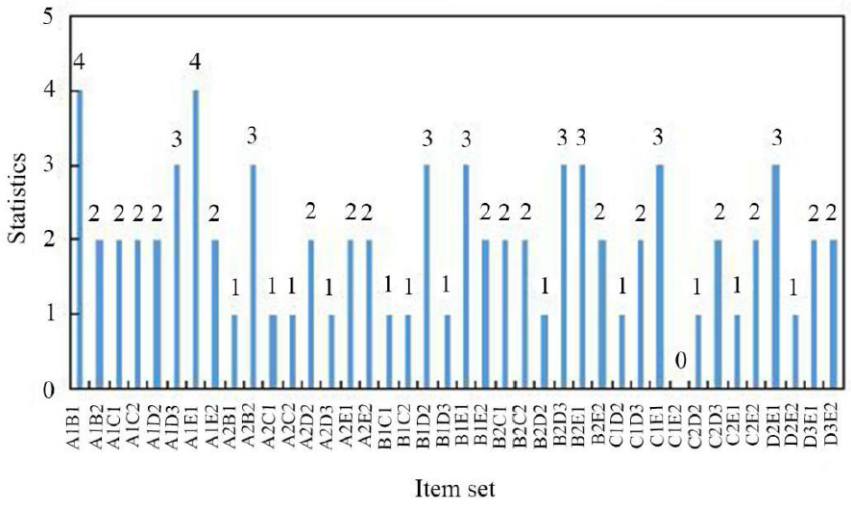


Figure 3: Candidate set B2

4) The statistics of the item sets in Figure 3 were compared with the measure of support; item sets whose statistics was smaller than 3 were deleted, and finally frequent set M2 was obtained, as shown in Table 4.

5) The item sets in frequent sets, M2 and M1, were combined in pairs, and then candidate set B3 was obtained as shown in Figure 4.

6) The statistics of the item sets in Figure 4 were compared with the measure of support; item sets whose statistics was smaller than 3 were deleted, and finally frequent set M3 was obtained, as shown in Table 5.

Frequent set M3 was the final output result, i.e., the potential law between the network fraud cases mined from the sample database, which was numbered A1B1E1; after the conversion according to Table 1, the law was that the loss of victims was high when network fraud crimes happened in residence community and suburb. According to this law, the public security department can pay more attention to the related information in the surrounding of residences communities in suburb, and take corresponding measures to prevent crimes, for example, through popularizing fraud prevention knowledge, reminding residents to use more complex, strong passwords in key settings to protect personal property, warning them not to disclose the password of bank cards, especially to the stranger, reminding residents who like online shopping not to do online transactions in public places, and not clicking on unidentified links sent by communication tools such as QQ or WeChat.

Table 3: Frequent set M1

Item set	Statistics	Item set	Statistics
A1	6	C2	3
A2	4	D2	4
B1	5	D3	4
B2	5	E1	6
C1	3	E2	4

Table 4: Frequent set M2

Item set	Statistics	Item set	Statistics
A1B1	4	B1E1	3
A1D3	3	B2D3	3
A1E1	4	B2E1	3
A2B2	3	C1E1	3
B1D2	3	D2E1	3

Table 5: Frequent set M3

Item set	Statistics
A1B1E1	3

5 Conclusion

This paper first introduced the definition of network fraud, summarized several characteristics of network

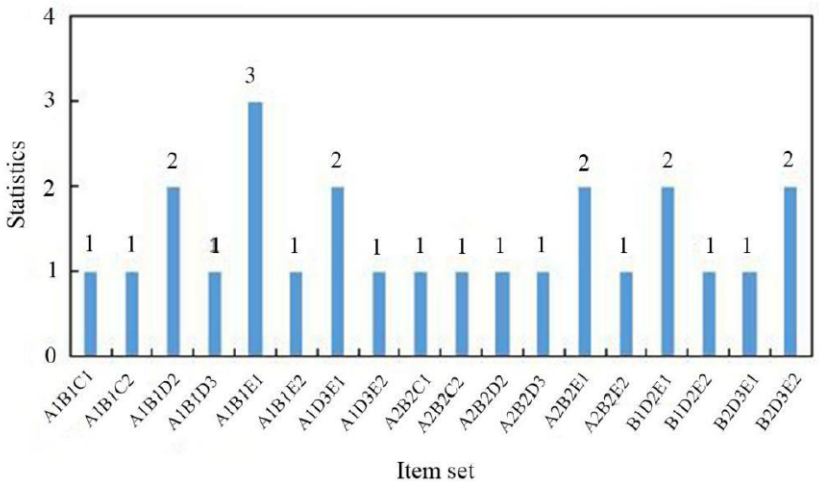


Figure 4: Candidate set B3

fraud, and performed association rules mining on the information of some network fraud case samples. The data attribute fields used for searching association rules are crime scene, scope of crime, time of crime, number of criminals and degree of loss. The inherent law found was that network fraud in residential communities in suburb will cause a higher loss. This rule provides a reference for preventing crimes and finding a way to solve cases, which can help the police arrange the police strength scientifically and rationally. Finally, several measures were put forward for preventing fraud.

References

[1] O. S. Adebayo, N. Abdulaziz, "Android malware classification using static code analysis and Apriori algorithm improved with particle swarm optimization," in *4th World Congress on Information and Communication Technologies (WICT'14)*, pp. 123–128, 2014.

[2] A. S. Bekirev, M. V. Kuzin, M. V. Kuzin, *et al.*, "Payment card fraud detection using neural network committee and clustering," *Optical Memory & Neural Networks*, vol. 24, no. 3, pp. 193–200, 2015.

[3] A. Bhandari, A. Gupta, D. Das, "Improvised apriori algorithm using frequent pattern tree for real time applications in data mining," *Procedia Computer Science*, vol. 46, pp. 644–651, 2015.

[4] K. M. Fanning, K. O. Cogger, "Neural network detection of management fraud using published financial data," *Intelligent Systems in Accounting Finance & Management*, vol. 7, no. 1, pp. 21–41, 2015.

[5] B. Hannibal, H. Ono, B. Hannibal, *et al.*, "Relationships of collapse: Network brokerage, opportunism and fraud in financial markets," *International Journal of Social Economics*, vol. 44, no. 12, pp. 2097–2111, 2017.

[6] A. Khalili, A. Sami, "SysDetect: A systematic approach to critical state determination for industrial intrusion detection systems using apriori algorithm," *Journal of Process Control*, vol. 32, no. 11, pp. 154–160, 2015.

[7] M. Nandhini, B. B. Das., "An assessment and methodology for fraud detection in online social network," in *IEEE International Conference on Science Technology Engineering and Management*, pp. 104–108, 2016.

[8] R. Puri, M. P. Hammer, D. Grottwassink, *Method and System for Defending a Mobile Network from a Fraud*, Patent WO/2016/148685, Sept. 22, 2016.

[9] T. Razooqi, P. Khurana, K. Raahemifar, A. Abhari, "Credit card fraud detection using fuzzy logic and neural network," in *Proceedings of the 19th Communications & Networking Symposium*, 2016.

[10] J. Shen, J. Liang, X. Liu, "P300-based deception detection in simulated network fraud condition," *Electronics Letters*, vol. 52, no. 13, pp. 1136–1138, 2016.

[11] A. K. Singh, A. Kumar, A. K. Maurya, "An empirical analysis and comparison of apriori and FP - growth algorithm for frequent pattern mining," in *International Conference on Advanced Communication Control and Computing Technologies*, pp. 1599–1602, 2015.

[12] J. R. Sun, M. L. Shih, M. S. Hwang, "Cases study and analysis of the court judgement of cybercrimes in Taiwan," *International Journal of Law, Crime and Justice*, vol. 43, no. 4, pp. 412–423, 2015.

[13] J. R. Sun, M. L. Shih, and M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure," *International Journal of Network Security*, vol. 17, no. 5, pp. 497–509, 2015.

[14] M. Uğurlu, S. Sevim, "Artificial neural network methodology in fraud risk prediction on financial statements; An emprical study in banking sector," *Journal of Business Research Turk*, vol. 7, no. 1, pp. 60–89, 2015.

[15] V. V. Vlasselaer, C. Bravo, O. Caelen, *et al.*, "APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions," *Decision Support Systems*, vol. 75, pp. 38–48, 2015.

[16] V. V. Vlasselaer, T. Eliassi-Rad, L. Akoglu, *et al.*, "GOTCHA! Network-based fraud detection for social security fraud," *Management Science*, vol. 63, no. 9, pp. 2773–3145, 2017.

[17] S. H. Wu, M. J. Chou, C. H. Tseng, *et al.*, "Detecting in situ identity fraud on social network services: A case study on facebook," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2432–2443, 2017.

Biography

Lei Zhang, born in November 1980, is now working in the department of investigation of Railway Police College, Henan, China. She has gained a master's degre from People's Public Security University of China, Beijing, China. She is interested in science of investigation and psychology.

Reviewers (Volume 20, 2018)

Bala Venkateswarlu Isunuri - Amandeep .
R CH A Naidu
Slim Abdelhedi
Mohd Faizal Abdollah
Ahmed Mohammed Abdullah
Malik Muneeb Abid
Subrata Acharya
Sodeif Ahadpou
Muhammad Najmi Ahmad Zabidi
Mohammad Reza Ahmadi
Asimi Ahmed
Mehrnaz Akbari Roumani
Abdul-Gabbar Tarish Al-Tamimi
Shahid Alam
Monjur M Alam
Sara Ali
Khalid Abdulrazzaq Alminshid
Rengarajan Amirtharajan
Karl Andersson
C. Annamalai
Benjamin Arazi
Razi Arshad
humaira ashraf
Travis Atkison
Cossi Blaise Avoussoukpo
Nazrulazhar Bahaman
saeed bahmanabadi
Anuj Kumar Baitha
Kavitha Balu
Tamer Mohamed Barakat
Pijush Barthakur
Eihab B Bashier
Eihab Bashier Mohammed Bashier
Adil Bashir
Sunny Behal
Akashdeep Bhardwaj
Sugandh Bhatia
Sajal Bhatia
Dharmendra Bhatti
Li Bin
Mitko Bogdanoski
amar buchade
Zhengjun Cao
Mukundha Ch
Chi-Shiang Chan
Eric Chan-Tin
Yogesh Chandra
Ya-Fen Chang
Ayantika Chatterjee
YI-Hui Chen
Chi-Hua Chen
Jan Min Chen
Chin-Ling Chen
Qingfeng Cheng
Hu Chengyu
Rachid Cherkaoui
Kaouthar Chetioui
Shu-Fen Chiou
MohamedSinnaiya ChithikRaja
Hassan Chizari
Tae-Young Choe
Kim-Kwang Raymond Choo
Yung-Chen Chou
Christopher P. Collins
Joshua C. Dagadu
Debasis Das
Ranjan Kumar Dash
Subhrajyoti Deb
Taher Delkesh
Pramod Bhausaheb Deshmukh
Abdelrahman Desoky Desoky
Subhasish Dhal
Nishant Doshi
Ahmed DRISSI
Qi Duan
Sherif M El-Kassas
Ahmed EL-Yahyaoui
Abd Allah Adel Elhabshy
Ahmed A. Elngar
Muawia A. Elsadig
Yousef Farhaoui
Arizona Firdonsyah
Yonggang Fu
Vladimir Sergeevich Galyaev
Rakesh C Gangwar
tiegang gao
Xinwei Gao
G. Geetha
Mohammad GhasemiGol
Ramesh Gopalan
Poornima Ediga Goud
Ke Gu
Rui Guo
Jatin Gupta
Arash Habibi Lashkari
Yasir Hamid
Abdallah Handoura
Charifa Hanin
Nareshkumar Dattatraya Harale
Seyed Hashemi
Ali Hassan
Wien Hong
Osama Hosam Eldeen
Tsung-Chih Hsiao
Yen-Hung Hu
Defa Hu
Yu-Chen Hu
Peng Hu
Chin-Tser Huang
Huajun Huang
Çiğir İlbaş
Remani Naga Venkata jagan mohan
Yogendra Kumar Jain
teena jaiswal
N Jeyanthi
Rong Jiang
Shaoquan Jiang
Rui Jiang
lin zhi jiang
Wang Jie
Lincy Elizebeth Jim
Ashish Joshi
Nandhini K
Arvind K S
Suganya K S
Omprakash Kaiwartya
Yoshito Kanamori
Nirmalya Kar
Vaishali D Khairnar

Asif Uddin Khan
Md. Al-Amin Khandaker
Malik Sikander Hayat Khiyal
vikas kolekar
Wei-Chi Ku
Pramote Kuacharoen
Beesetti Kiran Kumar
Vimal Kumar
K S Anil Kumar
Sajja Ratan Kumar
Yesem Kurt Peker
Jung-San Lee
Then Lee
Jiguo Li
Yunfa Li
Tzu-Chun Lin
Yang-Bin Lin
Chia-Chen Lin
Chih-Yang Lin
Guanfeng Liu
Auqib Hamid Lone
Yu Long
K. Shantha Kumari Luke
Jayakumar
Ming Luo
Lintao Lv
Sagar Bhaskar Mahajan
Tanmoy Maitra
Yassine Maleh
Arun Malik
Ali Mansouri
Mohd Zaki Mas'ud
Bo Meng
Suhail Qadir Mir
Amit Mishra
Pallaw Kumar Mishra
Anuranjan Misra
Belghachi Mohamed
Madihah Mohd Saudi
Guillermo Morales-Luna
Belmekki Mostafa
Hamdy M. Mousa
Phillimon Mwape Mumba
Zulkiflee Muslim
Ambika Nagaraj
Amin Nezarat
Vivian Ogochukwu Nwaocha
Nasrollah Pakniat
Siba Kumar Panda
Kailas Ravsaheb Patil
Suresh Kumar Peddoju
Edward Philemon
Emmanuel S Pilli
Kanthakumar Pongaliur
A Prakash
Mukesh Prasad
Septafiansyah Dwi Putra
Murad Abdo Rassam Qasm
Jiaohua Qin
Chuan Qin
Zhang Qiu-Yu
Kashif Naseer Qureshi
Uma Rani R
Anand R
Hashum Mohamed Rafiq
Kishore P C Raja
Mahalingam Ramkumar
Benjamin W. Ramsey
Anurag Rana
Dhivya Ravi
Siva Ranjani Reddi
Yeddula Venkatramana Reddy
Khaled Riad
Ou Ruan
Sandhya S
Prajwalasimha S N
Sanjay Kumar Sahay
Sabyasachi Samanta
Arif Sari
Arindam Sarkar
Balamurugan K S Sathiah
Michael Scott
Chandra Vorugunti Sekhar
Irwan Sembiring
Vrushank Shah
Tarun Narayan Shankar
Udhayakumar Shanmugam
Aditi Sharma
Varun Shukla
Jitendra Singh
Debabrata Singh
Anuj Kumar Singh
Rajeev Singh
V.Preetha Siva
Rajeev Sobti
C. Sreedhar
Bala Srinivasan
Deris Stiawan
Jeremy Straub
Karthikeyan Subramanian
Siva Shankar Subramanian
Haiyan Sun
Omkumar Sundaramoorthy
Sudalaimuthu T
Lathies Bhasker T
Manesh T
Fei Tang
Dan Tang
Maryam Tanha
Ariel Soares Teles
Lin Teng
Dr. Anitha Thangasamy
Miaomiao Tian
Xiuxia Tian
Geetam Singh Tomar
Yuan-Yu Tsai
Venkanna U
Subba Rao Y V
JANANI V S
Raghav V. Sampangi
Pushpendra Kumar Verma
Vandani Verma
Osman Wahballa
Ze Wang
Ying Wang
Li Wang
Ding Wang
Fangwei Wang
ZHE WEI
C. H. Wei
Fushan Wei
Na-I Wu
Xu Wu
Chenhuang WU
Degang Xu
Lei Xu
yashveer yadav
Prasant Singh yadav
Jun Ye
Huang Yiwang
Milad Yousefi
Qian Yu
Huifang Yu
Sherali Zeadally
Jianping Zeng
Zonghua Zhang
jie xiu zhang
Qianying Zhang
Yinghui Zhang
jianjun zhang

Yanshuo Zhang
Futai Zhang
Yi Zhao
Hongzhuan Zhao
Luo Zhiyong
Zhiping Zhou
Ye Zhu
Aaron Zimba

Guide for Authors
International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijns.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 7,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijns.jalaxy.com.tw or Email to ijns.publishing@gmail.com.