IJNS
International Journal of Network Security

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

Vol. 18, No. 3 (May 2016)

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

International Journal of Network Security

Vol. 18, No. 3 (May 1, 2016)

A Novel One-Time Identity-Password Authenticated Scheme Based on Biometrics for E-coupon System

Hongfeng Zhu, Yan Zhang and Xiaodan Wang
(Corresponding author: Hongfeng Zhu)

Software College & Shenyang Normal University of China
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C. 110034 - China
(Email:zhuhongfeng1978@163.com)
(Received Aug. 29, 2014; revised and accepted Mar. 23 & July 4, 2015)

Abstract

Nowadays, the application of e-coupons is quite a novel issue but is becoming increasingly popular among electronic commercial businesses owing to save much money by using the e-coupons. In this paper, a new robust biometrics-based one-time identity-password (OTIP) authenticated key agreement protocol is given for E-coupon system. Our proposed protocol adopts one-time password-authenticated algorithm, which is that a hash chain can update by itself smoothly and securely through capturing the secure bit of the tip, has the feature of high-efficient. In addition, biometrics-based algorithm can make the scheme become more secure and user friendly. The combination of above-mentioned algorithms can lead to a high-practical scheme in the universal client/server architecture. Security of the protocol is based on the biometric authentication and a secure one way hash function with the hash chain. At the same time the proposed protocol can not only refrain from many consuming algorithms, but is also robust to many kinds of attacks and owns much excellent features. Finally, we provide the secure proof and the efficiency analysis about our proposed scheme.

Keywords: Authentication, biometrics, e-coupon, one-time identity-password

1 Introduction

With the rapid development of mobile internet related to many service providers such as stock exchanging, commodity trading, and banking, many key agreement protocols have been studied widely. However, many authentication key agreement protocols used in M-commerce are designed for cable network and consume much communication rounds and computation costs, making them unfit for mobile internet surroundings. Furthermore, M-commerce are designed to satisfy user experience, especially for security and efficiency. So the paper purposes to design an authenticated key agreement scheme for E-coupon system which can achieve high-level security, high-efficiency and user friendly at the same time.

One time password (OTP) means that the password can be used only once. Nowadays, OTP has been widely used in the financial sector, telecommunications, online game field and so on. As a general rule, traditionally static password, for its security, can be easily stolen because of Trojan horse and keylogger program. It may also be cracked by brute force if an adversary spends enough time on it. Attackers can impersonate the legal user to communicate with the service server, and even modify the password of the legal user so that legal user cannot login the server. To address these conditions, OTP was developed as a solution. It is an approach to effectively protect the safety of the users.

Lamport [8] firstly put forward a method of user password authentication using a one way function to encode the password in 1981. Obviously, due to the higher safety request of the user, many schemes based on this method [4, 6, 11, 14, 16, 19, 21] have been proposed. In 2000, Tang [19] proposed a strong directed OTP authentication protocol with discrete logarithm assumption. In 2010, based on the use of OTP in the context of password-authentication key exchange (PAKE), which can offer mutual authentication, session key exchange, and resistance to phishing attacks, Paterson et al. [16] proposed a general technique which allows for the secure use of pseudorandomly generated and time-dependent passwords. In 2011, Fuglerud et al. [4] proposed an accessible and secure authentication way to log in to a banking server, which used a talking mobile OTP client rather than dedicated OTP generators. Later, Li et al. [11] proposed a two-layer authentication protocol with anonymous routing on small Ad-hoc devices. In 2012, Mohan et al. [14] proposed a new method using OTP to ensure that authenticating to

services, such as online shopping, was done in a very secure manner. In 2013, Huang et al. [6] proposed an effective simple OTP method that generates a unique passcode for each use. In Huang's method, OTP calculation used time stamps and sequence numbers. In addition, a two-factor authentication prototype for mobile phones using Huangs method has been used in practice for a year. In 2014, Xu et al. [21] proposed a self-updating OTP mutual authentication scheme based upon a hash chain for Ad hoc network. The updating process can be unlimited used without building a new hash chain.

However, these literatures [4, 6, 8, 11, 14, 16, 19, 21] only care about covering the password with one-time password. In fact, the identity information is equally important. Because an adversary can retrieve much useful information form the static identity by connecting with other information. Based on these motivations, the article presents a new simple biometrics-based one-time identity-password (OTIP) authenticated with key agreement protocol for mobile device using in E-coupon system between user and server to fit mobile internet communication setting. Compared with previous related protocols, the proposed scheme has the following more practical advantages: (1) it firstly presents the concept of one-time identity-password. (2) it provides a kind of biometric authentication function securely [10], (3) it provides simple and robust session key agreement by adopting one-time identity-passowrd, (4) it provides secure one-time identity-password and biometrics and Seed update function by using biometrics update protocol, and (5) it can decrease the total calculated amount and communication rounds due to the hash chain and Xored operation, (6) it is secure against well-known kinds of attacks.

The organization of the article is described as follows: some preliminaries are given in Section 2. Next, a biometrics-based one-time password-authenticated with key agreement scheme is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 Biometric Authentication

Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used. During the biometric collection phase, a biometric sample is collected, processed by a smart device, and stored which prepared for subsequent comparison. During the biometric authentication phase, the biometric system compares the stored sample with a newly captured sample. Obviously, smart device has powerful information confidentiality and flexible portability. When performing a biometric authentication process, a user inputs a smart device, and utilizes a simple finger touch or a glance at a camera to authenticate himself/herself [1, 3, 10].

2.2 Biometric Authentication

A secure cryptographic one-way hash function $h : a \to b$ has four main properties:

1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;

2) The function h is one-way in the sense that given a, it is easy to compute $h(a) = b$. However, given b, it is hard to compute $h^{-1}(b) = a$;

3) Given a, it is computationally infeasible to find a' such that $a' \neq a$,but $h(a') = h(a)$;

4) It is computationally infeasible to find any pair a, a' such that $a' \neq a$, but $h(a') = h(a)$.

2.3 Hard-Core Predicate

General speaking, a polynomial-time predicate b is called a hard-core of a function f if each efficient algorithm, given $f(x)$, can guess $b(x)$ with success probability that is only negligibly better than one-half.

Definition 1. *(Hard-Core Predicate) A polynomial-time-computable predicate $b : \{0,1\}^* \to \{0,1\}^n$ is called a hard-core of a function f for each probabilistic polynomial-time algorithm A', each positive polynomial $p(\cdot)$, and all sufficiently large n has $Pr[A'(f(U_n)) = b(U_n)] \leq \frac{1}{2} + \frac{1}{p(n)}$. U_n is a random variable uniformly distributed in $\{0,1\}^n$.*

2.4 Hash Chain

Definition 2. *(Hash Chain) Select a cryptographic secure hash function h with secure parameter $k : \{0,1\}^* \to \{0,1\}^k$. Pick a seed s randomly and apply h recursively N times to an initial seed s to generate a hash chain. The tip ω of the chain equals $h^N(s)$.*

$$\omega = h^N(s) = h(h^{N-1}(s)) = \underbrace{h(h(h(\cdots h(s))))}_{N \quad Times}$$

2.5 RSA Cryptography

Rivest, Shamir, and Adleman first designed the RSA cryptography system in 1977. Subsequently, several other researchers began to use the RSA system to accomplish the applications of digital signature and data encryption. In the RSA system,we can generate two keys - a public key and a private key. The keys can easily be built between Entity C as follows:

C first chooses two different large prime numbers p, q and computers $n = pq$. Then, C generates e that satisfies $\gcd(e,(n)) = 1$, where $\varphi(n) = (p-1)(q-1)$. Finally C can get d from computing $ed \equiv 1 \bmod \varphi(n)$.

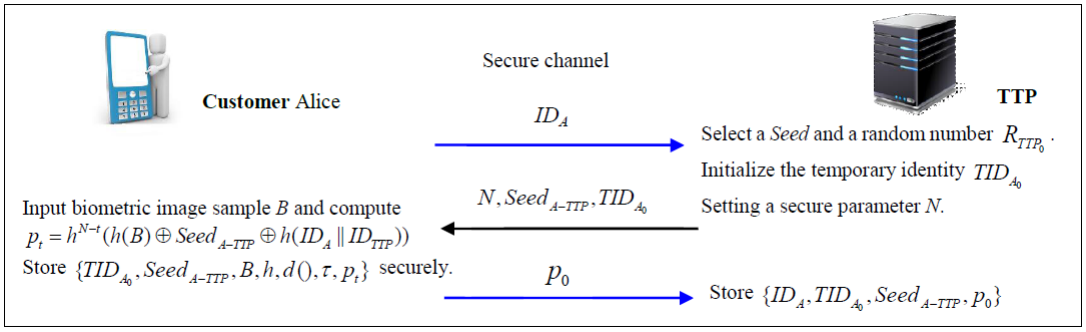


Figure 1: User registration phase (Customer Alice as an example)

As mentioned above, (n, e) is the public key and (p, q, d) is the private key. To protect the integrity of the message, the signer can use the private key to sign the message as $(m)^d$ and the verifier can use the signature and public key to check the integrity of the message m as $((m)^d)^e = (m)^{ed} \mod n = m$.

3 The Proposed Protocol

In this section, biometrics-based one-time identity-password authenticated key agreement scheme is proposed which consists of three phases: the user registration phase, authenticated key agreement phase and the Seed and one-time password update phase (because the temporary identity is updated in every authenticated key agreement phase). But firstly some notations are given which used in the proposed scheme.

3.1 Notations

The concrete notation used hereafter is shown in Table 1.

3.2 User Registration Phase

We assume that the user can register at his appointed server in some secure way or by secure channel. Figure 1 illustrates the user registration phase.

Step 1. When a user Alice wants to be a new legal user, she chooses her identity ID_A at liberty and sends it to the trusted third party **TTP** with some her necessary information.

Step 2. Upon receiving the request from Alice, TTP selects a $Seed$, a random number R_{TTP_0} and setting a secure parameter N. Then **TTP** initialize the temporary identity TID_{A_0} and computes $h(R_{TTP_0})$, $Seed_{A_{TTP}} \oplus R_{TTP_0}$ and sends $\{N, Seed_{A_{TTP}}, TID_{A_0}\}$ to Alice via a secure channel.

Step 3. Upon receiving the message $\{N, Seed_{A_{TTP}}, TID_{A_0}\}$, Alice inputs her personal biometric image sample B at the mobile device. Then Alice computes $p_t = h^{N-1}(h(B) \oplus Seed_{A_{TTP}} \oplus h(ID_A||ID_{TTP}))$ and submits P_0 to **TTP** via a secure channel. Finally Alice's mobile device stores $\{TID_{A_0}, Seed_{A_{TTP}}, B, h, d(), \tau, p_t(0 \le t \le N)\}$ securely, where $d(\cdot)$ is a symmetric parametric function and τ is predetermined threshold for biometric authentication. The parameter t is the reverse counter of the chosen hash chain: when $t = 0$, the $h^N()$ of hash chain is the first instance used in the proposed protocol. When $t = N - 1$, the $h^{N-(N-1)}() = h()$ of hash chain is the last used instance in our proposed protocol.

Step 4. Upon receiving the message $\{p_0\}$, **TTP** stores $\{ID_A, TID_{A_0}, Seed_{A_{TTP}}, p_0\}$ securely.

Remark 1. *In brief, the* **SHOP S** *can be as a user to registration on the* **TTP** *server. The only difference comparison with the customer Alice registration on the* **TTP** *server is the notations's subscripts, such as* $Seed_{S_{TTP}}$, ID_S, TID_{S_0} *and so on.*

3.3 Issue E-coupon Phase

Shop S has the biometric sample B^*, and her mobile device $(Seed, B, h, d(), \tau, p_t, TID_{A_t-1})$. **TTP** securely kept the secret information $\{Seed_{S_{TTP}}, p_{t-1}, TID_{S_{t-1}}, ID_s\}$. The concrete process is presented in the following Figure 2.

Step 1. If Shop **S** wishes to establish a session key with **TTP**, she imprints biometric B^* at the mobile device with her ID_S. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \ge \tau$, which means Shop **S** will get a connection refused response. If $d(B^*, B) < \tau$, which means Shop **S** will get a connection accepted response. Then the mobile device selects random R_{S_t}(the same length with $Seed_{S_{TTP}}$) and e-coupon z, then computes: $C_1 = M(Seed_{S_{TTP}}) \oplus M(R_{S_t}||ID_S||ID_{TTP}||z)$. After that, the mobile device sends $m_1 = \{TID_{S_{t-1}}, C_1\}$ to the **TTP**.

Table 1: Notations

Symbol	Definition
ID_A, ID_S ID_{TTP}	The identity of a user and the shop and the TTP server, respectively
TID_{A_t}	The temporary identity of Alice
R_{A_x}, R_{S_x}	Nonces
B	The biometric sample of user
τ	Predetermined threshold for biometric verification
$d(\cdot)$	Symmetric parametric function
h	A secure one-way hash function
$Seed$	An initial seed s to generate a hash chain by the TTP server
$\|\|$	Concatenation operation
$\oplus$	XORed operation
z	E-coupon
t	The reverse counter of the chosen hash chain by the server
$M(\cdot)$	Make both sides of XORed operation become the same length.

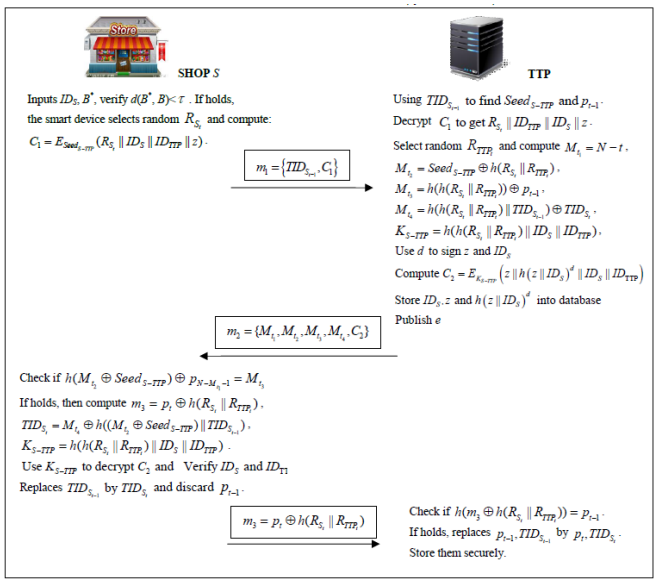


Figure 2: Issue e-coupon phase in our proposed scheme

Step 2. After receiving the message $m_1 = \{TID_{S_{t-1}}, C_1\}$ from S, **TTP** will do the following tasks:

1) Using $TID_{S_{t-1}}$ to find $Seed_{S_{TTP}}$ and p_{t-1} and decrypt C_1 to get $R_{S_t}||ID_{TTP}||ID_S||z$.
2) Selects random R_{TTP_t} and computes $M_{t_1} = N - t$, $M_{t_2} = Seed_{S_{TTP}} \oplus h(R_{S_t}||R_{TTP_t})$, $M_{t_3} = h(h(R_{S_t}||R_{TTP_t})) \oplus p_{t-1}$, $M_{t_4} = h(h(R_{S_t}||R_{TTP_t})||TID_{S_{t-1}}) \oplus TID_{S_t}$, $K_{S_{TTP}} = h(h(R_{S_t}||R_{TTP_t})||ID_S||ID_{TTP})$.
3) Use d to sign z and ID_S. Compute $C_2 = M(K_{S_{TTP}} \oplus M(z||h(z||ID_S)^d||ID_S||ID_{TTP}))$. Store ID_S, z and $h(z||ID_S)^d$ into database and publish e. Finally **TTP** sends the message $m_2 = \{M_{t_i}(i = 1, 2, 3, 4), C_2\}$ to **S**.

Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, C_2\}$, **S** will check if $h(M_{t_2} \oplus Seed_{S_{TTP}}) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, **S** terminates it simply. Otherwise that means **S** authenticates **TTP** in this instance. Then **S** computes $m_3 = p_t \oplus h(R_{S_t}||R_{TTP_t}$, $TID_{S_t} = M_{t_4} \oplus h((M_{t_2} \oplus Seed_{S_{TTP}})||TID_{S_{t-1}})$, $K_{S_{TTP}} = h(h(R_{S_t}||R_{TTP_t})||ID_S||ID_{TTP})$ and deletes p_t. Use $K_{S_{TTP}}$ to decrypt C_2 and verify ID_S and $IDTTP$. Finally **S** replaces $TID_{S_{t-1}}$ by TID_{S_t} and sends $m_3 = p_t \oplus h(R_{S_t}||R_{TTP_t})$ to **TTP**.

Step 4. After receiving m_3, **TTP** computes $p'_{t-1} = h(m_3 \oplus h(R_{S_t}||R_{TTP_t}))$ and verifies whether $p'_{t-1} = p_{t-1}$ or not. If it does not hold, **TTP** terminates it. Otherwise, **TTP** replaces p_{t-1},$TID_{S_{t-1}}$ by p_t,TID_{S_t} and stores them securely.

3.4 Download E-coupon Phase

Alice has the biometric sample B^*, and her mobile device ($Seed_{A_{TTP}}$,B,h,$d()$,τ,p_t,τ,$TID_{A_{t-1}}$). **S** securely kept the secret information $\{Seed_{A_{TTP}}, p_{t-1}, TID_{A_{t-1}}, ID_A\}$. This concrete process is presented in Figure 3.

Step 1. If Alice wishes to download e-coupon from **TTP**, she imprints biometric B^* at the mobile device with her ID_A. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, which means Alice will get a connection refused response. If $d(B^*, B) < \tau$, which means Alice will get a connection accepted response. Then the mobile device selects random R_{A_t}(the same length with $Seed$) and computes $C_1 = Seed_{A_{TTP}} \oplus R_{A_t}$. After that, the mobile device sends $m_1 = \{TID_{A_{t-1}}, C_1\}$ to the **TTP**.

Step 2. After receiving the message $m_1 = \{TID_{A_{t-1}}, C_1\}$ from Alice, **TTP** will do the following tasks:

1) Using $TID_{A_{t-1}}$ to find $Seed_{A_{TTP}}$ and p_{t-1} and decrypt C_1 to get R_{A_t}.

2) Selects random R_{TTP_t} and computes

$$\begin{aligned} M_{t_1} &= N-t, \\ M_{t_2} &= Seed_{A_{TTP}} \oplus h(R_{A_t}||R_{TTP_t}), \\ M_{t_3} &= h(h(R_{A_t}||R_{TTP_t})) \oplus p_{t-1}, \\ M_{t_4} &= h(h(R_{A_t}||R_{TTP_t})||TID_{S_{t-1}}) \\ &\quad \oplus TID_{A_t}, \\ K_{A_{TTP}} &= h(h(R_{A_t}||R_{TTP_t})||ID_A||ID_{TTP}). \end{aligned}$$

3) Use ID_S to find z and $h(z||ID_S)^d$, $C_2 = M(K_{A_{TTP}}) \oplus M(z||h(z||IDs)^d||ID_A||ID_{TTP})$. Finally **TTP** sends the message $m_2 = \{M_{T_1}, M_{T_2}, M_{T_3}, M_{T_4}, C_2\}$ to Alice.

Step 3. After receiving the message $m_2 = \{M_{T_1}, M_{T_2}, M_{T_3}, M_{T_4}, C_2\}$, Alice will check if $h(M_{t_2} \oplus Seed_{A_{TTP}}) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, Alice terminates it simply. Otherwise that means Alice authenticates **TTP** in this instance. Then Alice computes $m_3 = p_t \oplus h(R_{A_t}||R_{TTP_t}$, $TID_{A_t} = M_{t_4} \oplus h((M_{t_2} \oplus Seed_{A_{TTP}})||TID_{A_{t-1}})$, $K_{A_{TTP}} = h(h(R_{A_t}||R_{TTP_t})||ID_A||ID_{TTP})$ and deletes p_t. Use $K_{A_{TTP}}$ to decrypt C_2 and verify ID_A and $IDTTP$. Then Alice gets z and $h(z||ID_S)^d$. Next Alice replaces $TID_{A_{t-1}}$ by TID_{A_t} and sends $m_3 = p_t \oplus h(R_{A_t}||R_{TTP_t})$ to **TTP**. Finally Alice can use the E-coupon z and $h(z||ID_S)^d$ at anytime.

Step 4. When **TTP** obtains m_3, **TTP** computes $p'_{t-1} = h(m_3 \oplus h(R_{A_t}||R_{TTP_t}))$ and verifies whether $p'_{t-1} = p_{t-1}$ or not. If it does not hold, **TTP** terminates it. Otherwise, **TTP** replaces p_{t-1} by p_t to store p_t securely.

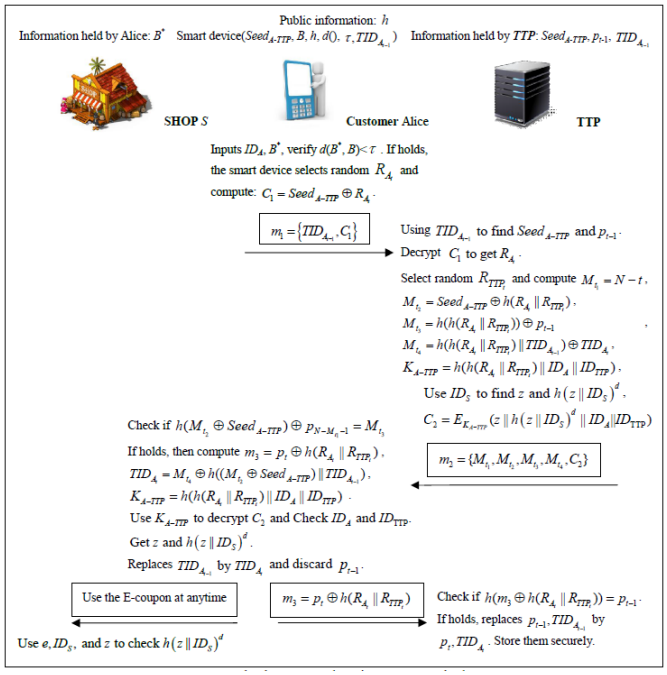


Figure 3: Download e-coupon phase in our proposed scheme

3.5 The Seed and One-time Password Update Phase

Figure 4 illustrates biometrics and password update phase. The steps are performed during the Seed and one-time password update phase as follows.

Step 1. When $t = N-1$, a user (Alice or Shop **S**) and **TTP** need to update the $Seed$ and one-time password at the same time. The user imprints biometric B^* at the mobile device. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, which means the user will get a connection refused response. If $d(B^*, B) < \tau$, which means the user will get a connection accepted response. Then the user inputs her ID_A, and the mobile device selects random $R_{A_{N-1}}$ and computes: $R_{A_{N-1}} \oplus Seed$. After that, the mobile device sends $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$ to **TTP**.

Step 2. After receiving the message $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$ from the user, **TTP** will do the following tasks:

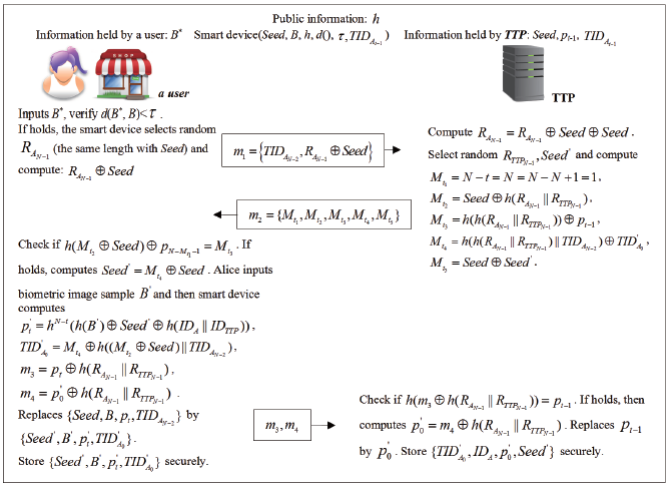


Figure 4: The Seed and one-time integrated information update phase (when $t = N-1$)

Table 2: Definition and simplified proof

Category	Security Attributes	Definition	Simplified Proof
Security threats can be wiped out owing to shift static identity-password to dynamic identity-password	Guessing attacks (On-line or off-line)	In an off-line guessing attack, an attacker guesses a password or long-term secret key and verifies his/her guess, but he/she does not need to participate in any communication during the guessing phase. In an undetectable on-line guessing attack, an attacker searches to verify a guessed password or long-term secret key in an on-line transaction and a failed guess cannot be detected and logged by the server.	There is no fixed password at all. And the mobile device authenticated Alice only by Alice's personal biometric image sample B.
	Privacy protection	A user may use a resource or service without disclosing the user's identity during the protocol interaction.	For all the transmitted messages, there is no useful information about users or **TTP**.
	Impersonation attack	An adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.	An attacker doesn't know the identity of the user at all, and he gets the temporary identities which are nothing but some random numbers.
	Man-in-the-middle attack(MIMA)	This is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.	The $m_i (1 \le i \le 3)$ contain the secret *Seed* and the nonces, a man-in-the-middle attack cannot succeed.
	Replay attack	A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.	Any replay attack can't be carried out, because the temporary identity can be used only once.
Immune to the security threats owing to adopt biometrics authentication	Key Compromise Impersonation Attacks (KCI attacks)	An adversary is said to impersonate a party B to another party A if B is honest and the protocol instance at A accepts the session with B as one of the session peers but there exists no such partnered instance at B [7].	There is no password at all and the mobile device authenticated user only by user's personal biometric image sample B.
	Losting smart device and guessing attacks	An adversary gets the user's smart device and then carries out the guessing attacks.	Anyone including an adversary cannot pass the biometric verification.
Resist the security threat owing by nonces	Mutual authentication	Mutual authentication refers to two parties authenticating each other suitably and simultaneously.	Either **TTP** or the user can authenticate the other based on secret *Seed*.

1) Compute $R_{A_{N-1}} = R_{A_{N-1}} \oplus Seed \oplus Seed$;
2) Selects random $R_{TTP_{N-1}}$, $Seed'$ and computes $M_{t_1} = N-t$, $M_{t_2} = Seed \oplus h(R_{A_{n-1}} || R_{TTP_{N-1}})$, $M_{t_3} = h(h(R_{A_{N-1}} || R_{S_{TTP-1}})) \oplus p_{t-1}$, $M_{t_4} = h(h(R_{A_{N-1}} || R_{TTP_{N-1}}) || TID_{A_{N-2}}) \oplus TID'_{A_0}$ and $M_{t_5} = Seed \oplus Seed$.

Finally **TTP** sends the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$ to the user.

Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$, the user will check if $h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1} = m_{t_3}$. If the equation does not hold, the user terminates it simply. Otherwise that means the user authenticates **TTP** in this instance. The user inputs biometric image sample B' and then mobile device computes $p' = h^{N-t}(h(B') \oplus Seed' \oplus h(ID_A))$, $TID'_{A_0} = M_{t_4} \oplus h((M_{t_2} \oplus Seed) || TID_{A_{N-2}})$, $m_3 = p_t \oplus h(R_{A_{N-1}} || R_{TTP_{N-1}})$ and $m_4 = p'_0 \oplus h(R_{A_{N-1}} || R_{TTP_{N-1}})$. Next the user sends m_3, m_4 to **TTP**. Finally the user's mobile device will replaces $\{Seed, B, p_t, TID_{A_{N-2}}\}$ by $\{Seed', B', p'_t, TID'_{A_0}\}$ and stores $\{Seed', B', p'_t, TID'_{A_0}\}$ securely.

Step 4. When **TTP** obtains m_3, m_4, **TTP** computes $p'_{t-1} = h(m_3 \oplus h(R_{A_{N-1}} || R_{TTP_{N-1}}))$ and verifies whether $p'_{t-1} = p_{t-1}$ or not. If it does not hold, **TTP** terminates it. Otherwise, **TTP** computes $p'_0 = m_4 \oplus h(R_{A_{N-1}} || R_{TTP_{N-1}})$ to replace p_{t-1} by p'_0 for storing $\{TID'_{A_0}, ID_A, p'_0, Seed'\}$ securely.

4 Security Consideration

The section analyzes the security of our proposed protocol. Let us assume that there are two secure components, including a secure one-way hash function and a secure symmetric encryption. Stored information, especially for seed, can be reserved in a secure way. Assume that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. The definitions and analysis of the security requirements [12, 13, 17, 20] will be illustrated in this section.

Remark 2. *Because there is no session key in our proposed scheme, so some security threats (such as known-key security, perfect forward secrecy and session key security and so on) need not to analyze. We can draw a conclusion that the proposed scheme provided one-time identity-password feature which can wipe out many attacks relating the static identity and static password. At the same time, our proposed protocol prevents the KCI attacks owing to OTIP mechanism. From the Table 2, we can see that the proposed scheme can provide privacy protection, mutual authentication and so on.*

5 Efficiency Analysis

In our proposed protocol, no time-consuming modular exponentiation and scalar multiplication on elliptic curves are needed.

Table 3 shows the computational cost of our proposed scheme and the comparisons between our proposed scheme and Chang's scheme of [2]. Therefore, as in Table 3, we can draw a conclusion that the proposed scheme has the lowest computational costs and is well suited to the mobile device applications. Here, the operations used in our proposed scheme include symmetric encryption/decryption **(S)**, asymmetric encryption/decryption **(As)**, Chebyshev chaotic maps operation **(Ch)**, the one-way hash function **(H)**, and biometric authentication **(BA)**.

Table 3: Computational cost of our proposed scheme and comparisons with [2]

Phase	Entity	Cryptography operation[2] (2014)					Our Proposed Scheme				
		S	*As*	*Ch*	*H*	*BA*	*S*	*As*	*Ch*	*H*	*BA*
① User registration phase	Shop	0	0	0	2	0	0	0	0	*N*+2	1
	Alice	0	0	0	2	0	0	0	0	*N*+2	1
	TTP	2	0	1	2	0	0	0	0	0	0
② Issue e-coupon phase	Shop	2	0	3	2	0	0	0	0	5	1
	TTP	3	1	2	0	0	0	1	0	5	0
③ Download e-coupon phase	Alice	2	0	3	2	0	0	0	0	5	1
	TTP	3	0	2	0	0	0	0	0	4	0
④ App recondition phase	Shop	0	1	0	0	0	0	1	0	0	1
	Alice	0	0	0	2	0	0	0	0	0	1
	TTP	1	0	1	2	0	0	0	0	0	0
⑤ Password renovation phase	User (Alice/Shop)	0	0	0	3	0	0	0	0	*N*+5	1
	TTP	1	0	0	3	0	0	0	0	4	0
Total		14	2	13	22	0	0	2	0	3*N*+32	7

Figure 5 illustrates the concrete values with the N changing between our proposed scheme and Chang's scheme of [2]. We compared the computation of symmetric encryption/decryption, Chebyshev chaotic maps operation and the one-way hash function. There are two reasons to exclude asymmetric encryption/decryption and biometric authentication: one side, its the same calculation times with asymmetric encryption/decryption for our protocol and the literature [2]. On the other side, the computation process of biometric authentication adopts dedicated hardware which can make biometric authentication complete quickly with a good user experience.

So we divided the total computations into two steps:

1) The first step including ① user registration phase and ⑤ password renovation phase which can only be used once. $(10T_H+1T_{CH}+3T_S)$ is the computations of [2] and $(13T_H+3NT_H)$ is the computations of our proposed scheme. Where T_H, T_{CH}, T_S means he time for executing the hash function, Chebyshev chaotic maps operation and symmetric encryption/decryption.

2) The second step including ② Issue e-coupon phase, ③ Download e-coupon phase and ④ App recondition phase which can be used $(N-1)$ times. $(8T_H+11T_{CH}+11T_S)$ is the computations of [2] and $19T_H$ is the computations of our proposed scheme at a time. So the difference of total calculated amount between literature [2] and our proposed scheme $(Total_{TD})$ is:

$$\begin{aligned} Total_{TD} &= Total_{[2]} - Total_{our} \\ &= (10T_H + 1T_{CH} + 3T_S) - (13T_H \\ &\quad +3NT_H) + (N-1)[(8T_H + 11T_{CH} \\ &\quad +11T_S) - 19T_H] \\ &= N(11T_{CH} + 11T_S - 14T_H) - 10T_{CH} \\ &\quad -8T_S + 8T_H. \end{aligned}$$

where $Total_{[2]}$ denotes the computations of [2], $Total_{our}$ denotes the computations of our protocol.

In Chang et al. [2] scheme, they coded a C language program of hash function, they input a 512-bit random string and implemented the program 10,000 times in a Window 7 workstation with an AMD X4 945 processor running at 3.00GHZ, 8192MB of RAM, and a 7200 RPM Western Digital WD5000AAKS-22V1A0465 GB ATA drive. They showed that the average time for one hash value was 0.605ms. In [18], Lee showed that one hash function operation was about one time faster than one Chebyshev chaotic maps operation. We can draw a conclusion that the average time for one Chebyshev chaotic maps operation was about 1.21ms. In addition, according to [9], we can come to a conclusion that one hash function operation is about 10 times faster than a symmetric encryption/decryption. So a symmetric encryption/decryption operation was about 6.05ms. Moreover, the computational cost of XOR operation could be ignored when compared with other operations.

So we have $1T_S \approx 10T_H$, $1T_{CH} \approx 2T_H$. Then we have:

$$\begin{aligned} Total_{TD} &= Total_{[2]} - Total_{our} \\ &= N(11T_{CH} + 11T_S - 14T_H) - 10T_{CH} \\ &\quad -8T_S + 8T_H \\ &\approx N(22T_H + 110T_H - 14T_H) - 20T_H \\ &\quad -80T_H + 8T_H \\ &= (118N - 92)T_H. \end{aligned}$$

That means our proposed scheme (even if $N = 1$) has much more efficient than the literature [2]. With the N increases linearly, our proposed schemes cost of computation will decrease linearly comparing with the literature of [2].

Figure 5 Total difference between the amount of computations between literature [2] and our proposed scheme As for store space, our proposed scheme just need 62.5K (assume $p_t = 128bits$, and $N = 500$). It is can be ignored at present contrasting to the TeraBit storage. Table 4 compares the functionalities and system efficiency of our proposed protocol and other, related coupon schemes [2, 5, 15]. The results of the comparisons show that our proposed scheme provides more functionalities, and is more suit for user-friendliness system.

Table 4: Comparisons between the related protocols and our proposed protocol

	[2] (2014)	[5] (2008)	[15] (2013)	Our scheme
System completeness	Very Good	Ordinary	Ordinary	Very Good
Digital signature	PKI-based	N/A	N/A	PKI-based
	Good	Weak	Weak	Good
Efficiency	CMs-based	Hash-based	XOR-based	Hash Chain-based
	Good	Very Good	Excellent	Very Good
Communication-rounds				
Registration	2	2	2	3
Authentication	3	2	2	3
Privacy protection	Good	Weak	Ordinary	Excellent

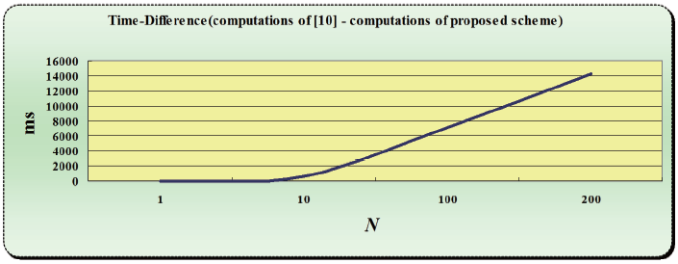


Figure 5: Total difference between the amount of computations between literature [2] and our proposed scheme

6 Conclusion

The paper proposed a novel and complete biometrics-based and one-time identity-password authentication scheme for e-coupon systems. There are many advantages about our protocol which described as follow: Firstly, from the standpoint of a security analysis, our scheme uses biometrics method and dynamic ID-password to achieve high-level security. Then, along with one-time password, we insert the dynamic ID which can consume the almost negligible computations, communications and size of memory. It is efficient method at least cost. Next, the core ideas of the proposed scheme are the features of security and efficiency in the mobile device and servers side, and the feature of user friendly for the users side. Finally, through comparing with recently related work, our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications.

References

[1] M. Aigner, S. Dominikus, and M. Feldhofer, "A system of secure virtial coupons using NFC technology," in *Proceedings of IEEE International Conference on Pervasive Computing and Communication Workshops*, pp. 362–366, 2007.

[2] C. C. Chang, C. Y. Sun, "A secure and efficient authentication scheme for E-coupon systems," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2981–2996, 2014.

[3] S. Dominikus, and M. Aigner, "mCoupons: An application for near field communication (NFC)," in *Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshops* , pp. 421–428, 2007.

[4] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 27-34, 2011.

[5] H. C. Hsiang, and W. K. Shih, "Secure mCoupons scheme using NFC," in *Proceedings of the International Conference on Business and Information*, pp.115–121, 2008.

[6] Y. Huang, Z. Huang, H. R. Zhao and X. J. Lai, "A new one-time password method," in *Informational Conference on Electronic Engineering and Computer Science*, pp. 32–37, 2013.

[7] J. Katz, J. S. Shin, "Modeling insider attacks on group key-exchange protocols," in *Proceedings of the 12th ACM Conference on Computer and Communications Security (CS'05)*, pp. 180–189, 2005.

[8] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[9] C. C. Lee, "A simple key agreement scheme based on chaotic maps for VSAT satellite communications," *International Journal of Satellite Communications and Networking*, vol. 31, no. 4, pp. 177–186, 2013.

[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. T. Li and 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, 2011.

[12] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architec-

ture using neural networks," *IEEE Transactions on Neural Networks*, vol. 12, no.6, pp. 1498–1504, 2001.
[13] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003
[14] R. Mohan and N. Partheeban, "Secure multimodal mobile authentication using one time password," *International Journal of Recent Technology and Engineering*, vol. 1, no. 1, pp. 131–136, 2012.
[15] S. W. Park, and I. Y. Lee, "Efficient mCoupon authentication scheme for smart poster environments based on low-cost NFC," *International Journal of Security and its Applications*, vol. 7, no. 5, pp. 131–138, 2013.
[16] K. G. Paterson, G. Kenneth and D. Stebila, "One-time password authenticated key exchange," in *Proceedings of 15th Australasian Conference on Information Security and Privacy*, pp. 264–281, 2010.
[17] R. S. Pippal, C. D. Jaidhar, S. Tapaswi, "Robust smart card authentication scheme for multi-server architecture," *Wireless Personal Communications*, vol. 72, no. 1, pp. 729–745, 2013.
[18] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C (2nd ed.)*, John Wiley & Sons, 1996.
[19] S. H. Tang, "Directed one-time password authentication scheme based upon discrete logarithm," *Journal of Circuits, Systems and Computes*, vol. 10, no. 3, pp. 173–180, 2000.
[20] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," *Computers & Security*, vol. 27, no. 3-4, pp. 155–121, 2003.
[21] F. Xu, X. Lv, Q. Zhou and X. Liu, "Self-updating one-time password authentication protocol for adhoc network," *Transactions on Internet and Information Systems*, vol. 8, no. 5, pp. 1817–1827, 2014.

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate 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. Dr. Zhu had published more than 50 international journal and international conference papers on the above research fields.

Yan Zhang 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.

Xiaodan Wang is a lecturer of the Kexin software college at Shenyang Normal University. She graduated from the Shenyang Institute of computing, Chinese Academy of Sciences of computing technology in 2011, and got the master degree of Engineering. Xiaodan Wang committed to professional teaching and research work for many years, accumulated rich experience in teaching and research, mainly engaged in network technology, information security, network programming and research direction. She has received provincial and university teaching awards.

A Reversible Data Hiding Scheme Based on IWT and the Sudoku Method

Fan Li[1], Qian Mao[1,2], and Chin-Chen Chang[2,3]
(Corresponding author: Chin-Chen Chang)

School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology[1]
516, Jungong Road, Yangpu, Shanghai 200093, P. R. China
Department of Computer Science and Information Engineering, Asia University[2]
500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan
Department of Information Engineering and Computer Science, Feng Chia University[3]
100, Wenhwa Road, Seatwen, Taichung 40724, Taiwan
(Email: alan3c@gmail.com)
(Received Oct. 15, 2013; revised and accepted Feb. 17 & Mar. 13, 2014)

Abstract

A reversible data hiding scheme based on integer-to-integer wavelet transform is proposed in this paper. The scheme uses a Sudoku-based method to embed data by modifying the wavelet coefficients. First, the algorithm performs the one-level integer wavelet transform of the host image and obtains four sub-bands, i.e., LL1, HL1, LH1, and HH1. Then, the HL1 sub-band is used as the base matrix, and the LH1 sub-band is used as the variable matrix to embed the secret digits according to a Sudoku table. A location map is created to record the embeddable coefficients, and the map is embedded into the sub-band of HH1. The experimental results showed that our proposed scheme produced a higher-quality stego image than those existing hiding schemes.

Keywords: Integer-to-integer wavelet transform, location map, reversible data hiding, Sudoku-based method

1 Introduction

Steganography refers to embedding secret information in a host image and transmitting the image without the secret information being discovered. The two focuses of the process are the embedding capacity and the invisibility of the embedded message. Generally, as the embedding capacity increases, the quality of the stego image decreases. Thus, there is always a trade-off between embedding capacity and the quality of the image, and different choices are made depending on the specific applications in which the process is used.

In recent years, with the rapid development of multimedia technology, steganography has been used extensively [5, 6, 14]. The aims of the reversible data hiding technique are to extract the embedded secret information and to restore the host image losslessly. In many fields (e.g., law enforcement, medical, and military), the recovery of the host image, as well as the secret information, is required [9]. Reversible data hiding can be implemented in the spatial domain [7, 8, 11, 12, 15, 18, 19, 20, 21, 22] and in the transformed domain [4, 13, 23, 24, 25]. In the spatial domain, Honsinger et al. used a modulo 256 addition algorithm to embed data in the spatial domain [7]. Tian proposed a reversible, data-embedding method using difference expansion between adjacent pixels [20]. Ni et al. proposed a reversible data hiding approach that involved the modification of the histogram of the host image [18]; in their approach, multiple pairs of maximum points and minimum points of the histogram are used to embed the secret data, and they achieved a high peak signal-to - noise ratio (PSNR) value, i.e., above 48 dB. Tai et al. proposed a reversible data hiding scheme based on modifying the histogram of pixel differences [19]. A reversible, image-hiding technique that uses predictive coding and histogram shifting is presented in [21]. Hu et al. performed difference expansion (DE)-based, reversible data hiding with an improved overflow location map [8]. Luo et al. proposed a reversible data hiding method based on preservation of the block median [15]. Tseng et al. presented a reversible data hiding scheme based on the expansion of the prediction error [22].

In the transformed domain, Xuan et al. presented a novel, high-capacity, lossless data hiding approach based on the integer wavelet transform (IWT); they used the modification of the histogram to prevent overflow/underflow caused by the modification of the wavelets coefficients [24]. A reversible hiding in discrete cosine transform (DCT)-based, compressed images was proposed in [4]. Wu et al. proposed a reversible data hiding algorithm based on histogram shifting using difference inte-

ger wavelet coefficients [23]. In each sub-band, the difference of two neighboring integer wavelet coefficients is obtained, and the peak point of the differences in the histogram is searched for data hiding in the wavelet coefficients. Although schemes in the transformed domain have been used for some time, the existing methods still have many problems, such as poor quality images even when the embedding capacity is small and difficulty in extending the embedding capacity.

In addition, some research on reversible data hiding has been done in encrypted images [16, 26]. Zhang presented a separable reversible data hiding method in encrypted images, in which an encryption key was used to encrypt the original, uncompressed image and a data-hiding key was used to create a sparse space to accommodate the secret. The receiver can extract the secret and recover the host image without any error only when he or she has both the encryption key and the data-hiding key [26].

The reference-table-based hiding schemes embed a secret digit into a pair of host pixels according to a predetermined table [2, 3, 27]. Zhang et al. proposed a data hiding technique that exploited the modification of directions (EMD), and a higher embedding efficiency was obtained [27]. Chang et al. presented an information hiding scheme using Sudoku, and the embedding capacity was improved notably [2].

Based on the Sudoku method proposed by Chang et al., we present a novel, reversible, data hiding approach in wavelet domain in this paper. The main contributions of our scheme include 1) high payload and 2) high image quality due to embedding in the wavelet domain.

The rest of the paper is organized as follows. Section 2 introduces related work, including the integer wavelet transform approach and the Sudoku hiding scheme. The proposed scheme is presented in Section 3. The experimental results and our analysis of them are presented in Section 4. Our conclusions are presented in Section 5.

2 Related Work

2.1 Integer Wavelet Transform

Digital images use integers to represent the pixels gray values. The integer wavelet transform (IWT) can map the gray values into integer wavelet coefficients losslessly. We can write the Haar transform as pairwise averages and differences:

$$s_{1,k} = \frac{s_{0,2k} + s_{0,2k+1}}{2}, \quad d_{1,k} = s_{0,2k+1} - s_{0,2k}. \qquad (1)$$

where $d_{i,k}$ is the k^{th} high frequency wavelet coefficient at the i^{th} level, $s_{i,k}$ is the k^{th} low frequency wavelet coefficient at the i^{th} level (i>0), and $s_{0,k}$ represents the k^{th} pixel itself [1].

Based on Equation (1), the forward transform and the inverse transform can be calculated according to Table 1.

The decomposition of the image at level 1 is shown in Figure 1, where LL1 denotes the low-frequency wavelet sub-band, and HL1, LH1, and HH1 represent detail wavelet sub-bands.

Table 1: Integer wavelet transform

Forward transform	Inverse transform
$d_{1,k} = s_{0,2k+1} - s_{0,2k}$	$s_{0,2k} = s_{1,k} - \lfloor d_{1,k}/2 \rfloor$
$s_{1,k} = s_{0,2k} + \lfloor d_{1,k}/2 \rfloor$	$s_{0,2k+1} = d_{1,k} + s_{0,2k}$

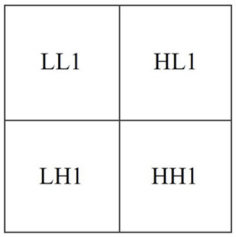


Figure 1: The decomposition of the image at level 1

2.2 Sudoku-Table-Based Hiding Scheme

Chang and Chou proposed a novel information hiding scheme using a Sudoku table. Assuming that the range of the gray values of the pixels in the host image is [0,255], the size of the reference table N should be 256×256, and it is constructed by duplicating a Sudoku table. An example of reference table N is shown in Figure 2. After that, the secret message is transformed to digits in the 9-ary notational system, i.e., S=$\{s_1,s_2,s_3,\ldots,s_k\}$ ($s_i \in [0,8]$, i=1,2,...,K), where K is the length of the 9-ary secret sequence. Assume that a pair of embeddable pixels in the host image is (p_i,p_{i+1}), where p is the pixels gray value, p_i and p_{i+1} are used as indices of the reference table, and a number can be found in the table, i.e., $N(p_i,p_{i+1})$. The steps to find the pixels gray values of the stego image, (p_i^s,p_{i+1}^s), is described as follows:

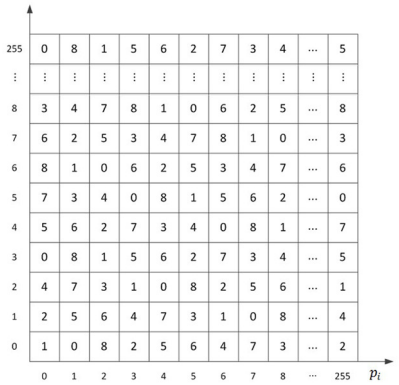


Figure 2: An example of the reference matrix N

S1: Keep p_i unchanged, search (p_i^V, p_{i+1}^V) in the vertical direction as follows:

$$p_i^V = p_i,$$

$$p_{i+1}^V = \begin{cases} p_{i+1} \pm a, & \text{where } N\left(p_i^V, p_{i+1}^V\right) = s_i, \text{ if } 3 < p_{i+1} < 25 \\ b, & \text{where } N\left(p_i^V, p_{i+1}^V\right) = s_i, \quad \text{if } p_{i+1} \le 3 \\ c, & \text{where } N\left(p_i^V, p_{i+1}^V\right) = s_i, \quad \text{else} \end{cases}$$

$$\text{for } a = 0, 1, 2, 3, 4;\ b = 0, 1, \cdots, 7, 8;\ \text{and } c = 247, 248, \cdots, 255. \tag{2}$$

S2: Keep p_{i+1}unchanged, searching (p_i^H, p_{i+1}^H) the horizontal direction as follows:

$$p_{i+1}^H = p_{i+1},$$

$$p_i^H = \begin{cases} p_i \pm a, & \text{where } N\left(p_i^H, p_{i+1}^H\right) = s_i, \text{ if } 3 < p_i < 252 \\ b, & \text{where } N\left(p_i^H, p_{i+1}^H\right) = s_i, \quad \text{if } p_i \le 3 \\ c, & \text{where } N\left(p_i^H, p_{i+1}^H\right) = s_i, \quad \text{else} \end{cases}$$

$$\text{for} a = 0, 1, 2, 3, 4;\ b = 0, 1, \cdots, 8;\ \text{and } c = 247, 248, \cdots, 255. \tag{3}$$

S3: When $p_i < 252$ and $p_{i+1} < 255$, record $x_n = \lfloor \frac{p_i}{3} \rfloor \times 3$, $y_n = \lfloor \frac{p_{i+1}}{3} \rfloor \times 3$, search (p_i^N, p_{i+1}^N) in the neighbors as follows:

$$\begin{cases} p_i^N = x_n + k \\ p_{i+1}^N = y_n + l \end{cases} \quad \text{if } p_i < 252, \text{and } p_{i+1} < 255,$$

$$\text{where } N\left(p_i^N, p_{i+1}^N\right) = s_i, \text{and } k{=}0, 1, 2; l = 0, 1, 2\,. \tag{4}$$

where $\lfloor x \rfloor$ denotes the largest integer smaller than x.

After the above searching operations, three corresponding candidates' positions, i.e., (p_i^V, p_{i+1}^V), (p_i^H, p_{i+1}^H), and (p_i^N, p_{i+1}^N), in the reference table can be obtained. Then, the distances from the locating point (p_i, p_{i+1}) to the candidates' position can be calculated, respectively. The candidate with the smallest distance is chosen, i.e., the corresponding candidate's position is recorded as (p_i^s, p_{i+1}^s). Then, the pixel pair in the host image, (p_i, p_{i+1}) is modified to (p_i^s, p_{i+1}^s) as the gray values in the stego image.

3 The Proposed Scheme

3.1 Framework of the Proposed Data Hiding Scheme

The main idea of the proposed scheme is to use a Sudoku-based scheme to embed data by modifying the integer wavelet coefficients in the wavelet domain. The proposed scheme includes two procedures, i.e., data embedding and data extraction with recovery of the host image. The flowcharts of the two procedures are shown in Figure 3 and Figure 4, respectively.

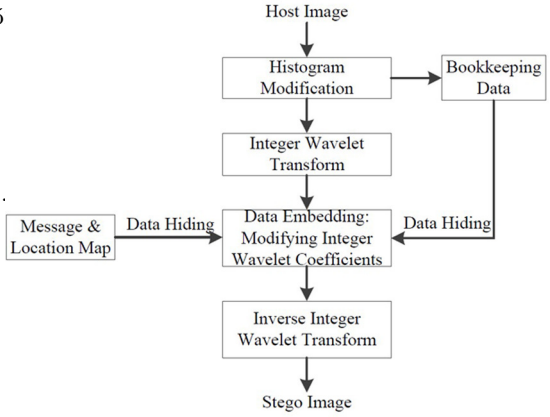


Figure 3: Flowchart of data embedding

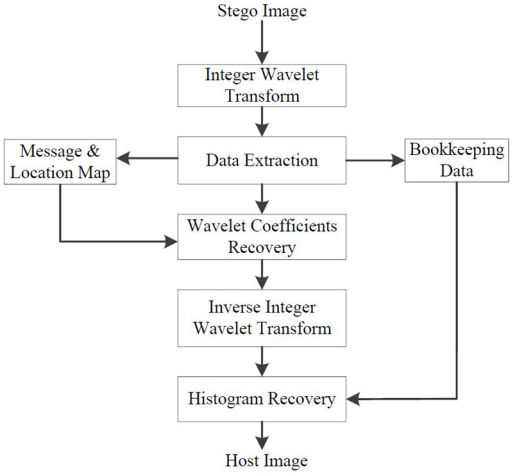


Figure 4: Flowchart of data extraction and host image recovery

For the data embedding part, histogram shifting is applied first to the host image to prevent overflow/underflow during the frequency transformation. In this process, overhead bookkeeping information is generated and recorded. After that, the modified host image is decomposed by IWT. The embedding algorithm is used in the selected wavelet coefficients. To extract the secret message and restore the host image, a location map that indicates the embedding positions is needed, and the map will be embedded in the IWT coefficients.

For data extraction and recovery of the host image, the location map and overhead bookkeeping information are extracted first. The location map is used to extract the secret information and to restore the wavelet coefficients. After that, the inverse integer wavelet transform is implemented, and the gray values in the spatial domain

are obtained. Finally, the original host image is obtained by inverse histogram shifting according to the overhead bookkeeping information.

3.2 Histogram Modification

As stated in Section 2.2, the Sudoku-table-based algorithm itself will not generate the problem of overflow/underflow. However, when it is used in the wavelet domain, after the wavelet coefficients are modified, it may influence their reconstruction, i.e., overflow/underflow may occur after the inverse IWT, and some gray values in the stego image may be out of the range of [0,255]. To prevent overflow/underflow, histogram modification was used in the paper. And overhead bookkeeping data were generated and recorded to recover the host image.

Here is an example that shows how to narrow down the histogram. Assuming that the size of the host image is 6× 6 with 8 gray scales, Figure 5 and Figure 6 show that the histogram is narrowed down 1 gray scale for both sides.

Figure 7 shows the pattern of the overhead bookkeeping information [22].

As shown in Figure 7, V is the length of the overhead bookkeeping information, and n is the shifted number of the gray scale for both sides. $left$ and $right$ are vectors, which are composed of 0 and 1. Scan the host image, $left$ is used to record information for the left-side shifted gray values. And, in a similar way, $right$ is used to record information for the right-side shifted gray values. The size of the $left$ is determined by the numbers of the shifted gray values in the left side, while the size of the $right$ is determined by the numbers of the shifted gray values in the right side. As shown in Figure 5, for the $left$, when we encounter gray value "0", we record a bit "1" in the $left$, whereas, when we encounter gray value "1" ; we record a bit "0" in the $left$. Finally, we obtain the $left$ information as "10100" and the $right$ information as "0100100".

3.3 Data Embedding

Assume that the size of the host image is M×N, the length of the secret is K, and the secret sequence is S=$\{s_1,s_2,s_3,\ldots,s_k\}$ ($s_i \in [0,8]$, i=1,2,...,K). Modify the histogram of the host image and apply the one-level

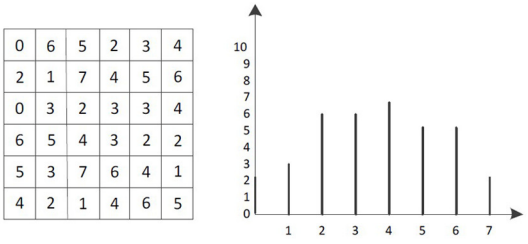


Figure 5: Original image data and histogram

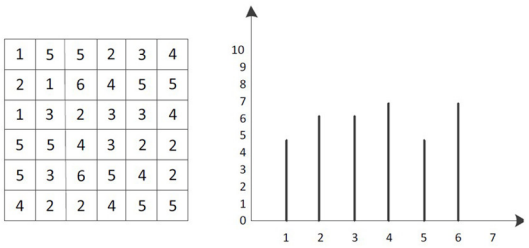


Figure 6: Modified image data and histogram

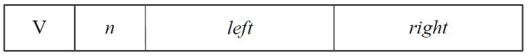


Figure 7: Overhead bookkeeping information

integer wavelet transform to the modified host image; then, four sub-bands (LL1, HL1, LH1, and HH1) are obtained after the decomposition. Note that the sizes of the sub-bands are all $(M/2) \times (N/2)$. After the integer wavelet transform, the wavelet coefficients in the four sub-bands may be beyond of the range of [0,255], for instance, the range of the transformed wavelet coefficients is $[c_{min}, c_{max}]$, where c_{min} may be less than 0, and c_{max} may be more than 255. We must adjust the wavelet coefficients to be above 0 to hide the secret message, so add $c_{min}+1$ to all the coefficients of IWT if $c_{min} < 0$, and the range of the modified wavelet coefficients is changed into$[1, c^*_{min}]$, where $c^*_{min} = c_{max} + c_{min} + 1$.

After modifying the wavelet coefficients, assume that the range of HL1 is [1,H] and that the range of LH1 is $[1, W]$. Therefore, the size of the reference table in our proposed scheme is $H \times W$. Figure 8 shows part of the coefficients in HL1 and LH1. To embed the secret digits, a reference table N is constructed by duplicating a Sudoku table with the size of $H \times W$ in both horizontal and vertical directions. After that, we subtract LH1 from HL1 to obtain a differential matrix,D, as below:

$$D(i,j) = HL1(i,j) - LH1(i,j) = 0, (i \in [1, M/2], j \in [i, N/2]). \tag{5}$$

The differential matrix D of the example shown in Figure 8 is represented in Figure 9(a). When embedding, we choose the coefficients in the same position, i.e.,(i,j), in LH1 and HL1, respectively, which are named as a *coefficient pair* in this paper, and we judge whether the coefficient pair is embeddable by the following requirement:

$$D(i,j) = k, \tag{6}$$

where $k = k_{min}, \ldots, -1, 0, 1, \ldots, k_{max}$, $1 \le i \le M/2$ and $1 \le j \le N/2$. Simultaneously, a location map that indicates the secret-carry-coefficient is generated, as shown in Figure 9(b).

151	151	149	148	149	149	150	148
149	148	149	151	150	148	148	150
149	150	150	149	151	151	150	148
152	151	150	150	147	151	154	152
149	150	149	149	152	150	146	148
150	148	151	150	147	149	151	151
150	150	150	148	152	151	148	148
150	149	150	150	147	149	148	150

(a)*HL1*

150	150	153	151	146	152	150	148
150	149	150	151	147	152	148	149
150	151	152	151	146	151	151	150
149	150	152	149	149	149	147	151
150	150	151	149	150	150	149	148
150	150	149	149	149	149	151	150
150	150	145	149	149	148	152	151
151	152	148	150	147	150	148	150

(b) *LH1*

Figure 8: Part of the coefficients in HL1 and LH1

1	1	-4	-3	3	-3	0	0
-1	-1	-1	0	3	-4	0	1
-1	-1	-2	-2	5	0	-1	-2
3	1	-2	1	-2	2	7	1
-1	0	-2	0	2	0	-3	0
0	-2	2	1	-2	0	0	1
0	0	5	-1	3	3	-4	-3
-1	-3	2	0	0	-1	0	0

(a)

0	0	0	0	0	0	1	1
0	0	0	1	0	0	1	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1
1	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0
0	0	0	1	1	0	1	1

(b)

Figure 9: Differential matrix and Location map (a) Differential matrix D between and ; (b) Location map L

When embedding, we use HL1 as the base matrix and LH1 as the variable matrix. That is to say, for an embeddable coefficient pair, we keep the coefficient HL1(i,j) unchanged and modify the coefficient LH1(i,j), according to the reference table, to embed a secret digit.

For example, consider the wavelet coefficients subject to $D(i,j) = HL1(i,j) - LH1(i,j), (i \in [1, M/2], j \in [1, N/2])$; the embedding procedures follow:

S1: Determine the wavelet coefficients subject to $D(i,j) = HL1(i,j) - LH1(i,j), (i \in [1, M/2], j \in [1, N/2])$ and the coefficient pair of which is (p_i, p_{i+1}), where $p_i = HL1(i,j)$ and $p_{i+1} = LH1(i,j)$.

S2: The size of reference table N is $H \times W$, and the next-to-be-embedded secret digit is s_i, so the stego coefficient pair,(p_i^s, p_{i+1}^s), as in Equation (7):

$$p_i^s = p_i,$$

$$p_{i+1}^s = \begin{cases} a, & \text{where } N(p_i^s, p_{i+1}^s) = s_i \\ & \text{and } a = 0, 1, \cdots, 8, \text{ if } p_{i+1} \le 3 \\ W - a, & \text{where } N(p_i^s, p_{i+1}^s) = s_i \\ & \text{and } a = 0, 1, \cdots, 8, \text{ if } p_{i+1} \ge W - 3 \\ p_{i+1} \pm a, & \text{where } N(p_i^s, p_{i+1}^s) = s_i \text{ and} \\ & a = 0, 1, \cdots, 4, \text{ if } 3 < p_{i+1} < W - 3. \end{cases} \quad (7)$$

S3: Record the stego coefficient pair as $HL1(i,j) = p_i^s$,$LH1(i,j) = p_{i+1}^s$.

Assuming that the sizes of HL1 and LH1 are 3×3, that the size of reference table N is $H \times W$, and that the next-to-be-embedded secret digit is $s_i = 6$, Fig. 10 shows the embedding procedure when the wavelet coefficients are subject to $D(i,j) = HL1(i,j) - LH1(i,j) = 0$, where $i \in [1, M/2]$ and $j \in [1, N/2]$.

Table 2: Different hiding levels L with their corresponding k

L	1	2	3	4	...	L_{max}
k	0	-1,0	-1,0,1	-2,-1,0,1,2	...	$k_{min} \cdots k_{max}$

To increase the payload, more values of k can be chosen. Table 2 shows different hiding levels L with various k.

To record the embedding positions, a location map is created and is compressed by run length encoding (RLE). After that, the compressed location map is embedded into the high-frequency sub-band HH1 using LSB replacement. If the location map is too large to be embedded into the LSB of HH1, then the second LSB and the third LSB of HH1 will be used to embed the location map.

Input: A host image I of size $M \times N$ and the secret message S;

Output: A stego image I';

Steps:

1) Modify the histogram of the host image to prevent overflow/underflow and record the bookkeeping data for the recovery of the host image.

2) Apply the one-level integer wavelet transform to the modified host image and obtain four sub-bands (LL1, HL1, LH1, and HH1) after the decomposition.

3) A reference table N that depends on the IWT coefficients is constructed by duplicating the Sudoku table in this step. That is, when $c_{min} < 0$, add $c_{min} + 1$ to the wavelet coefficients to ensure all the wavelet coefficients is greater than 0, and then find the maximum modified wavelet coefficients c'_{max} from HL1 and LH1 and duplicate the Sudoku table to achieve a reference table N in the range of $[0, c'_{max}]$.

4) Subtract LH1 from HL1 to obtain the differential matrix D. Go through D to find the elements subject to $D(i,j) = k$, where $k = k_{min}, \ldots, -1, 0, 1, \ldots, k_{max}$, $1 \le i \le M/2$ and $1 \le j \le N/2$, of which positions are recorded as $L1, L2, \ldots, Lk$, respectively. The matrices of $L1, L2, \ldots, Lk$ serve as the location map, which will be embedded into the high frequency sub-band HH1 using the LSB replacement.

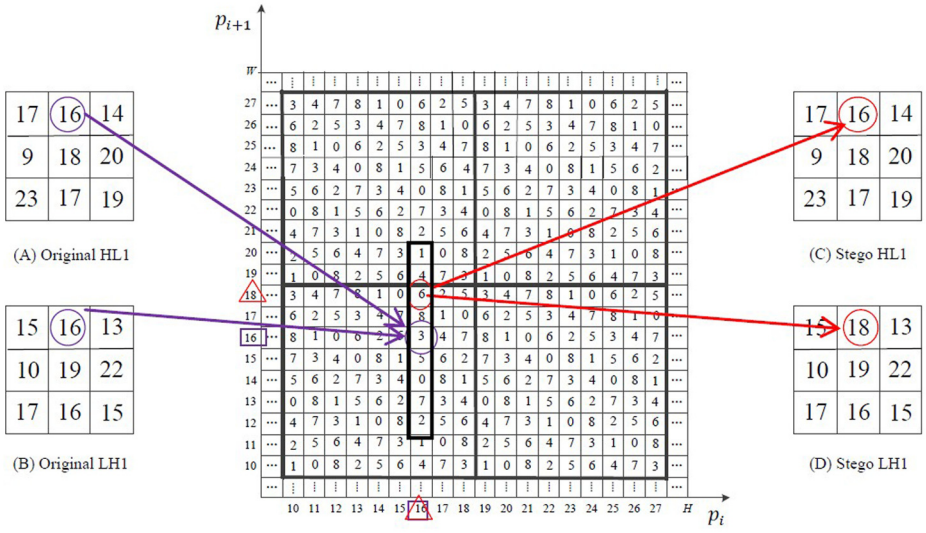


Figure 10: Example of embedding procedure

5) Use HL1 as the base matrix and LH1 as the variable matrix and apply the proposed embedding algorithm to the wavelet coefficients to embed the secret message.

6) Subtract $c_{min}+1$ to the wavelet coefficients if $c_{min} < 0$ in Step 3).

7) Perform the inverse integer wavelet transform to generate the stego image.

3.4 Data Extraction

In data extraction procedure, we extract overhead bookkeeping data and the location map from the stego image to obtain the secret message and restore the host image. As shown in the flowchart of data extraction in Figure 4, the process is described as follows:

Input: Stego image I';

Output: A host image I of size $M \times N$ and the secret message S;

Steps:

1) Apply the one-level integer wavelet transform to the stego image and get four sub-bands, LL1, HL1, LH1, and HH1, after the decomposition.

2) Extract the overhead bookkeeping data and location map from the LSB of the sub-band of HH1. According to the location map, the secret message can be obtained, and the modified wavelet coefficients can be restored.

3) Perform inverse integer wavelet transform to generate the image, the histogram of which has been shifted in the embedding phase. Using the extracted bookkeeping data, the host image can be recovered.

4 Theoretical Analysis and Experimental Results

The peak signal-to-noise ratio (PSNR) is used extensively to evaluate image quality, and PSNR is defined as:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}(dB), \quad (2)$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-I'(i,j)]^2, \quad (3)$$

where MSE is the mean square error, indicating the differences between the host image I and the stego image I', and $I(i,j)$ and $I'(i,j)$ represent the gray values in the host image and stego image at location (i,j), respectively.

In the following experiments, seven 512×512 grayscale images were selected to test the performance of our proposed scheme; the images are shown in Figure 11. The PSNRs of the stego images with different hiding levels, L, are shown in Table 3. The experimental results indicated that the embedding rate increased and the PSNR decreased as the L value increased.

We compared our algorithm with that proposed by Wu et al. [23] and Ni et al. [18]. Table 4 summarizes the experimental results of Wu et al.'s method and the proposed scheme in terms of the embedding rate and the quality of the stego image. The results show that, for similar embedding rates, the proposed method provided higher PSNR than Wu's scheme. Table 5 shows the experimental results of Ni et al.'s method and the proposed scheme in terms of the embedding rate and the quality of the stego image. For most embedding scenarios, the results showed that the performance of the proposed scheme was better than that of Ni's scheme.

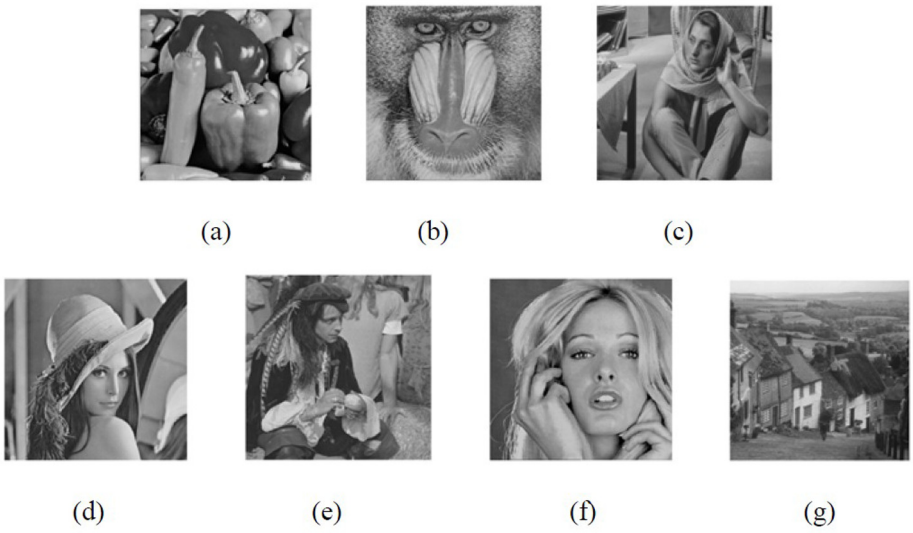


Figure 11: Host images (a) Peppers (b) Baboon, (c) Barbara, (d) Lena, (e) Man (f) Tiffany and (g) Goldhill

Table 3: Embedding rate, R, and its corresponding PSNR of the stego image with different hiding levels L

Image	$L=1$		$L=2$		$L=3$	
(512×512)	R/bpp	PSNR	R/bpp	PSNR	R/bpp	PSNR
lena	0.063	52.99	0.123	49.71	0.183	45.55
Tiffany	0.054	51.46	0.101	49.29	0.147	46.64
Baboon	0.019	57.33	0.037	54.50	0.059	52.80
Barbara	0.048	54.34	0.094	50.99	0.141	49.29
Peppers	0.058	51.05	0.114	48.85	0.170	46.05
Goldhill	0.042	54.87	0.083	51.64	0.122	49.92
Man	0.059	45.29	0.103	44.72	0.147	44.27

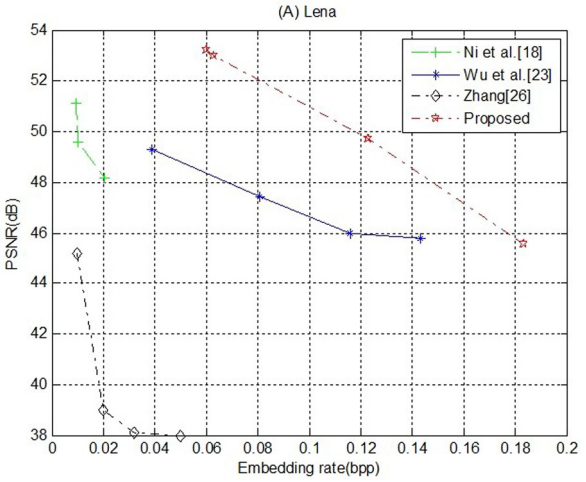
Table 4: Results of embedding rate and image quality comparisons with Wu et al.'s scheme [23]

Image	R/bpp		PSNR	
(512×512)	Wu et al.	Proposed	Wu et al.	Proposed
lena	0.143	0.183	45.81	45.55
Tiffany	0.103	0.147	45.25	46.64
Baboon	0.047	0.059	45.12	52.80
Barbara	0.130	0.141	45.74	49.29
Peppers	0.092	0.170	45.23	46.05
Goldhill	0.121	0.122	45.57	49.92
Man	0.108	0.147	41.37	44.27

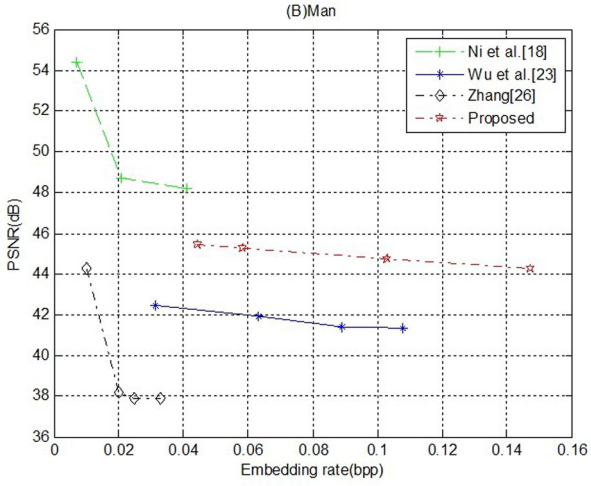
Table 5: Results of embedding rate and image quality comparisons with Ni et al.'s scheme [18]

Image	R/bpp		PSNR	
(512 × 512)	Ni et al.	Proposed	Ni et al.	Proposed
lena	0.021	0.063	48.18	52.99
Tiffany	0.029	0.054	48.26	51.46
Baboon	0.021	0.037	48.18	54.50
Barbara	0.018	0.048	50.18	54.34
Peppers	0.022	0.058	48.23	51.05
Goldhill	0.020	0.042	48.39	54.87
Man	0.041	0.059	48.22	45.29

Figure 12 shows the performance of our proposed scheme with respect to PSNR vs. embedding rate. The comparisons of our scheme with Wu et al.'s method [23], Ni et al.'s scheme [18], and Zhang's technique [26] also are shown. The experimental results indicated that Ni's scheme provided good image quality when the embedding rate was low. But, being restrained by the number of the peak points in the histogram of the host image, its embedding rate depended on the host image, and it was consistently low. When the embedding rate was high, the image quality of our proposed scheme was better than those of all of the existing schemes. This was because our scheme makes full use of the characteristics of the wavelet coefficients when we embed the secret message. We chose wavelet coefficients that had little impact on image quality in which to embed secret information, and the eventual result was good performance.



(a)



(b)

Figure 12: Comparisons of embedding performances: (a) Lena; (b) Man

5 Conclusions

In this paper, a reversible data hiding scheme is proposed based on integer-to-integer wavelet transform and a Sudoku-based hiding scheme. Our Sudoku-based data hiding algorithm scheme is reversible, which implies that the hidden data can be extracted and that the host image can be restored successfully. In addition, our proposed scheme takes advantage of the characteristics of the wavelet coefficients, which have different influences on image quality, to embed secret information, and it achieved good quality images and high embedding capacity. In addition, we can increase the capacity of the proposed scheme by adjusting the embedding positions. According to the simulation results, the proposed scheme provided a suitable capacity with high quality images. A comparison of the results achieved with the proposed technique to those achieved by Wu et al.'s method [23], Ni et al.'s method [18], and Zhang's method [26] demonstrated and confirmed the good performance of the proposed scheme.

References

[1] A. R. Calderbank, Daubechies, W. Sweldens, and B. Yeo, "Wavelet transforms that map integers to inte-

gers," *Applied and Computational Harmonic Analysis*, vol. 5, no. 3, pp. 332–369, 1998.

[2] C. C. Chang, Y. C. Chou, and D. Kieu, "An information hiding scheme using sudoku," in *Proceedings of The Third International Conference on Innovative Computing, Information and Control (ICICIC'08)*, pp. 17–20, Dalian, China, June 2008.

[3] C. C. Chang, T. D. Kieu, and Y. C. Chou, "Reversible data hiding scheme using two steganographic images," in *IEEE Region 10 Conference on TENCON'07*, pp. 1–4, Taipei, 2007.

[4] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," *Information Sciences*, vol. 177, no. 13, pp. 2768–2786, 2007.

[5] Q. Cheng and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Transacations on Multimedia*,vol. 3, no. 3, pp. 273–284, 2001.

[6] W. Hong and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 176–184, 2012.

[7] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, *Lossless Recovery of an Original Image Containing Embedded Data*, US Patent 6278791, 2001.

[8] Y. J. Hu, H. K. Lee, and J. W. Li, "De-based reversible data hiding with improved overflow location map," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250–260, 2009.

[9] L. C. Huang, L. Y. Tseng, and M. S. Hwang, "The study of data hiding in medical images," *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[10] X. G. Kang, W. J. Zeng, and J. W. Huang, "A multiband wavelet watermarking scheme," *International Journal of Network Security*, vol. 6, no. 2, pp. 121–126, 2008.

[11] H. J. Kim, V Sachnev, Y. Q. Shi, N Jeho, and H. G.Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 456–465, 2008.

[12] C. F. Lee and H. L. Chen, "A novel data hiding scheme based on modulus function," *Journalof Systems and Software*, vol. 83, no. 5, p. 832–843, 2010.

[13] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 321–330, 2007.

[14] Z. S. Liao, Y. Huang, and C. S. Li, "Research on data hiding capacity," *International Journal of Network Security*, vol. 5, no. 2, pp. 140–144, 2007.

[15] H. Luo, F. X Yu, H. Chen, Z. L. Huang, H. Li, and P. H. Wang, "Reversible data hiding based on block median preservation," *Information Sciences*, vol. 181, no. 2, pp. 308–328, 2011.

[16] Kede Ma, W. M. Zhang, and X. F. Zhao, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[17] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, 2006.

[18] Z. C. Ni, Y. Q. Shi, N. Ansari, and W. Su., "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354 –362, 2006.

[19] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910, 2009.

[20] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[21] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143,2009.

[22] H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding," *Information Sciences*, vol. 179, no. 14, pp. 2460–2469, 2009.

[23] X. Y. Wu and X. W. Zheng, "Reversible data hiding based on histogram shifting using difference integer wavelet coefficients," in *2011 International Conference on Business Computing and Global Informatization (BCGIN'11)*, pp. 383–386, Shanghai, July 2011.

[24] G. Xuan, C. Yang, Y. Zhen, Y. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," *Digital Watermarking Lecture Notes in Computer Science*, vol. 3304, pp. 115–124, 2005.

[25] G. Xuan, J. Zhu, J. Chen, Y. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," *Electronics Letters*, vol. 38, no. 25, pp. 1646–1648,2002.

[26] X. Zhang, "Separable reversible data hiding in encrypted image, *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[27] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 1–3, 2006.

Fan Li was born in Shandong Province, China, in 1990. She received the B.S. degree in Electronic and Information Engineering from Shandong Institute of Business and Technology, Shandong, China, in 2012. She is currently working toward the M.S. degree in Signal and Information Processing from University of Shanghai for Science and Technology, Shanghai, China. Her research

interests include information hiding and image processing.

Qian Mao was born in Shanxi Province, China, in 1978. She received the B.S. degree in Mechanical Engineering and Automation Science from Nanjing University of Aeronautics and Astronautics, Jiangsu, China, in 2000, the M.S. degrees in Traffic Information Engineering and Control from Shanghai Ship and Shipping Research Institute, Shanghai, China, in 2003, and the Ph.D. degree in Traffic Information Engineering and Control from Tongji University, Shanghai, China, in 2006. Since 2006, she has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China, where she is currently a lecturer. She is also a post-doctoral researcher of Asia University, Taiwan. Her research interests include information security, image processing, and information theory and coding.

Chin-Chen Chang received the B.S. degrees in Science in Applied Mathematics and M.S. degree in Science in computer and decision sciences. Both were awarded in National Tsing Hua University, Taiwan. He received his Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures. Since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes.

Feature Selection for Intrusion Detection System Using Ant Colony Optimization

Mehdi Hosseinzadeh Aghdam[1], and Peyman Kabiri[2]
(Corresponding author:Mehdi Hosseinzadeh Aghdam)
Department of Computer Engineering and Information Technology, Payame Noor University (PNU)[1]
P.O. BOX 19395-3697, Tehran, Iran
School of Computer Engineering, Iran University of Science and Technology[2]
Tehran, 16846-13114, Iran
(Email: mhaghdam@iust.ac.ir)
(Received March 30, 2014; revised and accepted Jan. 16 & Mar. 4, 2015)

Abstract

Intrusion detection is a major research problem in network security. Due to the nonlinear nature of the intrusion attempts, unpredictable behavior of the network traffic and the large number of features in the problem space, intrusion detection systems represent a complicated problem area. Choosing effective and key features for intrusion detection is a very important topic in information security. The purpose of this study is to identify important features in building an intrusion detection system such that they are computationally efficient and effective. To improve the performance of intrusion detection system, this paper proposes an intrusion detection system that its features are optimally selected using ant colony optimization. The proposed method is easily implemented and has a low computational complexity due to use of a simplified feature set for the classification. The extensive experimental results on the KDD Cup 99 and NSL-KDD intrusion detection benchmark data sets demonstrate that the proposed method outperforms previous approaches, providing higher accuracy in detecting intrusion attempts and lower false alarm with reduced number of features.

Keywords: Ant colony optimization, feature selection, intrusion detection system

1 Introduction

Intrusion Detection Systems (IDSs) have become important and widely used tools for ensuring network security. In recent years, intrusion detection based on statistical pattern recognition methods has attracted a wide range of interest in response to the growing demand of reliable and intelligent IDSs, which are required to detect sophisticated and polymorphous intrusion attacks [7]. In general, IDSs are usually classified into two categories in the literature: signature-based intrusion detection and anomaly-based intrusion detection [33]. Signature-based intrusion detection, misuse detection, approach can reliably identify intrusion attacks in relation to the known signatures of discovered vulnerabilities. Therefore, well-known intrusions can be detected efficiently with a very low false positive rate. Intrusions are usually polymorphic, and evolve continuously. Signature-based detection will fail easily when facing unknown intrusions and emergent intervention of security experts is required to define signatures or accurate rules, which limits the application of the signature-based detection approach to build intelligent IDSs. Signature-based detection is commonly used in the design of commercial IDSs [38].

Anomaly-based IDS usually deals with statistical analysis and pattern recognition problems. It can detect zero day attacks if the classification model has the generalization capability to extract intrusion pattern and knowledge during the training period [33]. In the anomaly-based intrusion detection approach, the system builds models for normal behavior in the network traffic and detects any deviation from this model as a potential intrusion attempt. This approach commonly suffers from high false positive rate on classifying normal network traffic. Due to the dynamic nature of the network traffic, discovering boundaries between normal and abnormal behavior is a major difficulty in this approach [38]. To overcome the anomaly intrusion detection problem, the data mining [14], machine learning [25] and immune system [37] approaches have been proposed in recent years.

Considering the available computational power and due to the large amount of audit data with a large number of features that IDS needs to examine, even for a small network, traffic analysis is a difficult task. Audit data captures various features of the connections. For example, the audit data would show the network service on the destination (http, telnet, etc.), or the number of wrong fragments or length of the connection (second). Selected features in the problem space might be correlated, which

is difficult for humans to discover. An IDS operating in real-time needs a reduced amount of data for the processing. Some of these features are irrelevant and redundant and thus can be eliminated before the processing [7]. Most of these features are not applicable to intrusion detection; even some noise data may badly affect the performance of the process of detecting intrusions. Extra and noisy features can increase the computation time, and can have a negative impact on the accuracy of the IDS [28]. Hence, we need to select some representative features from the original feature space to reduce the dimensionality of feature space and improve the efficiency and performance of IDS.

Feature Selection (FS) is a commonly used step in machine learning, especially when dealing with a high dimensional space of features. The objective of FS is to simplify a data set by reducing its dimensionality and identifying relevant underlying features without sacrificing predictive accuracy. By doing that, it also reduces redundancy in the information provided by the selected features. In real world problems FS is a must due to the abundance of noisy, irrelevant or misleading features. FS is extensive and it spreads throughout many fields, including text categorization, data mining, pattern recognition, signal processing and intrusion detection [1, 2].

Recently, Ant Colony Optimization (ACO) is gaining popularity as a new approach to the FS [1, 13, 36]. Some literatures provided experimental results that illustrated ACOs superiority over conventional approaches, such as sequential search and the genetic algorithm [13]. Dorigo and colleagues introduced meta-heuristic optimization algorithm based on behavior of ants in the early 1990s. ACO is a new solution finding method in artificial intelligence called Swarm Intelligence (SI). In SI interaction of cooperative individuals is such that a problem-solving behavior emerges. SI is the property of a system whereby the collective behaviors of unsophisticated individuals interacting locally with their environment cause coherent functional global patterns to emerge. Insects such as ants and bees live in colonies. An individual can only do simple behavior on its own, while their colonial cooperative work represents a complex behavior [10]. ACO algorithm is inspired by social behavior of ant colonies. Although they have no sight, ants are capable of finding the shortest route between a food source and their nest by chemical materials called pheromone that they leave when moving [6].

ACO algorithm was originally applied to the travelling salesman problem and later on, it was successfully applied to other optimization problems such as the quadratic assignment problem [18], routing in telecommunication networks, graph coloring problems, scheduling, etc. This method is particularly attractive for FS as there seems to be no heuristic that can lead the search to the optimal minimal subset every time [1]. In this paper a novel intrusion detection system using ACO has been introduced. The classifier performance and the length of selected feature subset are adopted as heuristic information for ACO. Thus, the proposed method needs no prior knowledge of features. Also the classifier performance and the length of selected feature vector are considered for performance evaluation. Finally, the proposed method is applied to KDD Cup 99 and NSL-KDD, the new version of KDD Cup 99, data sets.

The rest of this paper is organized as follows. Section 2 outlines the related work about feature selection methods in intrusion detection. The proposed ACO-based method for IDS is described in section 3. Section 4 reports computational experiments. It also includes a brief discussion of the results obtained and finally the conclusion and future works are offered in the last section.

2 Related Work

Feature selection is a process that selects a subset of original features. The significance of FS can be viewed in two facets. The frontier facet is to filter out noise and eliminate irrelevant and redundant features. FS is compulsory due to the abundance of noisy, irrelevant or misleading features in a data set. Second, FS can be considered as an optimization problem for an optimal subset of features that better satisfy a desired measure [12]. Quality of the FS optimization can be measured using certain evaluation criteria. Since FS is a NP-hard problem, there is no practical solution to find its optimal feature subset [17]. A typical FS process includes *subset generation, subset evaluation, termination criteria and result validation.* Subset selection procedure implements a search method that selects feature subsets for evaluation based on a certain search strategy. It may start with empty subset, full subset, a selected feature subset or some random feature subset. Those methods that start with an initial subset usually select this feature subset using heuristic methods. These search methods include forward selection, backward elimination and forward/backward combination methods. The process of subset selection and evaluation is repeated until a given termination condition is satisfied. The selected best feature subset usually needs to be validated using a different test data set [17].

Volume of the network traffic data and the high dimensionality of the feature space are main causes for prohibitively high processing overhead. This is why they are major problems in IDS design. Therefore, FS is an important phase in IDS design. Variation of the normal traffic often hinders anomaly-based IDS ability to accurately model normal state of the operation of the network. In any intrusion attempt there are some behavioral patterns and interrelations that are unique and recognizable. Since these patterns are hidden within the irrelevant and redundant features it is often difficult to discover them. Eliminating the less relevant features can improve both the speed and the accuracy of the classification [29].

In accordance to the literature, approaches to FS can be divided into filters, wrappers and embedded approaches [12]. The filter model separates FS from learning

algorithm and selects feature subsets that are independent of any learning algorithm. It relies on various measures of the general characteristics of the training data such as distance, information, dependency, and consistency. In the wrapper approach feature subset is selected using the evaluation function based on the same learning algorithm that will be used later for learning [17]. In this approach the evaluation function finds the optimal feature subset using the subset generation procedure. Finally, comparing the result with best subset resulted from the previous iterations subset evaluation procedure only keeps the best subset. Subset evaluation procedure tests the best subset against the termination criteria to determine if the selection process should end. Although, wrappers may generate a better result, their execution cost is high and may encounter problem in dealing with feature spaces with the very high dimensions. This is due to the use of learning algorithms in the evaluation of subsets, some of which can encounter problems while dealing with a high dimensional space of features [4, 12]. If the FS and learning algorithm are interleaved then the FS approach is a kind of embedded approach [20].

Feature selection is an important issue in intrusion detection. Elimination of the insignificant features may enhance accuracy of the detection. By concentrating on the most important features execution speed of the process can be increased without significant effect on the accuracy of detection. Chebrolu et al. employed the effectiveness of IDS in terms of real-time performance and detection accuracy from the feature selection perspective [7]. In the reported work, features were selected using two methods, Bayesian network and classification and regression trees. Four different sets of features were derived and used in their ensemble method for IDS. In their experiments, KDD Cup 99 data set is used. A very high detection rate is reported in their experiments. Their approach uses only 5092 records for the training and 6890 records for the test. They have proposed no generic subset. Their reported results show that different feature subsets with different length are more effective in detecting various types of attacks [7].

Sung and Mukkamala proposed a well-known closed-loop FS method for SVM-based IDS, called SVM-RFE, which recursively eliminated one feature at a time and compared the resulting performance in each SVM test [28]. They also ranked six significant features [29]. They used three methods and compared the performance of these methods in terms of classification accuracy on the test data set. In the reported work, they used support vector decision function ranking, linear genetic programming and multivariate adaptive regression splines [29]. Sung et al. reported a new feature subset that provides accurate results for the detection of different types of attacks [30]. They have used genetic algorithm to maximize inter-class difference and minimize size of the subset. Mukkamala and Sung applied SVM-RFE method to the KDD Cup 99 data and performed the feature ranking for FS [22]. They ranked the features into three categories: important, secondary, and insignificant according to three main performance criteria: overall accuracy of classification, training time, and testing time. 19 important features were identified and used in the experiments. This heuristic-based technique is time consuming. Additionally, unknown attack types are not considered in the reported work since the same data set (kddcup.data-10-percent.gz) was applied to the experiment.

Zhang et al. considered the capability of rough set theory in coming up with classification rules in detecting the attacks [39]. They showed that rough set classification using GA can produce a high detection rate. Speed of the feature ranking in the reported work is fast. They did not report the selected features used for classification process. Ohn et al. adopted genetic algorithm to find optimal feature subset for SVM [23]. 31 features were used with radial kernel function in their experiment and a very high detection rate was obtained for the original KDD Cup 99 test data set (corrected.gz). Since their training data set was sampled from the full data set (kddcup.data.gz), the challenge of the problem was reduced. The reason is that the number of attack types in the original training data set (kddcup.data-10-percent.gz) is intentionally employed more than the test data set (corrected.gz). These two data sets can challenge the methods of detecting the unknown type attack.

From these reported works, we can conclude that some features are really significant in intrusion detection. Also, it has been proven that there is no single generic classifier that can best classify all the attack types. Instead, in some cases, specific classifier performs better than others. Thus, most of these works lead to an ensemble or fusion of multiple classifier IDS.

3 Proposed ACO-based Method for Intrusion Detection System

In the early nineties an algorithm called Ant System (AS) was proposed by Dorigo and colleagues as a novel nature-inspired meta-heuristic approach for the solution of combinatorial optimization problems. First, algorithm was applied to the traveling salesman problem. Recently, it was extended and/or modified both to improve its performance and to apply it to other optimization problems. Improved versions of AS include, among others, Ant Colony System (ACS), MAX-MIN, AS and AS-rank. An ant colony optimization algorithm is essentially a system based on individuals which simulate the natural behavior of ants, including mechanisms of cooperation and adaptation. The inspiring source of ACO is the foraging behavior of real ants [9]. The ACO algorithm is based on a computational paradigm inspired by real ant colonies and the way they function. The idea is to use several constructive computational ants. Based on the results of previous experiments stored in the ant dynamic memory structure, each ant is guided to the constructed solution. The paradigm is based on the observation made by ethol-

ogists about the medium used by ants to communicate information regarding shortest paths to food by means of pheromone trails. While an isolated ant moves practically at random, exploration, an ant encountering a previously laid trail can detect it and decide with high probability to follow it, exploitation, and consequently reinforces the trail with its own pheromone. What emerges is a form of autocatalytic process through which the more the ants follow a trail, the more attractive that trail becomes to be followed. The process is thus characterized by a positive feedback loop, during which the probability of choosing a path increases with the number of ants that previously chose the same path. The mechanism above is the inspiration for the algorithms of the ACO family [21].

Before the training phase, a FS phase may also be considered. The FS process identifies which features are more discriminative than the others. This has the benefit of generally improving system performance by eliminating irrelevant and redundant features. In general, FS is not very popular procedure in IDS. However, a few studies use different FS methods for their experiments. This implies that FS could improve some certain level of classification accuracy in IDS. Given a feature set of size N, the FS problem is to find a minimal feature subset of size S ($S < N$) while retaining the previous accuracy. Therefore, there is no concept of solution path in FS problem. A partial solution, i.e. subset, does not define any order among the components, i.e. features of the solution, and the next component to be selected is not necessarily influenced by the last component added to the partial solution [5, 15]. FS problem solutions are not necessarily of the same size. The first step in FS using ACO is to address the problem of redefining the way that the ACO representation graph is used.

3.1 Graph Representation

The main goal of ACO algorithm is to model a problem as the search for a minimum cost path in a graph. Here nodes can be considered as features, with the edges between them denoting the choice of the next feature. The search for the optimal feature subset is then an ant traversal through the graph where a minimum number of nodes, features, are visited that satisfies the traversal stopping criterion. Nodes are fully connected to allow any feature to be selected next. On the basis of this reformulation of the graph representation, the transition rules and pheromone update rules of standard ACO algorithms can be applied. In this case, pheromone and heuristic value are not associated with links. Instead, each feature has its own pheromone value and heuristic value [1].

3.2 Heuristic Information

Generally, the representation of heuristic value is the attractiveness of features and the basic ingredient of any ACO algorithm is a constructive heuristic for probabilistically constructing solutions. A constructive heuristic assembles solutions as sequences of features from the finite set of features. A subset construction starts with an empty subset. Then, at each construction step the current subset is extended by adding a feature from the set of features. A suitable heuristic desirability of traversing between features could be any subset evaluation. In proposed method classifier performance is mentioned as heuristic information for FS. In other words, the classifier accuracy of each feature on training set is considered as heuristic information for each feature. The heuristic information of traversal and node pheromone levels are combined to form the so called probabilistic transition rule, denoting the probability that ant k will include feature i in its subset at time step t:

$$P_i^k(t) = \begin{cases} \frac{[\tau_i(t)]^\alpha . [\eta_i]^\beta}{\sum_{u \in J^k} [\tau_u(t)]^\alpha . [\eta_u]^\beta} & if i \in J^k \\ 0 & otherwise \end{cases} \quad (1)$$

where J^k is the set of feasible features that ant k can be added to its subset; τ_i and η_i are respectively the pheromone value and heuristic information associated with feature i. α and β are two parameters that determine the relative weight of the pheromone value and heuristic information. The transition probability used by ACO is a balance between pheromone intensity (i.e. history of previous successful moves), τ_i, and heuristic information (expressing desirability of the move), η_i. This effectively balances the exploitation-exploration trade-off. The best balance between exploitation and exploration is achieved through proper selection of the parameters α and β. If α=0, no pheromone information is used, i.e. previous search experience is neglected. The search then degrades to a stochastic greedy search. If β=0, the attractiveness (or potential benefit) of moves is neglected.

3.3 Pheromone Update

Pheromone updating is an important part for working the ACO algorithm suitably. After all ants have completed their solutions, pheromone evaporation on all nodes is triggered using Equation (2) and then according to Equation (3) all ants deposit a quantity of pheromone, $\Delta\tau_i(t)$, on each node that they have used.

$$\tau_i(t) = (1-\rho)\tau_i(t) \quad (2)$$

$$\tau_i(t+1) = \tau_i(t) + \Delta\tau_i(t) \quad (3)$$

with

$$\Delta\tau_i(t) = \sum_{k=1}^{m} \Delta\tau_i^k(t) \quad (4)$$

where m is the number of ants at each iteration and $\rho \in (0,1)$ is the pheromone trail decay coefficient. The main role of pheromone evaporation is to avoid stagnation, that is, the situation in which all ants constructing the same solution. All ants can update the pheromone according to Equations (3,4). Where $\Delta\tau_i^k(t)$ is the amount

of pheromone deposited by ant k on node i at time step t:

$$\Delta\tau_i^k(t) = \begin{cases} \omega.\gamma(S^k(t)) + \phi.(n/|S^k(t)|) & if i \in S^k(t) \\ 0 & otherwise \end{cases} \quad (5)$$

where $S^k(t)$ is the feature subset found by ant k at iteration t, and $|S^k(t)|$ is its length. The pheromone is updated according to both the measure of the classifier performance, $\gamma(S^k(t))$, and feature subset length. ω and ϕ are two parameters that control the relative importance of classifier performance and feature subset length, $\omega \in [0,1]$ and $\phi = 1-\omega$. This formula means that the classifier performance and feature subset length have different significance for FS process. In our experiment we assume that classifier performance is more important than subset length, so they were set as $\omega = 0.7$, $\phi = 0.3$.

Algorithm 1 ACO-based Feature Selection Algorithm for IDS

1: Begin
2: Initialize all parameters, i.e. $\alpha, \beta, \rho, m, \tau_0, \phi, \omega, T$.
3: Let $t = 1$.
4: **for** Each node i **do**
5: $\tau_i(t) = \tau_0$.
6: **end for**
7: Place m ants, $k = 1, , m$. // Initialize a population of ants with random positions
8: **while** $t \leq T$ **do**
9: **for** Each ant $k = 1, ..., m$ **do**
10: $S^k(t) = \{\}$
11: **while** Ant is able to increase the detection rate **do**
12: From current node, select next node i using Equation (1).
13: Add node i to subset $S^k(t)$.
14: **end while**
15: Calculate the subset length $|S^k(t)|$.
16: Calculate the classifier performance $\gamma(S^k(t))$.
17: **end for**
18: **for** Each node i **do**
19: Apply pheromone evaporation using Equation (2).
20: Calculate $\Delta\tau_i(t)$ using Equations (4,5).
21: Update pheromone using Equation (3).
22: **end for**
23: $t = t + 1$
24: **end while**
25: Return the subset $S^k(t)$ with highest $\gamma(S^k(t))$ as the solution.
26: End

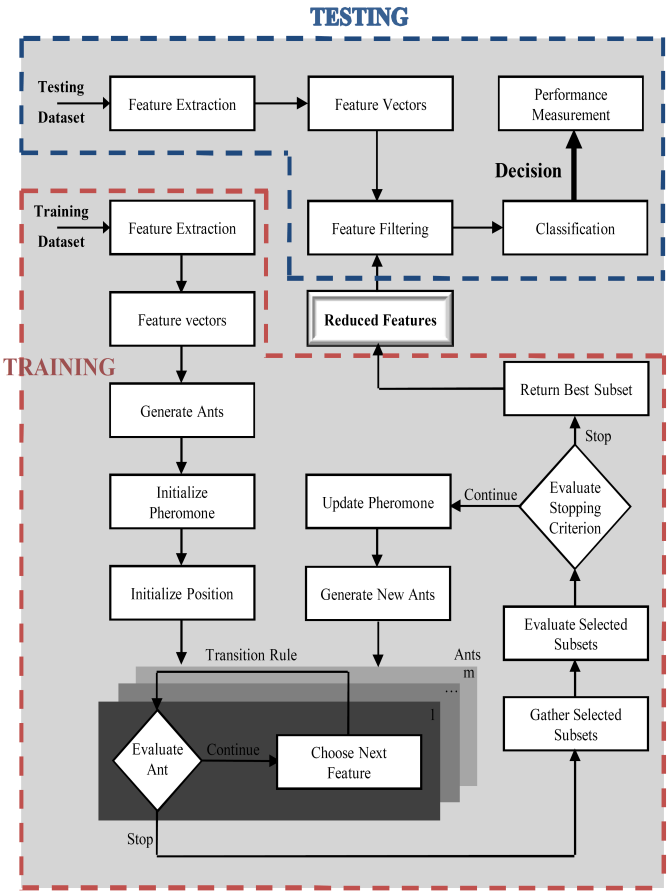


Figure 1: Overall process of proposed ACO-based IDS

3.4 Solution Construction

The overall process of ACO feature selection can be seen in Figure 1. The process starts by generating a number of ants which are then placed randomly on the graph i.e. each ant begins with one random feature. Alternatively, the number of ants to place on the graph may be set equal to the number of features within the data set; each ant starts path construction at a different feature. From these initial positions, they traverse nodes, features, probabilistically until a traversal stopping criterion is satisfied. The resulting subsets are collected and then evaluated. If an optimal subset is found or the algorithm is executed a certain number of times, then the process halts and outputs the best feature subset encountered. If none of these conditions occurred, then the pheromone is updated, a new set of ants are created and the process iterates once more.

In the proposed approach an IDS consists of several essential parts including feature extraction and FS. After preprocessing of compressed raw (binary) TCP dump data of 7 weeks of network traffic (DARPA 98), feature extraction is used to transform the input TCP dump data into a feature set, feature vector. FS is applied to the feature set to select more informative features and to reduce the dimensionality of the problem space. ACO algorithm is used to explore the space of all subsets of given feature set. The performance of selected feature subsets is measured by invoking an evaluation function with the corresponding reduced feature space and measuring the specified classification result. The best feature subset found

is then output as the recommended set of features to be used in the actual design of the IDS.

4 Experiments and Results

The following sections describe the data sets and implementation results.

4.1 Data sets

Since 1999, KDD Cup 99 data set from UCI repository is widely used as the benchmark data set for IDS evaluation [34]. The KDD Cup 99 contained 4,898,431 and 311,029 records in the training set and test set, respectively. Each of record contains 41 features and is labeled as either normal or an attack, with exactly one specific attack type. In our experiments, we apply its 10% training data set consisting of 494021 connection records for training. This data set is prepared by Stolfo et al. and is built based on the data captured in DARPA 98 IDS evaluation program [27]. The DARPA 98 intrusion detection evaluation program was prepared and managed by MIT Lincoln Labs. Lincoln Labs set up an environment to acquire nine weeks of raw TCP dump data for a LAN simulating a typical U.S. Air Force LAN. DARPA 98 is about 4 gigabytes of compressed raw (binary) TCP dump data of 7 weeks of network traffic, which can be processed into about 5 million connection records, each with about 100 bytes. The two weeks of test data have around 2 million connection records. All attacks fall in one of the following four categories:

- **Denial of Service (DoS):** Is an attempt to consume network resources in such a way that their services become limited or unavailable for the legitimate users.
- **User to Root (U2R):** Is an attack in which the attacker starts accessing a normal user account on a machine and gains root access to the machine by exploiting vulnerabilities.
- **Remote to Local (R2L):** Occurs when an attacker does not have an account on a remote system, but who has the ability to send packets to a system over a network and exploits vulnerabilities to gain local access as a user of that system.
- **Probing:** An attack in which the attacker scans network to collect information about its systems for the apparent purpose of circumventing its security controls.

KDD Cup 99 features can be classified into three groups:

1) **Basic features:** this category encapsulates all the attributes that can be extracted from a TCP/IP connection. Most of these features leading to an implicit delay in detection.
2) **Traffic features:** this category includes features that are computed with respect to a window interval.
3) **Content features:** Most of the DoS and Probing attacks have many intrusion frequent sequential patterns, this is due to the fact that these attacks establish many connections to the host(s) in a very short period of time. Unlike these attacks, the R2L and U2R attacks donot have any intrusion frequent sequential patterns. The R2L and U2R attacks are embedded in the payload of the packets, and normally include only a single connection. To identify these kinds of attacks, some relevant features are needed to identify suspicious behavior in the packet payload. These features are called content features [31].

Conducting a thorough analysis of the recent research trend in anomaly detection, one will encounter several machine learning methods reported to have a very high detection rate of 98% while keeping the false alarm rate at 1%. However, when we look at the state of the art IDS solutions and commercial tools, there is few products using anomaly detection, and practitioners still think that it is not a mature technology yet. Tavallaee et al. studied the details of a research in anomaly detection and considered various aspects such as learning and detection approaches, training data sets, testing data sets, and evaluation methods. Their study shows that there are some inherent problems in the KDD Cup 99 data set [31], which, is widely used as one of the few publicly available data sets for network-based anomaly detection systems.

The first important deficiency in the KDD Cup 99 data set is the large amount of redundant records. They found approximately 78% and 75% of the records are duplicated in the training and testing sets, respectively. This large number of redundant records in the training set will cause learning algorithms to be biased towards the more frequent records, and thus prevent it from learning infrequent records which are usually more harmful to networks such as U2R attacks. The existence of these repeated records in the test set, on the other hand, will cause the evaluation results to be biased by the methods which have better detection rates on the frequent records [31].

Tavallaee et al. applied 21 learned machines to analyze the difficulty level of the records in KDD Cup 99 data set. They labeled the records of the entire train and test sets, which provide 21 predicted labels for each record. All the 21 methods applied on the data set classified about 98% of the records in the train set and 86% of the records in the test set correctly. Tavallaee et al. reported these statistics on both KDD Cup 99 train and test sets since they have found similar results presented in many papers, random parts of the KDD Cup 99 training set are used as test sets. As a result, these papers obtain about 98% detection rate. Even applying the KDD test set will result in having a minimum detection rate of 86%, which makes the comparison of IDSs quite difficult since they all vary in the range of 86% to 100% [31]. In this paper, both the KDD Cup 99 and more recent and revised version

of KDD Cup 99 data set, NSL-KDD data set, are used for the experimentation. NSL-KDD data set is publicly available for the researchers and does not suffer from any of the mentioned problems [35]. Additionally, the number of NSL-KDD records in the train and test sets is more reasonable. This advantage makes it a good choice to run the approaches on the complete KDD Cup 99 data set without the need to randomly select a small portion.

It should be mentioned that the test set is not from the same probability distribution as the training set, and it includes unknown attack types that do not exist in the training set that makes it more realistic. The data sets contain a total number of 22 training attack types, with an additional 17 types in the test data set [19]. In Table 2, distribution of different attack types in the KDD Cup 99 and NSL-KDD data sets are listed.

In the KDD Cup 99 and NSL-KDD data sets there are 41 features (listed in Table 3) suggested for each record.

4.2 Performance Measures

The False Positive Rate (FPR) is defined as the number of normal records that are incorrectly detected as intrusions divided by the total number of normal records. The detection rate is defined as the number of intrusion records classified by the IDS divided by the total number of intrusion records present in the test data set. These are good performance measures, since they measure what percentage of intrusions the system is able to detect and how many incorrect classifications are made in the process. Usually True Positive Rate (TPR) and false positive rate are used for performance measurement. TPR also known as Detection Rate (DR) or sensitivity or Recall and FPR also known as the False Alarm Rate (FAR). They showed in the following equations:

$$Recall = TPR = \frac{TP}{TP+FN} \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$FDR = \frac{FP}{TN+FP} \quad (8)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

where TP, TN, FP, FN are the numbers of true positives, true negatives, false positives and false negatives, respectively. Another commonly used measure is F-measure that is defined in Equation (10) [26].

$$F-measure = \frac{2 \times Recall \times Precision}{(Recall + Precision)} \quad (10)$$

4.3 Results

A series of experiments was conducted to show the utility of proposed method. All experiments are executed on a machine with Intel(R) Core(TM) i7 CPU 3.2 GHz and 4 GB of RAM. The operating system was Windows 7 Professional. All tested models were implemented on MATLAB R2011b. Various values were tested for the parameters of the proposed method. The results show that the highest performance is achieved by setting the parameters to values as follow: $\alpha = 0.4, \beta = 0.6, \rho = 0.2$, the initial pheromone intensity of each feature is equal to 1 ($\tau_0 = 1$) the number of ant in every iteration is 50 (m=50) and the maximum number of iterations is 100 (T=100). These values were empirically determined in our preliminary experiments; however, we make no claims that these are optimal values. Parameter optimization is still a topic for future research.

Many papers have focused on improving detection rates of the IDSs using efficient classifiers, i.e. this is a quiet difficult approach. This paper puts forward a modified ACO-based FS algorithm aiming at building a classifier to detect intrusion attempts. In the experiments, the whole training set and test set were applied. Each record in the training set or the test set consisted of 41 features. Initially the proposed FS algorithm is used to select important features for each type of the previous discussed attacks. Later on, a classification system was used to classify the attacks were the results are reported. Each feature value is standardized using Equation (11) and then unimportant features are removed, i.e., leaving only the important features, as listed in Table 4. For each type of attacks, using selected features classification of the attacked is performed and results are compared with those using all 41 features. Finally, using the results of the comparisons, their performance in detecting attacks is evaluated.

$$StandardScore = \frac{X-\mu}{\sigma} \quad (11)$$

where X is a feature value to be standardized, μ is the mean of feature values and σ is the standard deviation of the feature values.

Results of classification using the proposed method are reported in Tables 5 and 6. In each class (normal or attack), each row shows the performance of the proposed method and baseline approach (using all features) in detecting attacks. Experimental results show that FS phase of the process improves the detection rate. In the normal class, studying input features with regard to the output shows that there is no linear relation between the input features and output. Therefore, comparing it versus the baseline approach, implementing the proposed method has significantly improved accuracy of the classification models. The best performance of this system, in terms of its accuracy, is reported to be 98.90%, with only 2.59% false positive rate.

Several experiments are performed to compare the two different IDSs. Results show that an IDS combined with the proposed ACO-based algorithm has higher detection rates in detecting attacks than the baseline approach. Figure 2 shows the true positive rate and the false positive rate for the proposed method as we change the number of selected features. The effect of selecting different fea-

Table 1: KDD Cup 99 and NSL-KDD data sets

Data set name		# Instances	Normal	DoS	U2R	R2L	PROBE
KDD Cup 99	Training set	494021	97278	391458	54	1124	4107
	Testing set	311029	60593	229853	2636	13781	4166
NSL-KDD	Training set	25192	13449	9234	11	209	2289
	Testing set	22544	9711	7458	533	2421	2421

Table 2: The distribution of attack types in the KDD Cup 99 and NSL-KDD

Attack category	Attack type	KDD Cup 99		NSL-KDD	
		Training set kddcup.data10percent	**Testing set** corrected.gz	**Training set** KDDTrain+20Percent	**Testing set** KDDTest+
Denial of Service (DoS)	Neptune	107201	58001	8282	4657
	Smurf	164091	280790	529	665
	Pod	264	87	38	41
	Teardrop	979	12	188	12
	Land	21	9	1	7
	Back	2203	1098	196	359
	Apache2	-	794	-	737
	Udpstorm	-	2	-	2
	Process-table	-	759	-	685
	Mail-bomb	-	5000	-	293
User to Root (U2R)	Buffer-overflow	30	22	6	20
	Load-module	9	2	1	2
	Perl	3	2	0	2
	Rootkit	10	13	4	13
	Spy	2	-	1	-
	Xterm	-	13	-	13
	Ps	-	16	-	17
	Http-tunnel	-	158	-	133
	Sql-attack	-	2	-	2
	Worm	-	2	-	2
	Snmp-guess	-	2406	-	331
Remote to Local (R2L)	Guess-password	53	4367	10	1231
	Ftp-write	8	3	1	3
	Imap	12	1	5	1
	Phf	4	2	2	2
	Multihop	7	18	2	18
	Warezmaster	20	1602	7	944
	Warezclient	1020	-	181	-
	Snmpgetattack	-	7741	-	178
	Named	-	17	-	17
	Xlock	-	9	-	9
	Xsnoop	-	4	-	4
	Send-mail	-	17	-	14
Probe	Port-sweep	1040	354	587	157
	IP-sweep	1247	306	710	141
	Nmap	231	84	301	73
	Satan	1589	1633	691	735
	Saint	-	736	-	319
	Mscan	-	1053	-	996

Table 3: Lists of features in KDD Cup 99 and NSL-KDD data sets

No.	Feature name	Description	Type
1	Duration	Length of the connection (second)	Continuous
2	Protocol-type	Type of protocol, e.g. tcp, udp, etc.	Discrete
3	Service	Network service on the destination, e.g., http, telnet, etc.	Discrete
4	Flag	Normal or error status of the connection	Discrete
5	Src-bytes	Number of data bytes from source to destination	Continuous
6	Dst-bytes	Number of data bytes from destination to source	Continuous
7	Land	1 if connection is from/to the same host/port; 0 otherwise	Discrete
8	Wrong-fragment	Number of wrong fragments	Continuous
9	Urgent	Number of urgent packets	Discrete
10	Hot	Number of hot indicators	Discrete
11	Num-failed-logins	Number of failed login attempts	Discrete
12	Logged-in	1 if successfully logged in; 0 otherwise	Discrete
13	Num-compromised	Number of compromised condition	Discrete
14	Root-shell	1 if root shell is obtained; 0 otherwise	Discrete
15	Su-attempted	1 if su root command attempted; 0 otherwise	Discrete
16	Num-root	Number of root accesses	Discrete
17	Num-file-creations	Number of file creation operations	Discrete
18	Num-shells	Number of shell prompts	Discrete
19	Num-access-files	Number of operations on access control files	Discrete
20	Num-outbound-cmds	Number of outbound commands in an ftp session	Discrete
21	Is-host-login	1 if the login belongs to the hot list; 0 otherwise	Discrete
22	Is-guest-login	1 if the login is a guest login; 0 otherwise	Discrete
23	Count	Number of connections to the same host as the current connection in the past two seconds	Discrete
24	Srv-count	Number of connections to the same service as the current connection in the past two seconds	Discrete
25	Serror-rate	Percent of connections that have SYN errors	Discrete
26	Srv-serror-rate	Percent of connections that have SYN errors	Discrete
27	Rerror-rate	Percent of connections that have REJ errors	Discrete
28	Srv-rerror-rate	Percent of connections that have REJ errors	Discrete
29	Same-srv-rate	Percent of connections to the same services	Discrete
30	Diff-srv-rate	Percent of connections to different services	Discrete
31	Srv-diff-host-rate	Percent of connections to different hosts	Discrete
32	Dst-host-count	Count for destination host	Discrete
33	Dst-host-srv-count	Srv-count for destination host	Discrete
34	Dst-host-same-srv-rate	Same-srv-rate for destination host	Discrete
35	Dst-host-diff-srv-rate	Diff-srv-rate for destination host	Discrete
36	Dst-host-same-src-port-rate	Same-src-port-rate for destination host	Discrete
37	Dst-host-srv-diff-host-rate	Diff-host-rate for destination host	Discrete
38	Dst-host-serror-rate	Serror-rate for destination host	Discrete
39	Dst-host-srv-serror-rate	Srv-serror-rate for destination host	Discrete
40	Dst-host-rerror-rate	Rerror-rate for destination host	Discrete
41	Dst-host-srv-rerror-rate	Srv-serror-rate for destination host	Discrete

Table 4: Selected features out of the 41 features

Category	# Feature	Selected features
Normal	5	Urgent, Num-failed-logins, Count, Rerror-rate, Dst-host-srv-diff-host-rate (9, 11, 23, 27, 37)
DoS	4	Duration, Flag, Root-shell, Dst-host-srv-diff-host-rate (1, 4, 14, 37)
U2R	4	Service, Dst-bytes, Count, Serror-rate (3, 6, 23, 25)
R2L	3	Count, Srv-count, Diff-srv-rate (23, 24, 30)
Probe	8	Protocol-type, Duration, Hot, Logged-in, Num-compromised, Num-access-files, Diff-srv-rate, Dst-host-diff-srv-rate (2, 4, 10, 12, 13, 19, 30,35)

Table 5: Proposed IDS performance on the KDD Cup 99 data set

Category	All features					Proposed IDS				
	Normal	DoS	U2R	R2L	Probe	Normal	DoS	U2R	R2L	Probe
#Correctly detected	45954	183928	29	537	2800	59024	229347	2465	13667	3110
# Miss detected	14639	45925	2607	13244	1366	1569	506	171	114	1056
Precision	77.74	87.86	46.77	82.23	6.68	69.60	81.66	6.53	13.07	86.41
Recall (TPR)	75.84	80.02	1.10	3.9	67.21	97.41	99.78	93.51	99.17	74.65
F-measure	76.78	83.76	2.15	7.45	12.15	81.19	89.82	12.21	23.10	80.10

tures for the all attack classes in each step of the proposed method is depicted in Figure 2. The maximum difference between true positive rate and false positive rate is in the 5th step. Hence the first five features are selected for modeling the system.

A comparison between the test results for the proposed method versus other machine learning methods tested on the KDD Cup 99 test set are presented in Table 7. It can be stated that all the machine learning algorithms tested on this data set offered an acceptable level of detection performance for Normal, DoS and Probe attacks but they did not have good performance on the U2R and R2L types. The proposed method shows better TPR for DoS, U2R and R2L attacks and offers an acceptable level of detection rate for Normal and Probe attacks. There are 18729 records of various new attacks in the KDD Cup 99 test set, which have never appeared in the training set. These new attack records make an IDS trained by a training set hard to achieve good performance for test set. Experiments show that the proposed method shows an acceptable detection rate for detecting new attacks.

Considering the reported results, ACO is faster in locating the optimal solution. In general, it can find the optimal solution within tens of iterations. If exhaustive search is used to find the optimal feature subset in the KDD Cup 99 data set, there will be tens of billions of candidate subsets, which, makes the search nearly impossible. Using ACO, the optimal solution is found after 100th iterations. ACO has powerful exploration ability; it is a gradual searching process that approaches optimal solutions. The execution time for the ACO is mainly affected by the dimensionality of the problem (number of the features), and the size of the data. ACO can search in

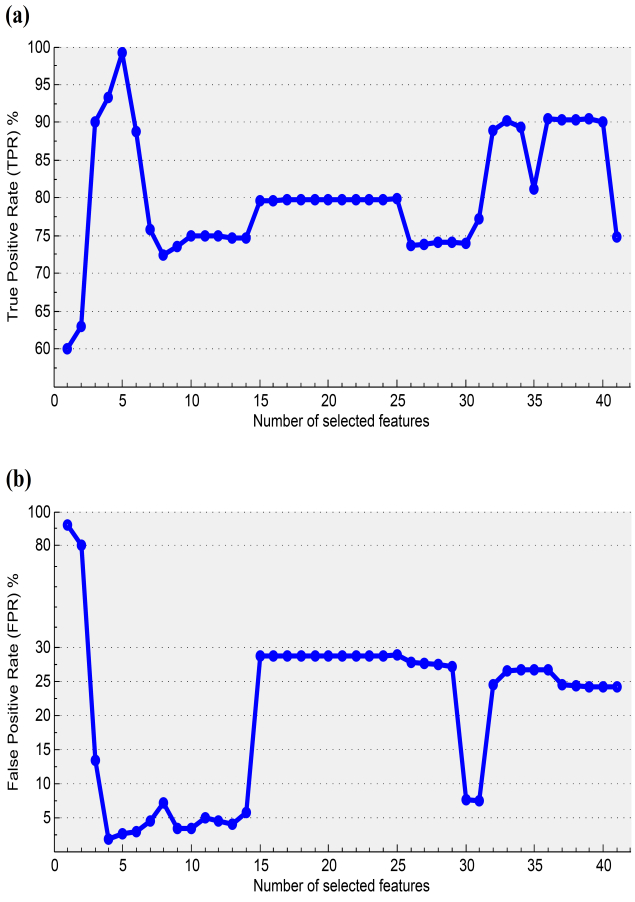


Figure 2: (a) TPR is depicted in each step and (b) FPR is shown in each step

Table 6: Proposed IDS performance on the NSL-KDD data set

Category	All features					Proposed IDS				
	Normal	DoS	U2R	R2L	Probe	Normal	DoS	U2R	R2L	Probe
#Correctly detected	9455	5131	28	454	1434	9483	5613	392	597	1667
# Miss detected	256	2327	505	1967	987	228	1845	141	1824	754
Precision	65.46	87.34	68.29	90.80	85.10	61.31	79.22	8.17	93.14	85.79
Recall (TPR)	97.36	68.80	5.25	18.75	59.23	97.65	75.26	73.55	24.66	68.86
F-measure	78.29	76.97	9.75	31.08	69.85	75.33	77.19	14.71	39.00	76.40

Table 7: Detection rate per record of KDD Cup 99 for the different algorithms performances on the test data set with corrected labels of KDD Cup 99 data set

Model	Normal(%)	DoS(%)	U2R(%)	R2L(%)	Probe(%)	Accuracy	FPR
Proposed method	97.41	99.78	93.51	99.17	74.65	98.9	2.59
PLSSVM [3]	95.69	78.76	30.7	84.85	86.46	Not reported	4.3
Clustering feature [11]	99.3	99.5	19.7	28.8	97.5	95.7	0.7
ESC-IDS [32]	98.2	99.5	14.1	31.5	84.1	95.3	1.9
KDDwinner [24]	99.5	97.1	13.2	8.4	83.3	91.8	0.5
KDD99 runner-up [16]	99.4	97.5	11.8	7.3	84.5	91.5	0.6

the feature space until the optimal solution is found. ACO comprises a very simple concept, and the ideas can be implemented in a few lines of computer code. It requires only primitive mathematical operators, and is computationally inexpensive in terms of both memory requirements and speed. Each ant has a separate memory. In ACO, each ant that passes the optimum solutions are tagged so that other ants can use them and knowledge of good solutions is retained by all ants.

5 Conclusions and Future Works

This paper addresses the problem of dimensionality reduction using ACO in intrusion detection problem area. ACO has the ability to converge quickly. It has a strong search capability in the problem space and can efficiently find minimal feature subset. Experimental results demonstrate a competitive performance. More experimentation and further investigation into this technique is required. The pheromone trail decay coefficient and pheromone amount have an important impact on the performance of ACO. Selection of the parameters is proved to be problem-dependent. The deposited pheromone expresses the quality of the corresponding solution. Evaporation becomes more important for more complex problems. If $\rho = 0$, i.e. no evaporation, the algorithm does not converge. If pheromone evaporates too much (a large ρ is used), the algorithm often converged to sub-optimal solutions. In many practical problems, it is difficult to select the best ρ without trial-and-error. α and β are also key factors in ACO for FS. For large data sets, to speed up the calculation of FS process, a parallel algorithm can be implemented.

The proposed method uses ACO algorithm and a simple classifier (nearest neighbor classifier) to select important features and a trained classifier to identify any kind of new attacks. Tests and comparisons are performed on KDD Cup 99 and NSL-KDD data sets, the test sets contains 17 kinds of different attacks. The proposed method reduced the number of features by approximately 88% and the detection error reduced by around 24% using KDD Cup 99 test data set. The proposed method will significantly reduce both the memory size and the CPU time required for intrusion detection by reducing number of the features used for the detection. This shows that the proposed method is very reliable for intrusion detection. Results indicate that the proposed ACO-based detection method outperforms other methods since it can provide better and more robust representation of the data. This is due to the fact that it can accurately detect a broader range of attacks using smaller number of features.

As for the future work, intention is to apply the proposed intrusion detection method using complicated classifiers to improve its performance and to combine the proposed method with other population-based algorithms. Analyzing packet payload is recently attracting lots of attention and many researchers report works carried-out in this area. It is notable that feature selection for the payload-based intrusion detection is not mature yet. Intension will be to extract and selection appropriate features from the packet payload to improve the detection rate.

Acknowledgments

This study was supported by the Iran University of Science and Technology. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. H. Aghdam, N. Ghasem-Aghaee, and M. E. Basiri, "Application of ant colony optimization for feature selection in text categorization," in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC'08)*, pp. 2872–2878, 2008.

[2] M. H. Aghdam, J. Tanha, A. R. Naghsh-Nilchi, and M. E. Basiri, "Combination of Ant Colony Optimization and Bayesian Classification for Feature Selection in a Bioinformatics Dataset," *Journal of Computer Science and System Biology*, vol. 2, pp. 186–199, 2009.

[3] F. Amiri, M. M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," *International Journal of Network and Computer Applications*, vol. 34, pp. 1184–1199, 2011.

[4] J. Bins, *Feature Selection from Huge Feature Sets in the Context of Computer Vision*, Ph.D. dissertation, Colorado State University, 2000.

[5] C. Blum, and M. Dorigo, "The hyper-cube framework for ant colony optimization," *IEEE Transaction on Systems, Man, and Cybernetics*, Part B, vol. 34, no. 2, pp. 1161–1172, 2004.

[6] E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*, Oxford University Press, New York, 1999.

[7] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *International Journal of Computers and Security*, vol. 24, pp. 295–307, 2005.

[8] P. S. Chung, C. W. Liu, and M. S. Hwang, "A Study of Attribute-based Proxy Re-encryption Scheme in Cloud Environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[9] M. Dorigo, and C. Blum, "Ant colony optimization theory: A survey," *Theoretical Computer Science*, pp. 243–278, 2005.

[10] A. P. Engelbrecht, *Fundamentals of Computational Swarm Intelligence*, John Wiley & Sons, London, 2005.

[11] S. J. Horng, M. Y. Su, Y. H. Chen, T. W. Kao, R. J. Chen, J. L. Lai, C. D. Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *International Journal of Expert Systems with Applications*, vol. 38, no. 1, pp. 306–313, 2011.

[12] R. Jensen, *Combining Rough and Fuzzy Sets for Feature Selection*, Ph.D. dissertation, School of Information, Edinburgh University, 2005.

[13] K. J. Lee, J., Joo, J., Yang, and V. Honavar, "Experimental comparison of feature subset selection using GA and ACO algorithm," in *Advanced Data Mining and Applications*, LNCS 4093, pp. 465–472, Springer, 2006.

[14] W. Lee, S. J. Stolfo, K. W. Mok, "Adaptive intrusion detection: a data mining approach," *International Journal Artificial Inteligence Review*, vol. 14, no. 6, pp. 533–567, 2000.

[15] G. Leguizamon, and Z. Michalewicz, "A New Version of Ant System for Subset Problems," *In Proceedings of IEEE Congress on Evolutionary Computation*, 1999.

[16] I Levin, "KDD-99 classifier learning contest LLSofts results overview," *International Journal of SIGKDD Explorations*, vol. 1, no. 2, pp. 67–75, 2000.

[17] H. Liu, and L. Yu, "Toward integrating feature selection algorithms for classification and clustering," *IEEE Transactions on Knowledge and Data Engineering*, pp. 491–502, 2005.

[18] V. Maniezzo, A. Colorni, "The Ant System Applied to the Quadratic Assignment Problem," *IEEE Transaction on Knowledge and Data Engineering*, vol. 11, no. 5, pp. 769–778, 1999.

[19] MIT Lincoln Labs, *1998 DARPA Intrusion Detection Evaluation*, Feb. 2012. (`http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html`)

[20] D. Mladeni, "Feature Selection for Dimensionality Reduction," in *Subspace, Latent Structure and Feature Selection, Statistical and Optimization, Perspectives Workshop (SLSFS'06)*, LNCS 3940, pp. 84–102, Springer, 2006.

[21] R. Montemanni, L. M. Gambardella, A. E. Rizzoli, and A. V. Donati, "A new algorithm for a Dynamic Vehicle Routing Problem based on Ant Colony System," in *Second International Workshop on Freight Transportation and Logistics*, pp. 27–30, 2003.

[22] S. Mukkamala, and A. H. Sung, "Feature ranking and selection for intrusion detection systems using support vector machines," in *Proceedings of the International Conference on Information and Knowledge Engineering*, pp. 503–509, 2002.

[23] S. Y. Ohn, N. H. Nguyen, D. S. Kim, and J. S. Park, "Determining Optimal Decision Model for Support Vector Machine by Genetic Algorithm," in *Computational and Information Science*, LNCS 3314, pp. 895–902, Springer, 2005.

[24] B. Pfahringer, "Winning the KDD 99 classification cup: bagged boosting," *International Journal of SIGKDD Explorations*, vol. 1, no. 2, pp. 65–66, 2000.

[25] M. Ramadas, S. Ostermann, and B. Tjaden, "Detecting anomalous network traffic with self-organizing maps," in *Proceedings of Sixth International Symposium on Recent Advances in Intrusion Detection*, pp. 36–54, 2003.

[26] C. J. Rijsbergen, *Information Retrieval (2nd ed.)*, London, UK: Butterworth, 1979.

[27] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, P. K. Chan, "Cost-based modeling for fraud and intrusion detection: Results from the jam project," in *In*

Proceedings DARPA Information Survivability Conference and Exposition (DISCEX'00), pp. 130–144, 2000.

[28] A. H. Sung, and S. Mukkamala, "Identifying important features for intrusion detection using support vector machines and neural network," in *Proceedings of International Symposium on Applications and the Internet*, pp. 209–216, 2003.

[29] A. H. Sung, and S. Mukkamala, "The Feature Selection and Intrusion Detection Problems," in *Proceedings of Advances in Computer Science - ASIAN: Higher-Level Decision Making. 9th Asian Computing Science Conference*, LNCS 3321, pp. 468–482, 2004.

[30] W. S. Sung, H. L. Chi, "Using Attack-Specific Feature Subsets for Network Intrusion Detection," in *Advances in Artificial Intelligence*, LNCS 4304, pp. 305–311, Springer, 2006.

[31] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data set," in *Proceeding of the IEEE Symposium on Computational Intelligence in Security and Defense Applications*, pp. 57–62, 2007.

[32] A. N. Toosi, and M. Kahani "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," *International Journal of Computer Communications*, vol. 30, pp. 2201–2212, 2007.

[33] C. Tsang, S. Kwong, and H. Wang, "Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection," International Journal of Pattern Recognition, vol. 40, pp. 2373–2391, 2007.

[34] UCI, *KDD Cup 1999 Data*, The UCI KDD Archive Information and Computer Science University of California, Irvine, Oct. 2014. (`http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`)

[35] UNB, *NSL-KDD Data Set for Network-based Intrusion Detection Systems*, Mar. 2014. (`http://nsl.cs.unb.ca/NSL-KDD/`)

[36] S. M. Vieira, J. M. C. Sousa, and T. A. Runkler, "Fuzzy classification in ant feature selection," in *IEEE International Conference on Fuzzy Systems*, pp.1763–1769, 2008.

[37] P.D. Williams, K. P. Anchor, J. L. Bebo, G. H. Gunsch, and G. D. Lamont, "CDIS: towards a computer immune system for detecting network Intrusions," in *Proceedings of Fourth International Symposium on Recent Advances in Intrusion Detection*, pp. 117–133, 2001.

[38] S. X. Wu, and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *International Journal of Applied Soft Computing*, vol. 10, pp. 1–35, 2010.

[39] L.H. Zhang, G. H. Zhang, L. Yu, J. Zhang, and Y. C. Bai, "Intrusion Detection Using Rough Set Classification," *International Journal of Zheijiang University Science*, vol. 5, no. 9, pp. 1076–1086, 2004.

Mehdi Hosseinzadeh Aghdam is a Ph.D. candidate in the computer engineering department at the Iran University of Science and Technology, he is also a lecturer at Payame Noor University (PNU). He graduated with a master's in computer engineering Artificial Intelligence from University of Isfahan (UI) in 2008. At UI, he worked on swarm intelligence-based method for feature selection. His main research interests are: Data Mining (Feature Selection, Recommendation Systems), Computational Intelligence, Pattern Recognition and Social Network Analysis.

Peyman Kabiri is assistant professor of computer engineering at the Iran University of Science and Technology (IUST). He received a B.Eng. degree in computer hardware engineering from IUST in 1992 and the M.Sc. and Ph.D. degrees in computer science at the Nottingham Trent University, UK, in 1996 and 2000 respectively. He is the director of the Intelligent Automation Laboratory at the Department of Computer Engineering-IUST. Dr. Kabiri has authored a number of publications including journal articles, book chapters, and conference papers. He is editor of a book in intrusion detection work area.

The Policy Mapping Algorithm for High-speed Firewall Policy Verifying

Suchart Khummanee and Kitt Tientanopajai
(Corresponding author: Suchart Khummanee)
Department of Computer Engineering, Khon Kaen University
Khon Kaen 40002, Thailand
(Email: khummanee@gmail.com)
(Received Feb. 8, 2015; revised and accepted June 5 & Aug. 12, 2015)

Abstract

In this paper, we have proposed a novel algorithm and data structures to improve the speed of firewall policy verification. it is called the policy mapping (PMAP). Time complexity of the proposed technique is *O(1)* to verify incoming-outgoing packets against the firewall policy. Besides, the algorithm is not limited to handle IP network classes as IPSET which is the top of high-speed firewall open source today. PMAP can also optimize the firewall rule decision by employing the firewall decision state diagram (FDSD) to clarify ordering of policy verifying. The consumed memory of PMAP is reasonable. It consumes the memory usage around 3.27 GB for maintaining rule data structures processing the firewall rule at 5,000 rules.

Keywords: Firewall policy, packet matching, packet verifying, policy mapping, policy verifying

1 Introduction

In the realm of network security, firewalls are an essential tool for protecting against undesirable traffic from untrusted networks. Generally, firewalls are usually equipped at the gateway between trusted (Private network) and untrusted networks (Public network) as shown in Figure 1. Firewalls consider inbound-outbound packets passing through itself by following the defined policies (technically called rules). Firewall rules mean the instruction sets compounded from various conditions e.g., IP address, protocol, port number and action. If a packet matches one of the defined rules in the firewall, either *accept* or *deny* is selected from the action field. The *accept* action allows packets to pass the firewall; on the other hand, the *deny* action entirely drops packets to the trash can as shown in Table 1.

According to Table 1, rule no. 7 (r_7) represents that firewall permits source IP addresses ranging from 10.0.0.0 to 10.0.0.255 (256 hosts) onto destination IP addresses in the range of 20.0.0.0 to 20.0.0.255 (256 hosts), any source ports (0 - 65,535), a destination port number 80 and 443, and TCP or UDP protocol to pass through the firewall. In contrast, rule no. 4 (r_4) always drops every packet form source IP addresses ranging from 10.0.0.0 to 10.0.0.3 onto destination IP addresses in the range of 20.0.0.0 to 20.0.0.3, any source port, a destination port number 80, and both protocols. Besides, firewalls always set the final rule (usually called an implicit denying rule: r_8) at the bottom of the rule list by dropping all packets that are not matched with the above rules.

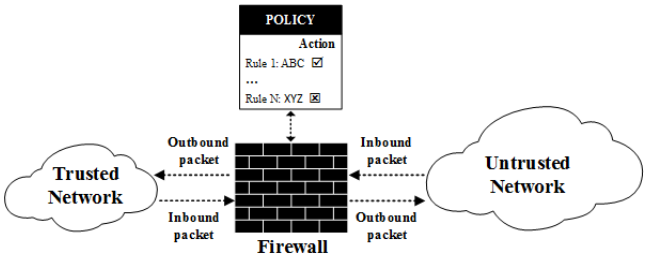


Figure 1: The basic firewall operation and installation

Basically, firewall rules are executed from the top to bottom, denoted as $r_1 \Longrightarrow r_2 \Longrightarrow \cdots \Longrightarrow r_n$. Firewalls working in this manner are called Rule-List or Rule-Base firewalls. For evaluating the effectiveness of Rule-Base firewall verification, the time complexity has very slow efficiency, that is *O(n)*, where n is the number of firewall rules. Nevertheless, memory consuming is quite small. Rule-Base firewalls are appropriate for individual persons and small businesses. However, it is not proper for large companies because firewall rules are usually diverse. Chapple et al. [3] surveyed and found that the size of firewall rule lists ranged from 2 to 17,000 rules, and an average of rules around 140 - 200 approximately. In a large organization, a firewall has about 2,000 rules, with each rule checking between 4 and 7 fields. Thus, the firewall needs to verify rules against 14,000 times per one

Table 1: Firewall rule examples

No.	Source IP	Destination IP	Source Port	Destination Port	Protocol	Action
r_1	10.0.0.10	20.0.0.2	*	21 - 22	TCP, UDP	ACCEPT
r_2	10.0.0.10	20.0.0.2	5000	23 - 25	TCP, UDP	DENY
r_3	10.0.0.0-3	20.0.0.2	*	80	TCP, UDP	DENY
r_4	10.0.0.0-3	20.0.0.0-3	*	80	TCP, UDP	DENY
r_5	10.0.0.2	20.0.0.2	*	80 - 145	TCP, UDP	ACCEPT
r_6	10.0.0.*	20.0.0.*	*	*	TCP, UDP	ACCEPT
r_7	10.0.0.*	20.0.0.*	*	80, 443	TCP, UDP	ACCEPT
r_8	*	*	*	*	*	DENY

packet in the worst case (7 x 2,000).

To improve performance of firewall rule verification, Clark and Agah [4] presented a firewall policy diagram (FPD) and data structures to seek and solve the problem of a large network behavior in firewall policy. Liu and Gouda [10] proposed a diverse firewall approach that produced time complexity as $O(n^d)$, where n is the number of firewall rules and and d is the number of checked fields. After that Acharya and Gouda [1] claimed that their liner time algorithm improved on the diverse firewall from $O(n^d)$ to $O(nd)$. For dealing with rules and continually increasing traffic, researchers tried to solve this problem. Hamed et al. [6] presented a statistical search tree model for filtering and matching packets, whose computational complexity was $O(n * log(n))$, Gouda and Liu [5] proposed the firewall decision diagram (FDD) which clarified packet matching and increased the speed of verifying to $O(log(n))$. In addition, Puangpronpitag et al. [8] introduced a single domain decision concept to get rid of firewall rule conflicts and improve the verifying speed to be $O(log(n))$ by using tree structure. A tree-rule proposed on cloud computing by Xiangjian et al. [15], produced a processing time for $O(log(n))$. Due to huge traffic of a gigabit in the network today, IPSet [12] which is under the Netfilter project and the top of high-speed firewall open source nowadays is $O(1)$ for firewall rule verification. It rearranges the rules of Rule-Base firewall to groups of similar behavior like IP addresses in the same class before deploying the modified groups to a hashing method. However, one drawback of IPSet is the limitation of IP class management. It can only be implemented in a IP Classes C and B – excluding Class A.

According to the weakness of the IPSet as mentioned above, our research focuses on the firewall policy verification because it is the major key to reduce a firewall's performance. Consequently, in this paper, we propose the novel algorithm for high-speed firewall rule verification, called **the policy mapping (PMAP)**, which is *O(1)*. PMAP also handles all IP network classes. The rest of the paper is organized as follows: Section 2 presents the firewall background, the design of policy mapping and implementation are explained in Section 3. In Section 4, we demonstrate the performance evaluation of firewalls, which is divided into two sorts, i.e., the computation time and space complexity. In addition, we compare the performance of our proposed model against other firewalls. Finally, we give conclusions and future work in Section 5.

2 Firewall Background

2.1 The Rule-Base Firewall

Basically, the Rule-Base firewall rule consists of six conditions, which are source IP address (*src_ip*), destination IP address (*dst_ip*), source port (*src_port*), destination port (*dst_port*), protocol (*pro*) and an action (*act*). The first five conditions (*src_ip* to *pro*) are called the predicate, and an *act* is called the decision, which is formulated as follows:

$$\langle predicate \rangle \rightarrow \langle decision \rangle$$

$$\langle src\_ip \wedge dst\_ip \wedge src\_port \wedge dst\_port \wedge pro \rangle \rightarrow \langle act \rangle$$

Where $\wedge$ denotes AND operation. *src_ip* and *dst_ip* are unique addresses used to locate and identify a device over the network. The unique address is a 32-bit number (Internet Protocol Version 4: IPv4) consisting of 4 octets (oct) separated by dots such as 192.168.10.100, 200.0.*.* ($* \in \mathbb{Z}_n^+ : n \geq 0 \wedge n \leq 255$). Indeed, an IP address can be transformed to the positive integer ($\mathbb{Z}_n^+ : n \geq 0, n \leq 2^{32} - 1$) as shown the following equation.

$$Octet_1 \times 2^{24} + Octet_2 \times 2^{16} + Octet_3 \times 2^8 + Octet_4 \times 2^0$$

For example, converting an IP address such as 192.168.10.100 to $\mathbb{Z}_n^+$, the conversion process can be performed as follows:

$$192 \times 2^{24} + 168 \times 2^{16} + 10 \times 2^8 + 100 \times 2^0 = 3,232,238,180.$$

src_port and *dst_port* are used to distinguish itself from other applications running over TCP or UDP by reserving and using a 16-bit port number. The port number 80 [14], for example, is reserved for the Hyper text transfer protocol (HTTP), Domain Name System (DNS) is assigned to port number 53, etc. Also, the reserved ports are called the well-known ports. The last one of the predicates is a standard protocol [7] which defines a method of

exchanging data over a computer network such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It has an 8-bit number ranging from 0 - 255, i.e., the port no. 6 for TCP, no. 17 for UDP respectively.

Finally, *act* is the decision that is either *accept* or *deny*. The *accept* allows the traffic or packets that can pass through the firewalls to the destination networks, while the others are discarded.

2.2 Defining Rule-based Firewall Rule

Let r denote a firewall rule, and n denote the rule number ($n \in \mathbb{Z}^+$ and $n \neq 0$). We frequently specify the firewall by writing:

$r_1 : \langle predicate_1 \rangle \langle decision_1 \rangle \Rightarrow 1^{st}$ rule.
$r_2 : \langle predicate_2 \rangle \langle decision_2 \rangle \Rightarrow 2^{nd}$ rule.
...
$r_n : \langle predicate_n \rangle \langle decision_n \rangle \Rightarrow$ the final rule.

Table 1 demonstrates examples of the actual Rule-Base firewall rules. For the sake of simplicity, we represent the range of host IP addresses using "-", and "*" for any range of IP addresses. In r_3, for example, *src_ip* is 10.0.0.0-3, which represents the range of IP address from 10.0.0.0 - 10.0.0.3 (or 167,772,160 - 167,772,163 in a decimal format), and 10.0.0.* ($src\_ip_{r_6}$) substitutes a set of IP addresses between 10.0.0.0 and 10.0.0.255 (256 hosts).

2.3 Packet Matching vs. Mismatching

Let p denote packets flowing in and out of firewalls, and x denote the packet number by $x \in \mathbb{Z}^+$ and $x \neq 0$. We can form a set of packets to be $p_x = \{p_1, p_2, ..., p_x\}$. The packet is a formatted unit of data carried by a packet mode in the computer network. Generally, a packet consists of two types of data, i.e., control commands and user information (payload). The control commands provide the communication standards that the network needs to deliver the user information, i.e., source and destination IP addresses, error detection codes, sequencing information and so forth. In fact, control commands are set in both headers and trailers of the packet, and the payload is placed in the middle. In this paper, we only take four key fields from the packet for verifying against firewall rules, which are *src_ip*, *dst_ip*, *dst_port* and *pro*. Assuming that an incoming packet (p_1) flows into the firewall; it is formed from *src_ip* = 10.0.0.10, *dst_ip* = 20.0.0.2, *src_port* = 1,024, *dst_port* = 21 and *pro* = TCP. We can rewrite a set of packets $p_1 = \{src\_ip_1, dst\_ip_1, src\_port_1, dst\_port_1, pro_1\} = \{10.0.0.10_1,\ 20.0.0.2_1,\ 1024_1,\ 21_1,\ \mathrm{TCP}_1\}$. The packet p_1 is matched with firewall rules r_1, r_6 and r_8 in the Table 1. However, for Rule-Base firewalls, the packet p_1 will be always executed with the top of firewall rules; which is r_1 only.

The Packet Matching Definition. The packet p_i matches the firewall rule r_n if $(src\_ip_{p_i} \in src\_ip_{r_n}) \wedge (dst\_ip_{p_i} \in dst\_ip_{r_n}) \wedge (src\_port_{p_i} \in src\_port_{r_n}) \wedge (dst\_port_{p_i} \in dst\_port_{r_n}) \wedge (pro_{p_i} \in pro_{r_n}) =$ TRUE. The statement "p_i **matches** r_n" is written $p_i \in r_n$. For example, given the packet $P_1 = \{10.0.0.2_1,\ 20.0.0.2_1,\ 1234_1,\ 80_1,\ TCP_1\}$ and $P_2 = \{22.2.0.10_2,\ 20.0.0.5_2,\ 5000_2,\ 37_2,\ UDP_2\}$, thus $P_1 \in$ firewall rule $r_3 - r_8$ (Table 1), and $P_2 \in r_8$ only.

The Packet Mismatching Definition. The packet p_i mismatches the firewall rule r_n if $(src\_ip_{p_i} \notin src\_ip_{r_n}) \vee (dst\_ip_{p_i} \notin dst\_ip_{r_n}) \vee (src\_port_{p_i} \notin src\_port_{r_n}) \vee (dst\_port_{p_i} \notin dst\_port_{r_n}) \vee (pro_{p_i} \notin pro_{r_n}) =$ TRUE. The statement "p_i **mismatches** r_n" is written $p_i \notin r_n$. For example, let the packet $P_3 = \{10.0.0.10_3, 20.0.0.2_3, 1234_3, 20_3, TCP_3\}$, $P_3 \in r_6$ and r_8 only. On the other hand, $P_3 \notin r_1 - r_5$ and r_7.

2.4 Firewall Rule Verification

Firewall rule verification is the matching process between inbound-outbound packets against the defined rules. The result of matching in a normal case is either an *acceptance* or a *denial*. On the other hand, if firewall rules are the anomaly or conflict, the matching result is probably both acceptance and denial simultaneously. We can distinguish the processing of firewall rules verification into three steps. Firstly, searching the first firewall rule that matches with the packet as fast as possible. Secondly, investigating conflicts of firewall rules. Lastly, analyzing for vulnerabilities and security risks in the rules. The performance evaluation of firewall rule verification is proportional to the speed of searching algorithms. For example, matching a packet with Rule-Base firewall (Sequential searching) is $O(n)$, $O(log_2(n))$ for tree structures, and $O(1)$ for hashing approach, where n is the number of firewall rules.

3 The Policy Mapping Design and Implementation

In this section, we explain the concept and development of our policy mapping model. The aims of the model are to improve the processing time of policy verifying, defeat limitations of IPSet and suitably consume the memory space. Thus, we then focus on hashing functions (the fastest algorithm of searching) to solve the speed of the firewall rule verification. However, hashing functions have one major weakness, which is the collision of hashed keys (key = $\boldsymbol{H}(x)$, H is hashing function and x is the information). With the massive size of data or information, the collision probability of hashed keys will be increasingly high. To avoid this problem, we deployed arrays to be the data structure instead of the $\boldsymbol{H}(x)$. Besides, arrays are also very fast to access and retrieve the stored data without any collision, and they are also easier to understand and implement array structures.

3.1 Key Contributions

In this paper, we make four major contributions. First, we optimize rules of the Rule-Base firewall to a state diagram in order that the order of rules are cleaned form an ambiguous packet matching, called the firewall decision state diagram (FDSD). Second, we present the policy mapping algorithm (PMAP) and data structures for fast handling firewall policies. Third, we get rid of limitations of IPSet and key duplication of hashing function by PMAP. Last, we conduct extensive experiments to evaluate our proposed model against other models.

3.2 PMAP Design

There are five procedures to be included in the design of PMAP:

1) Make firewall rules in the traditional style (Rule-Base) as shown in Step 1 of Figure 2 and Table 2;
2) Build a decision state diagram structure (DSD) from the rule list from Step 1 by using the firewall decision state diagram algorithm (FDSD);
3) Map DSD from step 2 to array structures by the policy mapping algorithm (PMAP);
4) Get the mapped DSD in a format of array data structures;
5) Test the matching speed of PMAP and evaluate performance.

Step 1: Making Rule-Base Firewall Rules

Among user interfaces of firewalls such as Rule-Base ([2, 12, 13]), tree styles ([15]) and the structured query language (SQL) ([11]); almost all of firewall interfaces are Rule-Base. The reason is that it is influenced by the nature of the reading and writing of humans who generally read rules from left-to-right and top-to-bottom; and it is still a popular user interface nowadays. Therefore, we still use the Rule-Base interface to create firewall rules in Step 1. In order to simplify our model, we have presented easy firewall rules that consist of four fields: src_ip, dst_ip, dst_port and act as shown in Table 2.

The src_ip, dst_ip and dst_port has a maximum scope in the range from 1 to 100 only. An a means an acceptance action and d indicates a denial action. For instance, r_1 has source IP addresses between 10 and 30 (src_ip), destination IP addresses (dst_ip) ranging from 20 to 30, a destination port (dst_port) as 80 and an acceptance action (a). In real experiments, we have added one field into firewall rules, that is pro.

Step 2: Building the DSD

The firewall decision state diagram (FDSD) is a great tool for optimizing confusing Rule-Base firewall rules to a clearly firewall decision route. For example, in Table 2, assume that a packet p_i is composed of $src\_ip_i = 15$, $dst\_ip_i = 25$ and $dst\_port_i = 80$. Thus, p_i matches both r_1 and r_3 but both of them are in conflict ($act_{r_1} \neq act_{r_3}$). In case of this rule base, p_i is only matched with r_1. However, rule bases often make administrators confused. To solve the problem, we demonstrate the FDSD to correct uncertain rules. This model was adapted from the firewall decision diagram of Liu [9]. The demonstrations for building DSD by FDSD are shown in Algorithm 1.

Table 2: Easy firewall rules for proving PMAP

no.	src_ip	dst_ip	dst_port	act
r_1	10 - 30	20 - 30	80	***a***
r_2	1 - 15	50 - 60	25 - 30	***a***
r_3	1 - 40	25 - 35	80	***d***
r_4	15 - 45	1 - 100	60 - 90	***d***

We first start a full description of the FDSD procedure in Situation 1 (in the black circle) of Figure 3. The FDSD first reads sets of dst_port of $r_{1,2,3,4}$ from the rule list of the firewall in Table 2. After that, it builds a start state (S0) which is a first state of DSD. Next, it makes a new state ($S1_1$) and creates a link from S0 to $S1_1$ (S0-$S1_1$). This link means a transition state from S0 to $S1_1$ and contains a set of $dst\_port_{r_1}$ as $\{80 - 80\}$. In Situation 2, FDSD reads $dst\_port_{r_2}$ form the rule list. The $dst\_port_{r_2}$ ($\{25\text{-}30\}$) is compared with a set of the transition states from S0 to $S1_1$ (S0-$S1_1$ = $\{80\}$) which $dst\_port_{r_2}$ is not a subset of $dst\_port_{r_1}$ ($dst\_port_{r_2} \nsubseteq dst\_port_{r_1}$). Consequently, FDSD needs to build a new state, namely $S1_2$ in Situation 2, and it establishes a transitional link from S0 to $S1_2$ (S0-$S1_2$). It assigns a set of $dst\_port_{r_2}$ to the S0-$S1_2$. In Situation 3 of Figure 3, FDSD reads $dst\_port_{r_3}$ form firewall rules and compares it with the transitional state S0-$S1_1$ first. As a result, $dst\_port_{r_3}$ is the subset of S0-$S1_1$ ($dst\_port_{r_3} \subseteq dst\_port_{r_1}$: $\{80\} \subseteq \{80\}$). Hence, FDSD does not need to take any action. Lastly, FDSD inserts $dst\_port_{r_4}$ ($\{60\text{-}90\}$) to DSD, it verifies $dst\_port_{r_4}$ with the transitional state S0-$S1_1$ and S0-$S1_2$ respectively. The $dst\_port_{r_4}$ is not subset of S0-$S1_2$ but it is a proper superset of S0-$S1_1$ ($dst\_port_{r_4} \supset dst\_port_{r_1}$: $\{60\text{-}90\} \supset \{80\}$). So, FDSD builds a new state $S1_3$, and makes a new transitional state S0-$S1_3$ in DSD. FDSD computes a set which assigns to S0-$S1_3$ by S0-$S1_3$ = $dst\_port_{r_4}$ - $dst\_port_{r_1}$ ($\{60\text{-}90\}$ - $\{80\}$ = $\{60\text{-}79, 81\text{-}90\}$). The first level of DSD is finished in Situation 4 of Figure 3 (dst_port level).

To establish the Level 2 (dst_ip level) of DSD, FDSD reads $dst\_ip_{r1,2,3,4}$ from the firewall rules. First, it makes a new state $S2_1$ which is the first state in Level 2 as shown in Situation 5 of Figure 4. Then it links a new transition $S1_1$-$S2_1$ from a state $S1_1$ to $S2_1$, and sets dst_ip_{r1} to the link, that is $\{20\text{-}30\}$. In Situation 6, dst_ip_{r2} ($\{50\text{-}60\}$) is verified with $S1_1$-$S2_1$ ($\{20\text{-}30\}$), the result shows that dst_ip_{r2} is not a subset of $S1_1$-$S2_1$ ($\{50\text{-}60\} \not\subset \{20\text{-}30\}$). Consequently, FDSD builds a $S2_2$ state, links a new $S1_2$-$S2_2$ transition and assigns a set of dst_ip_{r2} ($\{50\text{-}60\}$) to

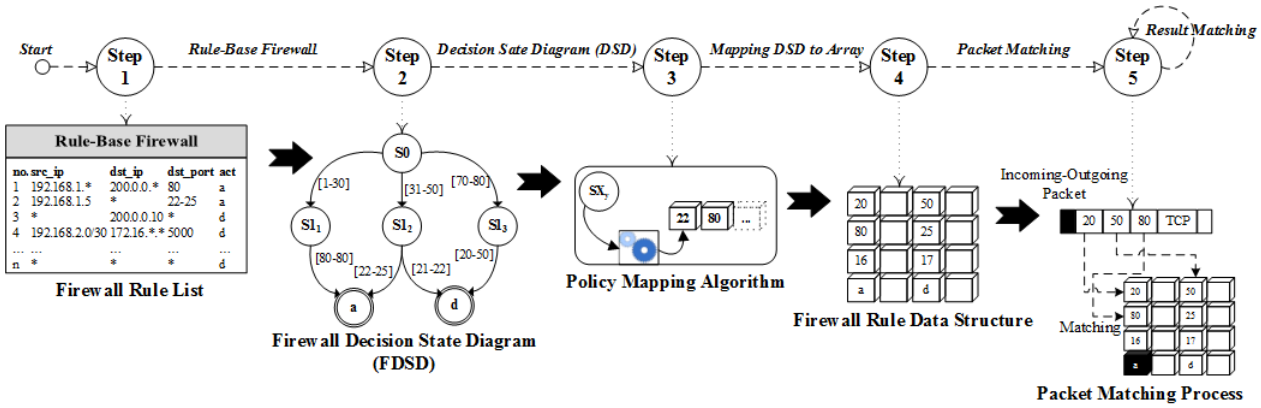


Figure 2: An overview of PMAP design

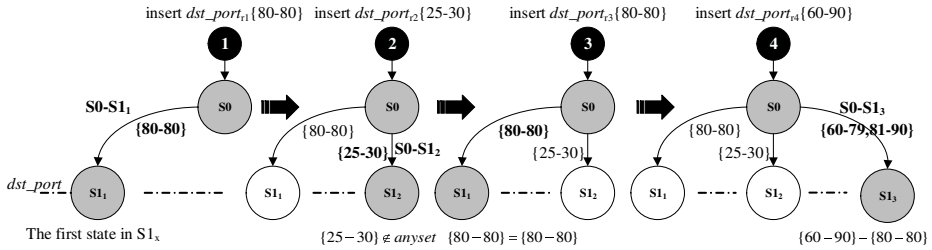


Figure 3: Inserting $dst\_port_{r_{1,2,3,4}}$ to Level 1 of DSD (dst_port)

the $S2_2$ state respectively. Next (Situation 7), a set of dst_ip_{r3} ({25-35}) is inserted into the DSD. It is compared with $S1_1$-$S2_1$ and $S1_2$-$S2_2$, there are several elements in dst_ip_{r3} to be members of $S1_1$-$S2_1$ ({20-30} ∩ {25-35} = {25, ..., 30}) but none of dst_ip_{r3} elements are in $S1_2$-$S2_2$. As a result, FDSD builds a new $S2_3$ state, links a transitive $S1_1$-$S2_3$ to $S2_3$ and sets a set {31-35} ({20-30} - {25-35} = {31, ..., 35}) to $S1_1$-$S2_3$ transition. The last situation (8) of Level 2, the dst_ip_{r4} ({1-100}) is a superset of $S1_1$-$S2_1$ and $S1_1$-$S2_3$ but it is not a subset of $S1_2$-$S2_2$ because they are different port numbers (port numbers of S0-$S1_2$ ⊄ S0-$S1_1$). So, FDSD needs to build a new state as $S2_4$ and $S2_5$, establishes a link $S1_1$-$S2_5$ to this state and defines two sets to $S1_1$-$S2_5$ transition to be {1-19, 36-100}(dst_ip_{r4} - ($S1_1$-$S2_1$) - ($S1_1$-$S2_3$) = {1-100} - {20-30} - {31-35} = {1-19, 36-100}), and defines a set to link $S1_3$-$S2_4$ as {1-100} respectively.

In the last level for building DSD (src_ip), the FDSD feeds $src\_ip_{r1,2,3,4}$ to DSD like the previous situation. For example, src_ip_{r1} is {10-30}, it is processed in a state path from S0, $S1_1$ and $S2_1$ respectively as shown in Situation 9 of Figure 5. It suddenly builds the new sate $S3_1$ because it is the first state in this level there. In this state, $S3_1$ is assigned the a that means an acceptance state. Because of the action of r_1 is an acceptance ($act_{r1} = a$). According to Situation 10, FDSD inserts src_ip_{r2} ({1-15}) to the diagram. The src_ip_{r2} traverses in a path from S0 - $S1_2$ - $S2_2$ and is not a subset of any state. So, FDSD builds a new $S3_2$ state and assigns the status of this state to be a (act_{r2} = accept). Situation 11 in Figure 5, some elements of src_ip_{r3} ({1-40}) are a subset of $S2_1$-$S3_1$ ({10-30}) and some elements are not. Thus, FDSD creates a new $S3_3$ state and the $S2_1$-$S3_3$ transition, assigns the status of this node to be d. It sets a set of {1-9, 31-40} to the $S2_1$-$S3_3$ transition (src_ip_{r3} - $S2_1$-$S3_1$ = {1-40} - {10-30} = {1-9, 31-40}). For some elements that are not a subset of $S2_1$-$S3_1$, the FDSD builds a new state as $S3_4$ for storing a denial action (d) of r_3. The last situation of Level 3 is shown in Situation 12 of Figure 5.

Step 3: Mapping DSD to array data structures

In this section, we fully describe the process of mapping DSD to arrays applied to maintain clearness of firewall rules as shown in Algorithm 2.

From the Algorithm 2, the policy mapping (PMAP) starts by creating an array of one dimension that has the size equal to 1 x a maximum of the port number (in this example equal to 1 x 100), namely S0-S1 as shown in Figure 6. In case of real experiments, we set the size of the S0-S1 array to be 1 x 65,536 (Maximum port number = 0 - $(2^{16} - 1)$). Next, PMAP map sets in a transitional state S0-$S1_1$, S0-$S1_2$ and S0-$S1_3$ to S0-S1 array respectively. In case of S0-$S1_1$, it has a single destination port, that is the port number 80 ({80-80}). T_1 in Figure 6 shows the first tree or state path in DSD Level 1 which is used to mark a position for referring to an array of DSD Level 2. PMAP sets 1 (T_1) to an S0-S1 array in the position 80.

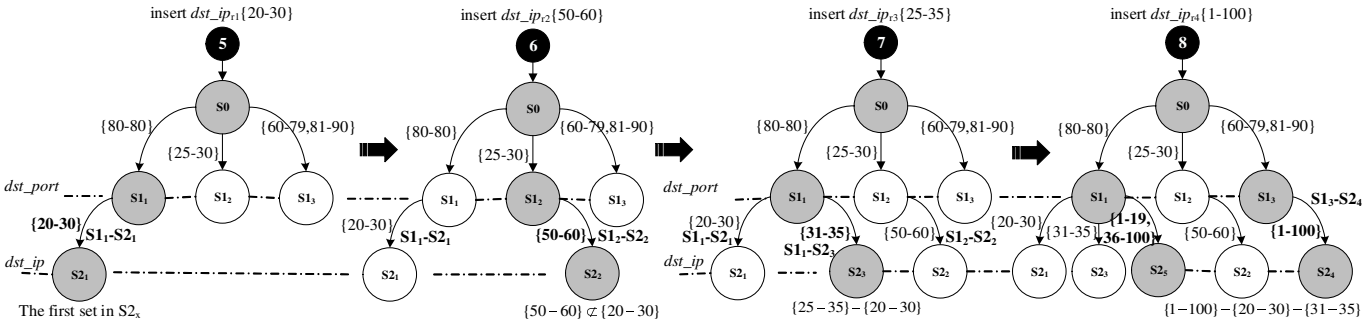


Figure 4: Inserting $dst\_ip_{r1,2,3,4}$ to Level 2 of DSD (dst_ip)

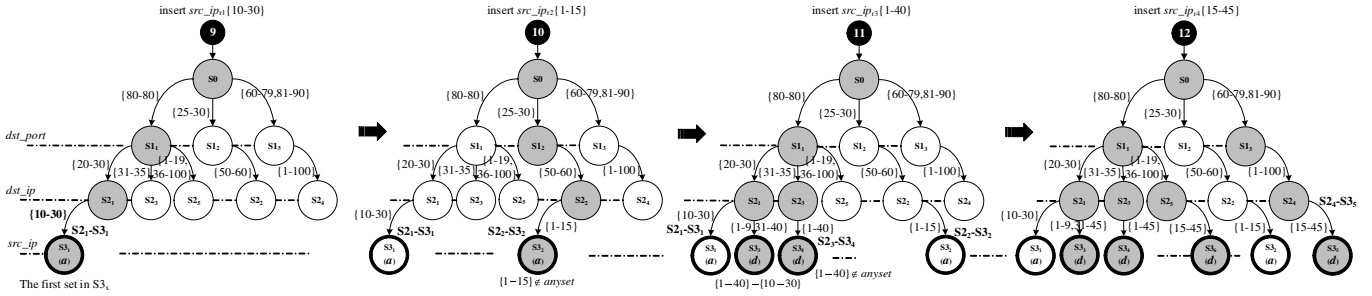


Figure 5: Inserting $src\_ip_{r_{1,2,3,4}}$ to Level 3 of DSD (src_ip)

The number 1 refers to S1-S2 array in the row = 1 and column = $dst\_ip_{p_i}$ (p_i = any packet) of the next level demonstrated in Figure 7. The S0-S1$_2$, which has the number of ports between 25 and 30, maps to S0-S1 array in the position 25 to 30. These positions are set to be 2 (T_2 in DSD). Lastly, S0-S1$_3$ has two subsets consisting of {60-79} and {81-90}. They are mapped to S0-S1 array in position 60 to 79, and 81 to 90 which positions are set to be 3 (T_3 in DSD). The total memory size that maintains DSD Level 1 is 200 bytes (1 row x 100 ports x unsigned 16-bit). An array of an unsigned 16-bit can refer to firewall rules between 1 and 65,536.

Tht map of Level 2 of DSD to S1-S2 array is illustrated in Figure 7. Firstly, PMAP builds the two dimensional array named S1-S2 that allocates the memory size as 20 Kb for handling 100 state paths (100 state paths x 100 of dst_ip x unsigned 16-bit). PMAP maps the transitional state S1$_1$-S2$_1$, S1$_1$-S2$_3$, S1$_2$-S2$_2$ and S1$_3$-S2$_4$ to the S1-S2 array respectively. The results show that S1-S2[1][20 - 30] = 1 (T_1), S1-S2[1][31 - 35] = 2 (T_2), S1-S2[2][50 - 60] = 3 (T_3), S1-S2[3][1 - 19] = 4 (T_4) and S1-S2[3][36 - 100] = 4 (T_4).

Mapping DSD Level 3 to S2-S3 array is displayed in Figure 8. PMAP maps a transition state S2$_1$-S3$_1$ to S2-S3[1][10-30] = a (T_1), S2$_1$-S3$_3$ to S2-S3[1][1-9] = d (T_2), S2$_1$-S3$_3$ to S2-S3[1][31-45] = d (T_2), S2$_3$-S3$_4$ to S2-S3[2][1-45] = d (T_3), S2$_2$-S3$_2$ to S2-S3[3][1-15] = a (T_4) and finally S2$_4$-S3$_5$ to S2-S3[4][15-45] = d ($T_5$2) respectively.

Step 4: Getting the completed DSD in array structures

Firewall rules and state paths: A state path is a route that traverses from the starting state to the accepting state. For example, in Situation 12 of Figure 5, there are five state paths. The first state path is traversable from the starting state (S0) to S1$_1$, S2$_1$ and S3$_1$ (an accepting state) respectively. The second state path is from the starting state (S0), S1$_1$, S2$_1$ and S3$_3$ (an accepting state) and so forth. The number of firewall rules always exceeds the number of state paths (firewall rules $\geq$ state paths). For instance, in Table 2, there are four rules; however, they are generated to five state paths as shown in Situation 12 of Figure 5.

After Step 3 is complete, the arrays contained the DSD consist of S0-S1 for DSD Level 1, S1-S2 for DSD Level 2 and S2-S3 of DSD Level 3. The total memory size of arrays is around 40.2 Kb for holding 100 state paths in this simulation case. However, in the real implementations, the total size of arrays successively increases following by the number of state paths. In case of real implementations, arrays are complicated due to the size of src_ip (32 bits), dst_ip (32 bits), dst_port (16 bits) and pro (8 bits) as shown in Figure 9. Thus, the total of memory size for handling 5,000 state paths is 3.2 GB. That is S0-S1 (dst_port) = 1 x 65,536 x unsigned 16 bits integer x 5,000 = 655.36 MB; S1-S2 (dst_ip) and S2-S3 (src_ip) = 256 x 256 x 16 bits x 5,000 x 4 = 2,621.44 MB and S3-S4 (pro) = 1 x 256 x 16 bits x 5,000 = 2.56 MB.

Step 5: Testing the matching speed and evaluating the performance

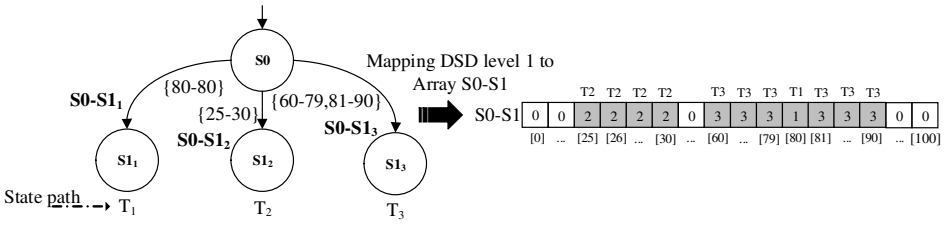


Figure 6: Mapping DSD Level 1 to one dimension array (S0-S1)

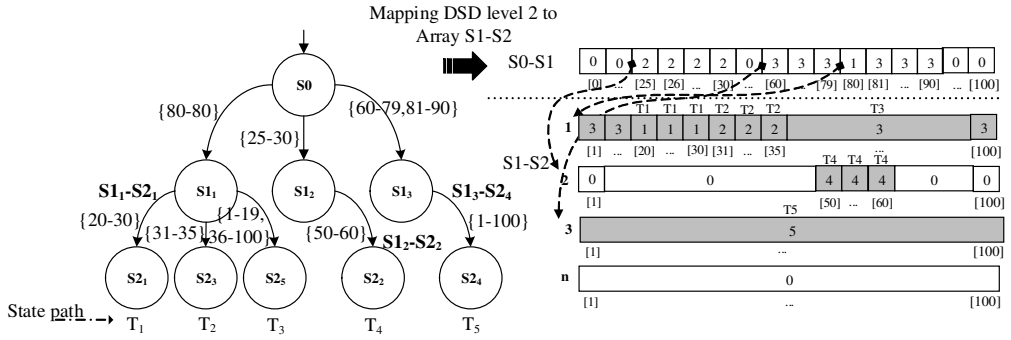


Figure 7: Mapping DSD Level 2 to two dimension array (S1-S2)

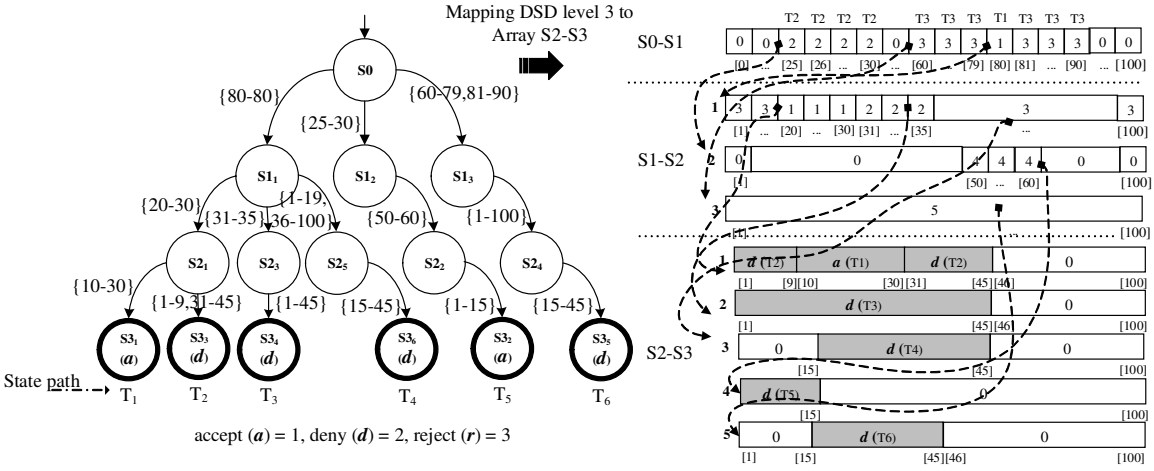


Figure 8: Mapping DSD Level 3 to two dimension array (S2-S3)

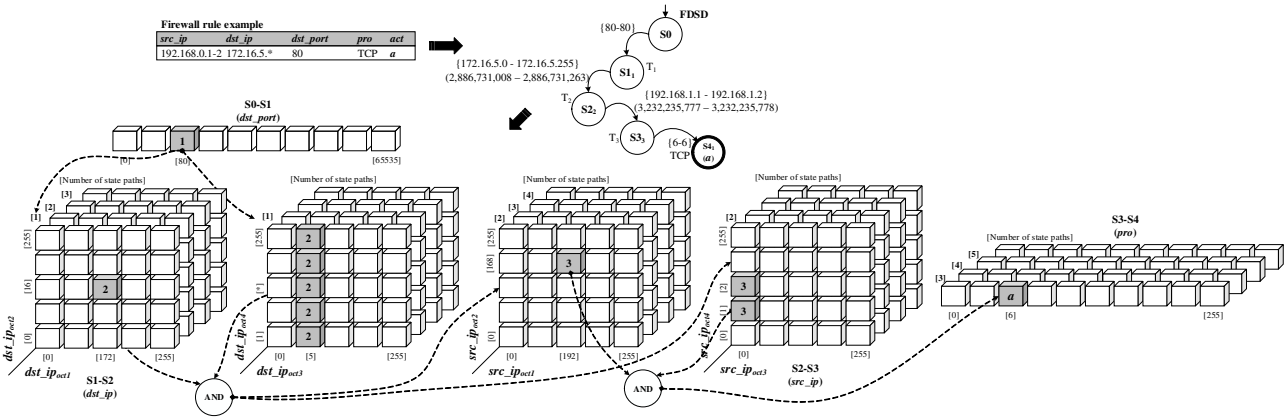


Figure 9: Arrays for real implementation

Algorithm 1 Firewall Decision State Diagram (FDSD)

1: **Input**: Rules $\{r_1, r_2, ..., r_n\}$, where $n \in \mathbb{Z}^+, n \neq 0$
2: **Output**: A decision state diagram (DSD)
3: **if** DSD = $\emptyset$ **then**
4: Build S0 *(starting state)*
5: Set l = 1
6: Set max_level = i *(i = the number of levels)*
7: **while** l $\leq$ max_level **do**
8: Set state, path, loop = 1
9: **while** loop $\leq$ n **do**
10: **if** $dst\_port_{r_{loop}} \subseteq$ S(l-1)-S(l)$_{path}$ **then**
11: do nothing and break
12: **else**
13: Build the state S(l)$_{path}$
14: Create transitional state S(l-1)-S(l)$_{path}$
15: temp = S(l-1)-S(l)$_{path-1}$ - $dst\_port_{r_{loop}}$
16: S(l-1)-S1(l)$_{path}$ = temp
17: **if** l = max_level **then**
18: Set S(l)$_{path}$ = $act_{r_{loop}}$ *(acceptance state)*
19: **end if**
20: path = path + 1
21: **end if**
22: loop = loop + 1
23: **end while**
24: l = l + 1
25: **end while**
26: **end if**
27: Return DSD
28: End

According to Steps 3 and 4 in Figure 2, the firewall rules are already stored in the arrays. Accessing the rules in arrays uses indexes which can directly access the data quickly. So, to operate any instructions on data in arrays is always one instruction ($O(1)$). The algorithm that is used for matching firewall rules in arrays is shown in Algorithm 3 and Figure 10.

3.3 The Policy Mapping Implementation

In this section we reveal the implementation of the policy mapping approach. The details are as follows.

Hardware and Software Development Tools. The policy mapping is developed on the Intel 64-bits processor, Core i7, 2GHz, installed memory (RAM) 8 GB DDR3 and hard disk 750 GB 5400 RPM. In addition to the software development, we chose Python language (version 3.4), Numpy and Psutil to implement our policy mapping running on MS Windows 8 operating system.

Firewall Rule and Packet Generator. In each performance testing scenario, the firewall rule generator software generates the random policies (or rules) from 5 to 5,000 rules, and the intelligently random packets (10,000 packets per epoch) from the packet generator software. According to the random packet algorithm, the algorithm is able to define the ratio of matched packets between 5 and 95% of packets that pass though the firewall.

4 The Performance Evaluation

This section details the performance evaluation of the firewall rule matching by comparing several approaches such as Rule-Base firewall, tree rule, and hashing. We set up the experimental scenarios as shown in Figure 11.

Firstly, the firewall rule generator software generates a number of firewall rules from 5, 10, 50, 100, 200, 350, 500, 750, 1,000, 2,000, 3,000, 4,000 and 5,000 respectively for evaluating the time-space complexity of the algorithms. The number of generated firewall rules in each round is executed 30 rounds per algorithm; that is, the number of generated rules x 30 x the number of tested algorithms (three algorithms for this paper) = 13 x 30 x 3 = 1,170 rounds.

In the next step, the packet generator generates the intelligent random packets for evaluating time-space com-

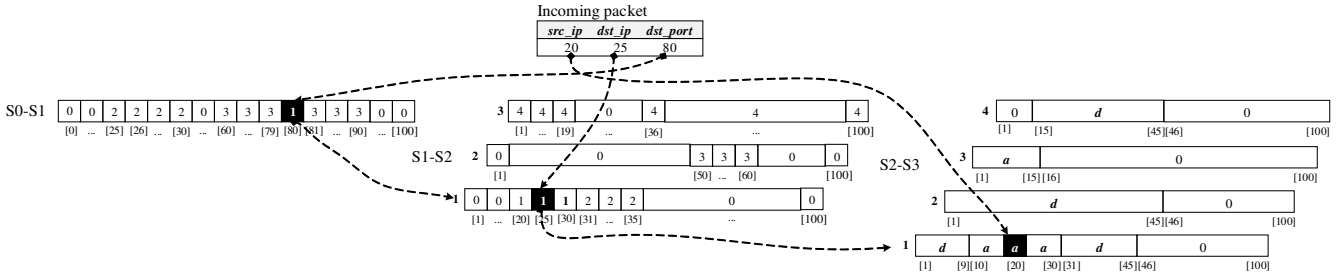


Figure 10: A packet$_i$ matching example

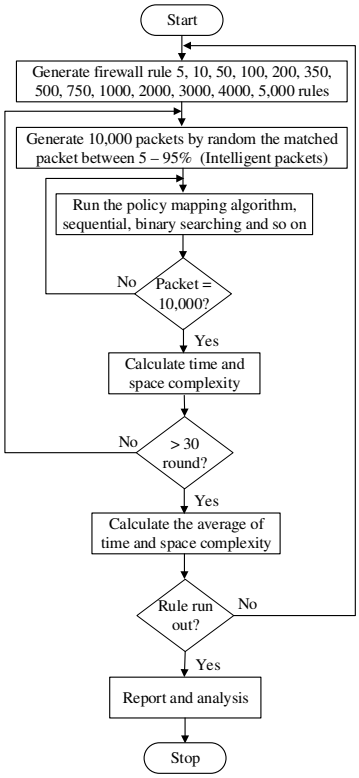


Figure 11: Performance evaluation for matching rules

plexity of each algorithm by 10,000 packets per round. The intelligent random packet applies the random algorithm of the packet generator, which is able to designate the percentage of packet matching with firewall rules. For example, 10 percent of intelligently packet matching of 10,000 packets is 1,000. In our testing, we chose the ratio of random for matching packet from 5 to 95 percent.

Next, we execute each algorithm against generated rules and random packets by a number of tested packets in each algorithm, which is 4,200,000 packets (13 (generated rule) x 10,000 (random packet) x 30 (round)). The chosen algorithms in our experiments are sequential-based approach (generic or Rule-Base firewall), tree and hashing (policy mapping) approach. Finally, we record and plot results (time and space complexity) of each algorithm for analyzing in the next section.

Table 3: Time for generating firewall rule structures (Generic = Rule-Base, Tree rule = Tree structure, and Policy mapping = hashing algorithm)

Time for generating rule structures (sec)			
No.	Generic	Tree rule	Policy mapping
5	0.00208	0.00190	0.01566
10	0.00156	0.00476	0.01562
50	0.00625	0.02187	0.04687
100	0.00521	0.07422	0.13188
200	0.01667	0.27411	0.17188
350	0.02761	0.83719	1.00080
500	0.04416	1.66761	1.32480
750	0.07992	3.78536	1.48440
1,000	0.11055	6.39945	1.78319
2,000	0.22052	24.11578	2.14030
3,000	0.22572	50.02818	2.30150
4,000	0.39503	93.91504	2.92790
5,000	0.49315	148.19096	5.62890

4.1 Time Complexity Analysis

We set up the criteria to evaluate the time complexity of each algorithm in this paper as follows: (i) the time for generating firewall rule structures, and (ii) the time for verifying (matching) firewall rules. The generating time denotes the period of declaring structure variables for storing the data (rules) including time for collecting data to the variables. The verifying time refers to the processing time from the first bounced packet to the last packet on the firewall. The experimental results of the generating time is shown in Table 3 and the graph of the results is illustrated in Figure 12. The results of verifying time is shown in Table 4 and Figure 13 respectively.

From Table 3, the tree rule firewall spends more time on generating data structures than other algorithms. The time complexity will be dramatically grown up from 93.91 to 148.19 seconds while processing firewall rules between 4,000 and 5,000 – as the binary firewall also needs to sort the data. Similarly, the time generating of policy mapping also grew up from 2.92 to 5.62 seconds between executing firewall from 4,000 to 5,000 rules. Because of the majority of the consumption is spent by mapping the firewall policy to arrays. On the other hand, the generic firewall is hardly

Algorithm 2 The Policy Mapping (PMAP)

Input: DSD
Output: Arrays that maintain firewall policies
if DSD $\neq \emptyset$ **then**
  Set Array Sx-Sy = 0
  Set l = 1
  Set max_port = p *(p = 0 - 65535)*
  Set max_level = i *(i = the number of levels)*
  Set max_src-dst$_{ip}$ = k *(k = 0 - 2^{32-1})*
  while l $\leq$ max_level **do**
    count = Count state node of level l
    if l = 1 **then**
      Set i = 1
      S(l-1)-S(l) = Create array 1 x p
      while i $\leq$ count **do**
        T$_i$ = Read set in S(l-1)-S(l)$_i$
        while Read (T$_i$) $\neq \emptyset$ **do**
          Set S(l-1)-S(l)[T$_i$] = i
        end while
        i = i + 1
      end while
    end if
    l = l + 1
    while l $\leq$ max_level **do**
      Set i = 1
      S(l-1)-S(l) = Create array 1 x max_src-dst$_{ip}$ x count
      while i $\leq$ count **do**
        T$_i$ = Read set in S(l-1)-S(l)$_i$
        while Read (T$_i$) $\neq \emptyset$ **do**
          if l = max_level **then**
            Set S(l-1)-S(l)[1][T$_i$][S(l-2)-S(l-1)[i]] = S(l)$_{count}$
          else
            Set S(l-1)-S(l)[1][T$_i$][S(l-2)-S(l-1)[i]] = i
          end if
        end while
        i = i + 1
      end while
    end while
  end while
end if
Return Arrays S0-S1, S1-S2, S2-S3
End

changed.

In the case of matching firewall rule (in Figure 13), the consumed time of the generic firewall increased in a linear aspect ($O(n)$), the tree rule firewall is the logarithmic nature ($O(log_2 n)$) and $O(1)$ for policy mapping. Indeed, policy mapping directly accesses data in any arrays by using indexes, so the speed of accessing is very fast. From Table 4, the time of verification of the policy mapping is faster than a generic and tree rule firewall in every scenarios, and constant. Although, the policy mapping is the best of a verifying speed; however, it has a tiny overhead to access arrays by 3 times in the simulation

Algorithm 3 Matching firewall rules in arrays

Input: Array Sx-Sy, Packet$_i$ (p_i), $(i, x, y \in \mathbb{Z}^+ \mid i, y \neq 0)$
Output: a (accept) or d (deny)
while TRUE **do**
  if (dst_port = S0-S1[dst_port$_{pi}$]) != 0 **then**
    if (dst_ip = S1-S2[dst_port][dst_ip$_{pi}$]) != 0 **then**
      if (result = S2-S3[dst_ip][src_ip$_{pi}$]) != 0 **then**
        return result
      end if
    end if
  end if
end while
End

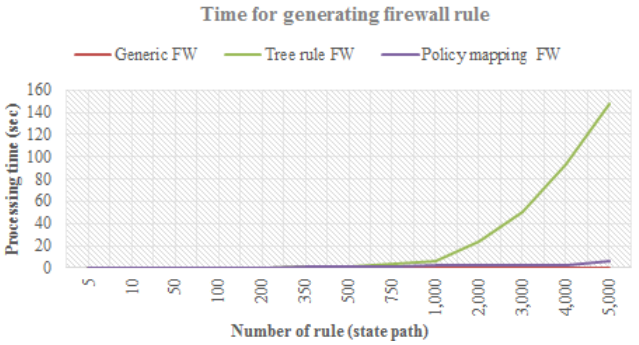


Figure 12: Time for creating firewall rule structures

case or 6 times in real experiment. So, the policy mapping usually consumes a time for verifying to be $O(1)$ x C, where $C = 6$ (*dst_port*:S0-S1, *dst_ip*:S1-S2 x 2, *src_ip*:S2-S3 x 2 and *pro*:S3-S4).

Table 4: Time for verifying of each algorithm

Time for verifying firewall rule (sec)			
No.	Generic	Tree rule	Policy mapping
5	0.06771	0.05505	0.01559
10	0.11094	0.06632	0.01563
50	0.35054	0.07073	0.01563
100	0.44377	0.07949	0.01563
200	1.11984	0.07725	0.01563
350	1.75737	0.07805	0.01562
500	2.68214	0.07985	0.01563
750	4.45257	0.08125	0.01601
1,000	6.55203	0.08453	0.01501
2,000	12.66570	0.08486	0.01563
3,000	13.92543	0.09997	0.01562
4,000	22.35969	0.10676	0.01401
5,000	28.08013	0.10781	0.01801

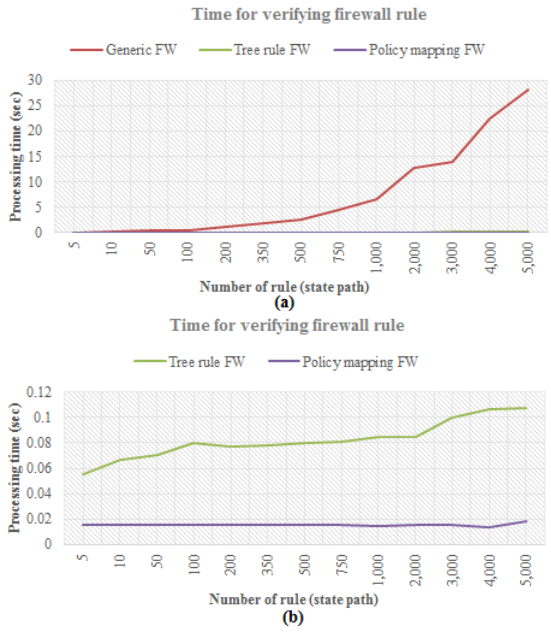


Figure 13: Time verifying for each algorithm. (a) comparing all algorithms, and (b) correlating between Tree rule and Policy mapping only

4.2 Space Complexity Analysis

We classify the memory allocation of algorithms to two groups, which are: (i) the memory space for generating firewall rule structures, and (ii) the memory for running firewall. Table 5 and Figure 14 represent the memory for generating rule structures. From the experimental results, the tree rule firewall consumed the memory space more than other algorithms. As running the tree rule firewall at the rule number 1,000; the memory usage quickly grew up around 1 GB approximately. Because the memory is used for building tree structures of rules. In contrast, the memory usage of generic firewall increased around 4.52 Kb only (at rule no. 1,000); and lightly grew up to 21.52 Kb to execute the firewall rule no. 5,000. The policy mapping continuously consumed about 131 MB (rule no. 1,000) to 655 MB (rule no. 5,000). Because the policy mapping needs more memory to build a firewall decision state diagram (DSD) and arrays. Also, the memory usage of a tree rule firewall tremendously increased to 22.6 GB while it processed the rule number 5,000.

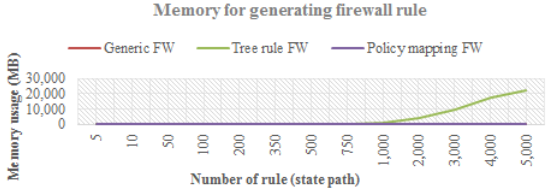


Figure 14: Memory usage for creating rule structures

In the last experiment, we estimated the memory usage of algorithms as shown in Table 6 and Figure 15 by using psutil module in Python while each algorithm was running. Policy mapping consumed the most memory, next order is the tree rule and the last is the generic firewall respectively.

Table 5: memory usage for generating rule structures

Memory for generating firewall rule (MB)			
No.	Generic	Tree rule	Policy mapping
5	0.00007	0.10	0.66
10	0.00010	0.18	1.32
50	0.00027	3.12	6.56
100	0.00046	10.53	13.11
200	0.00084	43.82	26.21
350	0.00145	126.82	45.88
500	0.00214	257.29	65.54
750	0.00312	587.03	98.31
1,000	0.00452	1,057.98	131.08
2,000	0.00828	4,348.74	262.16
3,000	0.01337	9,918.38	393.25
4,000	0.01697	17,873.39	524.33
5,000	0.02152	22,621.06	655.41

Table 6: Memory usage for running firewalls

Memory for running firewalls (MB)			
No.	Generic	Tree rule	Policy mapping
5	22.08	22.10	27.12
10	22.16	22.11	32.05
50	22.39	22.42	72.22
100	22.59	23.05	128.82
200	22.65	25.68	228.91
350	22.49	31.71	372.16
500	22.65	41.39	522.22
750	22.98	63.83	772.25
1,000	23.30	95.83	1,022.57
2,000	23.79	316.58	2,029.97
3,000	24.80	663.22	3,030.30
4,000	25.82	1,172.54	4,031.13
5,000	26.57	1,600.76	5,031.65

5 Conclusions and Future Work

The verification techniques of firewall rule are classified to three major groups: the sequence, tree and hashing. In case of a sequential approach, which is a primitive verifying technique, it is easy to understand and implement, and consumes a small memory space. However, time complexity of a sequence is very slow, that is $O(n)$. In contrast, a tree approach is difficult to understand and implement, and it consumes a large memory space – though it has an excellent processing speed ($O(log_2 n)$). The best speed to verify data is the hashing approach ($O(1)$), but it encounters a trouble of key duplication while performing on enormous data. Unfortunately, it can not satisfactorily be applied to the firewall rule because rules are huge ($\approx 2^{104-bit}$). Another disadvantage of hashing functions

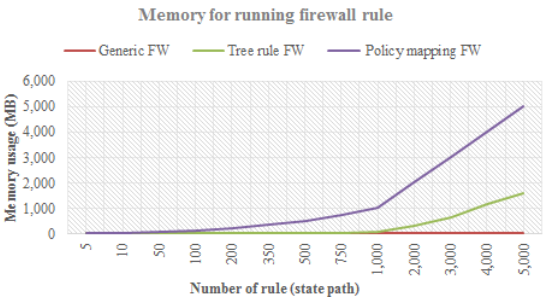


Figure 15: Memory for running firewalls

is that they consume a huge memory space to maintain data.

In this paper, we propose a new algorithm to speed up firewall rule verification, called the policy mapping (PMAP). The distinctive points of the algorithm are: (i) it is as fast as hashing approaches, (ii) it can perform without duplicate keys, (iii) it reasonably consumes the memory space and (iv) it is easy to understand and implement. Our experimental results show that the speed of the policy mapping is faster than sequential and tree rule firewalls, and it also consumes a suitable memory space. Moreover, the policy mapping is as fast as IPSet [12] (top of the high-speed and popular open source firewall today). However, the policy mapping is not limited to the IP network class management like IPSet which is only available for the IP class C and B. Moreover, IPSet always requires to rearrange rules before deploying to the firewall engine.

In the future work, we will optimize the memory size of the PMAP to be better.

References

[1] M. G. Acharya, H. B. Gouda, "Projection and division: Linear-space verification of firewalls," in *Proceedings of The International Conference on Distributed Computing Systems (ICDCS'10)*, pp. 176–180, Genova, June 2010.

[2] A. Blyth, "An architecture for an XML enabled firewall," *International Journal of Network Security*, vol. 8, no. 1, pp. 31–36, 2009.

[3] M. Chapple, A. Striegel, "An analysis of firewall rulebase (mis) management practices," *ISSA: The Global Voice of Information Security*, 2009. http://mike.chapple.org/an-analysis-of-firewall-rulebase-mismanagement-practices/

[4] P. G. Clark and A. Agah, "Firewall policy diagram: Structures for firewall behavior comprehension," *International Journal of Network Security*, vol. 17, no. 2, pp. 150–159, 2013.

[5] M. G. Gouda and A. X. Liu, "Structured firewall design," *Computer Networks*, vol. 51, pp. 1106–1120, 2007.

[6] H. Hamed, A. El-Atawy, and E. Al-Shaer, "On dynamic optimization of packet matching in high-speed firewalls," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1817–1830, 2006.

[7] IETF, *Internet Official Protocol Standards*, 2008. `http://tools.ietf.org/html/rfc5000`

[8] S. Khummanee, A. Khumseela, and S. Puangpronpitag, "Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules," in *Proceedings of The Computer Science and Software Engineering (JCSSE'13)*, pp. 93–98, Abu Dhabi, May 2013.

[9] A. X. Liu, "Formal verification of firewall policies," in *IEEE International Conference on Communications*, pp. 1494–1498, Beijing, May 2008.

[10] A. X. Liu and M. G. Gouda, "Diverse firewall design," *IEEE Transaction on Parallel and Distributed Systems*, vol. 19, no. 9, pp. 1237–1251, 2008.

[11] A. X. Liu and M.G. Gouda, "Firewall policy queries," *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, vol. 20, no. 6, pp. 766–777, 2009.

[12] Netfilter, *IP Set*, Aug. 24, 2015. `http://ipset.netfilter.org/index.html`

[13] Netfilter, *IPTables*, June 25, 2015. `http://ipset.netfilter.org/iptables.man.html`

[14] J. Touch, E. Lear, et al., *Service Name and Transport Protocol Port Number Registry*, RFC 6335, Aug. 6, 2015. `http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml`

[15] P. N. Zhiyuan, X. Tan, T. C. He, "Improving cloud network security using the tree-rule firewall," *Future Generation Computer Systems*, vol. 30, pp. 116–126, 2013.

Suchart Khummanee is a Ph.D student at Khon Kaen University, Khon Kaen, Thailand. His research is in the field of Computer Networks and Security.

Kitt Tientanopajai is a full Professor of computer engineering with Khon Kaen University, Khon Kaen, Thailand. His research interests focus on Free/Open Source Software, Information Security, Quality of Service Routing, Computer Networks and Educational Technology.

New Random Generator of a Safe Cryptographic Salt Per Session

Younes Asimi[1], Abdallah Amghar[2], Ahmed Asimi[1], and Yassine Sadqi[1]
(Corresponding author: Ahmed Asimi)
Departments of Mathematics and Computer Science & Information Systems and Vision Laboratory, Ibn Zohr University[1]
Department of Physic & Information Systems and Vision Laboratory, Ibn Zohr University[2]
B. P. 8106, City Dakhla, Agadir, Morocco.
(Email: *asimiahmed2008@gmail.com*)
(Received Nov. 14, 2013; revised and accepted Sept. 5 & Dec. 16, 2014)

Abstract

Nowadays, client authentication in Web applications for each user based on passwords and a statically salts [11, 13, 18, 19]. The aim of this article is to propose random generator of a safe cryptographic salt per session ($RGSCS$). The interest to introduce this regenerator is to contribute to the evolution of the cryptographic quality of the systems of strong zero knowledge authentication based on passwords. In Section 3, we propose a model for regeneration a SOTS based on random functions and on CRC code. To study the behavior of the $RGSCS$, which is the objective of Section 4, we have, in one hand, defined and proved a metric on the finite set of periodic binary sequences not necessarily the same period, the uncorrelation, the impact of the distribution of lengths and the unpredictability of primitive signals and in the other hand, evaluated the performance of our purpose by using several tests. The outcome showed that $RGSCS$ has a chaotic behavior. As for Section 5, is devoted to the implementation of our $RGSCS$ algorithm under PHP5. This article is finished by a conclusion.

Keywords: *CRC code, passwords, random generator RGSCS, safe one time salt, strong zero knowledge authentication*

1 Introduction

Design methods of passwords are the first authentication techniques in the web, which is based in one hand on hash functions for example MD5 [23] (complete collisions) and $SHA-1, 2$ [17, 22] (theoretical collisions) and in the other hand on statically salts.

The objective of this paper is to improve the authentication mechanism by preposition and behavioral study of a new model that regenerates a safe one time salt for each session successfully connected. This system is based on pseudo-random functions and the error detection code (CRC) [21] with a variable length to ensure the integrity of the generated binary sequences.

This paper is organized as follows: In Section 3, we propose a design of a new model to regenerate a safe one time salt ($RGSCS$) composed by three processes. The first process consists to regenerate the one time salt from random functions defined in PHP, denoted by OTS. To increase the security level of OTS, which is the goal of the process II, we apply the CRC of variable lengths on primitive signal associate to OTS for regenerate a safe one time salt, denoted by SOTS. Hence the authentication parameter for each user is ($SOTS$, N) where N is the number of bits equal to one in a primitive signal of SOTS. The process III consists to check the integrity of SOTS for each attempt to connect and to update the authentication parameter after successful connection. The Section 4 studies the behavior of $RGSCS$. Therefore we define and prove a metric on the finite set of periodic binary sequences not necessarily the same period. And we finished this section by the evaluation the performances of $RGSCS$ by using several tests according the length, period and distribution of primitive signals of $SOTS$. As for the fifth section, we realized an implementation of our $RGSCS$ algorithm which reassures its cryptographic nature and its capacity to detect any unexpected perturbations of OTS and the some conclusion are draw in final section.

In this section, we introduce the notations that will be used throughout this paper in Table 1.

2 Related Work

The concept of salts was introduced by Morris and Thompson [11] as another alternative of one time passwords OTP to ensure the security password on $UNIX$. They are based on storing passwords salted and hashed to reduce the risk of password file compromise [1]. We also underline that several extensions have been proposed to

Table 1: Notations

$\mathbb{N}$:	Set of natural numbers.
$\mathbb{R}$:	Set of real numbers.
F_K:	Set of periodic binary functions of same period K.
Γ:	Set of periodic binary functions not necessarily the same period.
$L(S)$:	Length of binary sequence S.
$S_P(F)$:	Primitive signal of binary function F.
$P(x)$:	Probability of event x.
$Lmc(K_1, \ldots, K_r)$:	Lowest common multiple of positive integers $K_1, \cdots, K_r$.
CRC:	Cyclic Redundancy Check.
$SOTS$:	Safe One Time Salt.
OTS:	One Time Salt.
$NIST$:	National Institute of Standards and Technology.
$\ll$:	Inferior.
$\gg$:	Superior.

evolve the security of the password against multiple attacks specifically against Phishing and Spyware attacks. The technical of SpoofGuard [3] is a browser extension that examines Web pages and notifies the user when data requests may be part of a spoof attack (Phishing). Halderman et al [7] proposed a mechanism operates entirely on the client. This extension allows the reassurance of the passwords against the attacks of dictionary by means of a hash function. We are stretching the hash function, it can complicate the calculation of the original password. More critically, it generates the static passwords unable to resist against multiple attacks (Phishing or Replay attack). In 2005, the technique PwdHash [13] was developed for Internet Browsers Explored and Mozilla Firefox. It allows to evolve the security of the passwords in the Web applications. It generates a different password for each site seamlessly. This extension applies a cryptographic function on a password in clear and its private salt stored in the client computer. In general, this extension allows to generate a global salt (equivalent to the domain name of remote site) specific to each site. This technique helps to prevent Phishing attack but remains unable to resist against network attacks (Man in the middle, Replay attack) and attacks against servers (brute force attack, dictionary attack, theft of the database). In addition, neither the robustness and nor the integrity of this salt are verified. Indeed, this salt allows to extend the length of passwords chosen by the user. Yet, it is incapable to touch at the bottom the cryptographic quality of the passwords. More critical, for the users who have the same original passwords will have the same final password. In general, all the studies in this field have shown that the problem of memorization and storage is among the major causes of the inability of users to respond to recommendations of the computer security related to passwords [2, 4, 6, 12, 20]. It is necessary to note also that numerous studies on the JavaScript attacks showed that the implementation in complete safety of the hashing in the browser is rather difficult on the modern Web applications [9].

At that time, the $HTTPS$ protocol was the only way to ensure the confidentiality and the integrity of data which transit on the network. But, thanks to an analytical study made by American researchers [10], the monitoring of the Web traffics leaves enough information even if the data which transit are encrypted. However, the security of the authentication systems based on the passwords represents a big challenge to the development of the digital enterprises. The interest to introduce this $RGSCS$ regenerator is to contribute to the evolution of the cryptographic quality of the passwords to meet the requirements of the IT security and also push aside the limits and the concerns of the users which are unable to maintain complex passwords. In our proposal, following to the cryptographic nature of the OTS, it is almost impossible to find the same final password for two users with the same original passwords.

3 RGSCS Algorithm

A salt is a safe one time (SOTS) if it's specific for each user session, regenerated by a pseudo-random and unfalsifiable regenerator.

- **Specific to each session:** After the opening of each session a new salt will be regenerated. Therefore, the decrease in the probability of attacking users.
- **Pseudo-random:** Its aim is to produce dynamics OTS with uncorrelated primitive signals.
- **Unfalsifiable:** The regenerated binary sequences are protected with a mechanism for errors detecting CRC with variables lengths to check their integrity.

We refer to [11, 13, 18, 19], to get the following results:

- **A global salt:** Consists to add the only salt for all sites and for all users (equivalent to the domain name of remote site). This is easy technique to perform.

Furthermore, this salt is not secret, which explains that the use of this technique is just for increase the complexity of time. Because only one dictionary necessary to attack all members of the site.

- **One salt for each user:** This technique is similar to the previous one. Except in this case, we have a user-specific salt. This is the most common technique used so far due to the following factors: The simplicity of programming and the level of protection against dictionary attacks.

- **A salt per session:** This is a technique requires the handling of twice salts: A global salt and a salt regenerated for each session. A global salt used for password deformation to register before you encrypt with a cryptographic hash function. The other salt is used to protect all stored passwords. This technique is very difficult to implement yet.

In all cases, the regeneration of these salts based on a random strings or on a random number generated by the function rand(). Also, the implementation of these techniques is based on AJAX and JavaScripts that generate the following drawbacks [9, 21].

- **The function Rand():** Uses a linear congruential regenerator and generates a sequence of integers. Hence, the interval of numbers introduced by this function is limited. In fact, we can test all possible numbers with a simple script.

- **Scripts AJAX:** Checks the existence of an identifier of a user after each entry of a character in the login field to return the salt that is transmitted in clear text. This facilitates dictionary attacks and brute force attacks.

- **The JavaScripts:** The client-side security is not assured in spite of the use of CryptJS.

To remedy the problems of static salt and salt per session, we propose a new conception of random generator of a safe cryptographic salt ($RGSCS$). This algorithm allows, from three functions: Rand(), Microtime() and mcrypt_create_iv(), to regenerate a safe one time salt. It consists of three processes. The first aims to regenerate a dynamic salt for each successful connection. The second applies the CRC of variable lengths (that we call CVL) on primitive signal associate to OTS for regenerate a safe and one time salt ($SOTS$). The third checks the integrity of SOTS and updates the authentication parameters ($SOTS$, N).

3.1 Process I

The main objective of this process is the regeneration of OTS, by using three functions Rand(), Microtime() and mcrypt_create_iv(), as follows:

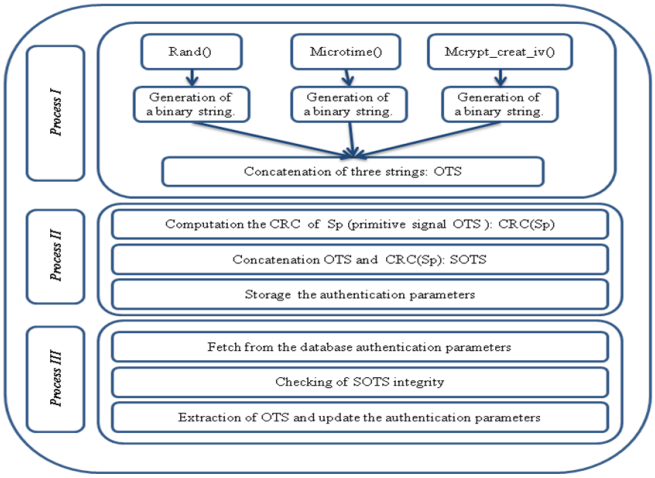


Figure 1: RGSCS algorithm

- Let S, R and T be three strings regenerated respectively by Rand(), Microtime() and mcrypt_create_iv().

- Let $S2$, $R2$ and $T2$ be three binary representations of S, R and T respectively.

- OTS is the concatenation of $S2$, $R2$ and $T2$.

- OTS is seen as a concatenation of primitive signals.

3.2 Process II

This process improves the security level of any dynamics salt created in process I, specifically the OTS integrity, as flows:

- Let S_P be the primitive signal of OTS and G a polynomial generator of CRC.

- K is the number of S_P bits set to 1.

- $M = max(K, strelen(S_P) - K)$.

- $N = strelen(S_P) moduloM$.

- The polynomial G is associated to binary representation of N.

- Compute $R = CRC(S_P)$.

- $SOTS$ is the concatenation of S_P and R.

- Store $SOTS$ and N in database.

- The authentication parameters per session are SOTS and N.

3.3 Process III

This process occurs for each new connection. It builds on the previous two processes. It will verify the integrity of $SOTS$ through each attempt to connect and update authentication parameters $(SOTS, N)$ after each successful connection. For that we proceed as follows:

- Fetch the authentication parameters $SOTS$ and N.
- Compute G associate to N.
- Check of $SOTS$ integrity.
- If this verification is successful, then we deduce OTS of $SOTS$.
- Otherwise the validation is failed.
- In the favorable case, we use the previous two processes to update $SOTS$ and N.

4 Behavioral Study of $RGSCS$ Algorithm

To estimate the complexity of the $RGSCS$ algorithm, a behavioral study is dedicated to analysis of the generated primitive signals. However, the testing of these classes of binary functions shows that not necessarily the same period. Hence, the difficulty of computing their Hamming distances and analyze the results. Therefore, we are reduced to define and prove a distance which is an extension of a Hamming distance of sets of periodic strings that are not necessarily the same period.

4.1 Metric on the Set of Periodic Binary Strings

From [15, 16], we deduce some results:

Definition 1. *We call a binary function, all function defined from $\mathbb{N}$ into $\{0,1\}$.*

Definition 2. *For each binary function F, we associate the only binary string f defined by $f = F(0)\ F(1)\ F(2)\ \cdots\ F(n)\ \cdots$. And if there is an integer k such that $f = F(0)\ F(1)\ F(2)\cdots F(k-1)\ F(0)\ F(1)\ F(2)\cdots$, therefore F is periodic with period k, and if more k is the smallest integer, then the sequence $F(0)\ F(1)\ F(2)\cdots F(k-1)$ is called primitive signal of f, which denotes by $S_P(F)$. In this case, $F(n) = F(n \bmod L(S_P(F)))$ for all $n \in \mathbb{N}$.*

And if f is a finite sequence, we extended to a unique periodic infinite sequence with a length of its primitive signal is a divider of $L(f)$.

We call regenerative signal of F, that we denote by $S_R(F)$, a concatenation of the its primitive signal.

Definition 3. *Let S and S' be two elements of F_K. S and S' are equal and we denote $S = S'$ if and only if $S(n) = S'(n)$ for all $n \in \mathbb{N}$.*

Theorem 1. *Let S and S' be two elements of F_K. The following conditions are equivalent:*

1) $S = S'$.

2) $S_P(S) = S_P(S')$.

4.1.1 Metric on the Finite Set of Periodic Binary Sequences of Same Period

In this section, we focus on the definition of the distance between binary sequences with same period K.

Definition 4. *[16] A metric space is a nonempty set E together with a function d called a metric, denoted by (E, d).*

Definition 5. *[16] Let E be a metric space. The metric d on E is a function defined from $E\times E$ into $\mathbb{R}^+$ and satisfied the following axioms for all x, y, z in E:*

1) $d(x,y)\geq 0$ et $d(x,y) = 0 \Longleftrightarrow x = y$.

2) $d(x,y) = d(y,x)$.

3) $d(x,y)\leq d(x,z) + d(z,y)$.

Lemma 1. *[16] Let S, S' and S'' be three elements of F_K. We consider the following sets:*
$T = \{i \in \{0,...,J-1\}/S(i) \neq S'(i)\}$,
$H = \{i \in \{0,...,J-1\}/S(i) \neq S''(i)\}$
and $G = \{i \in \{0,...,J-1\}/S''(i) \neq S'(i)\}$.
we have $T \subset H \cup G$.

Proposition 1. *Let S and S be two elements of F_K. The function D:*

$$\begin{array}{rccc} D & : & F_K\times F_K & \longrightarrow & \mathbb{N} \\ & & (S, S') & \longmapsto & \displaystyle\sum_{i=0}^{K-1}((S(i)+S'(i))\%2). \end{array}$$

Proof. We have $D(S,S') = \displaystyle\sum_{i=0}^{K-1}((S(i)+S'(i))\%2) \geq 0$ for all $(S,S') \in F_K^2$.

$$\begin{array}{rcl} D(S,S') = 0 & \Leftrightarrow & \displaystyle\sum_{i=0}^{K-1}((S(i)+S'(i))\%2) = 0 \\ & \Leftrightarrow & (S(i)+S'(i))\% = 0\ \forall i \in \{0,...,K-1\} \\ & \Leftrightarrow & S(i) = S'(i)\ \forall i \in \{0,...,K-1\} \\ & \Leftrightarrow & S = S'\ (Theorem\ 1). \end{array}$$

$$\begin{array}{rcl} D(S,S') & = & \displaystyle\sum_{i=0}^{K-1}((S(i)+S'(i))\%2) \\ & = & \displaystyle\sum_{i=0}^{K-1}((S'(i)+S(i))\%2) \\ & = & D(S',S). \end{array}$$

We have $T \subset H \cup G$ (Lemma 1).

$$\begin{aligned} D(S,S') &= \sum_{i=0}^{K-1}((S(i)+S'(i))\%2) \\ &= \sum_{i\in T}((S'(i)+S(i))\%2) \\ &\leq \sum_{i\in H}((S(i)+S''(i))\%2) \\ &\quad +\sum_{i\in G}((S''(i)+S'(i))\%2) \\ &\leq D(S,S'')+D(S'',S'). \end{aligned}$$

Therefore D is a metric on F_K. □

4.1.2 Metric on the Finite Set of Periodic Binary Sequences not Necessarily the Same Period

In this section, we denote by Γ a finite set of periodic binary sequences, not necessarily the same period and the lowest common multiple of their periods.

Proposition 2. *The function D': $\Gamma\times\Gamma\to[0,1]$ defined by:*

$$D'(S,S') = \frac{\sum_{i=0}^{T-1}((S(i)+S'(i))\%2)}{T}$$

is a distance on Γ.

The proof of this proposition is similar to the proof of Proposition 1.

Corollary 1. *Let S and S' be two elements of Γ of periods k and k' respectively and $K = Lmc(k,k')$.*

The function D': $\Gamma\times\Gamma\to[0,1]$ defined by:

$$D'(S,S') = \frac{\sum_{i=0}^{K-1}((S(i)+S'(i))\%2)}{K}$$

is a normalized distance of Γ.

Proof. It suffices to see that:

$$\sum_{i=0}^{T-1}((S(i)+S'(i))\%2) = \frac{\sum_{i=0}^{K-1}((S(i)+S'(i))\%2)}{K}\times T$$

Thus, from proposition 2, we deduce that:

$$D'(S,S') = \frac{\sum_{i=0}^{K-1}((S(i)+S'(i))\%2)}{K}.$$

□

Definition 6. *[16] A square matrix $H=(d_{ij})$ is called metric matrix if it satisfies the following properties:*

1) $d_{ij} = d_{ji}$ for all i and j (symmetric).
2) $d_{ij} = 0$ for all $i = j$ (diagonalized).
3) $d_{ij} \geq 0$ for all $i \neq j$.

Proposition 3. *For all S and S' in Γ, the normalized distance D' satisfies the following equality:*

$$D'(S,S') = 1 - D'(S,\overline{S'}).$$

Proof. Let M be the cardinal number between two bits strings S and S' such that have the same period. Then we get:

$$M = \sum_{i=0}^{K-1}((S(i)+S'(i))\%2).$$

Hence

$$D'(S,S') = \frac{M}{K}$$

or

$$\begin{aligned} \sum_{i=0}^{K-1}((S(i)+\overline{S'(i)})\%2) &= K - \sum_{i=0}^{K-1}((S(i)+S'(i))\%2) \\ &= K - M. \end{aligned}$$

Then

$$D'(S,\overline{S'}) = \frac{K-M}{K} = 1 - \frac{M}{K}.$$

We also deduce

$$D'(S,S') = 1 - D'(S,\overline{S'}).$$

□

Definition 7. *Two binary strings of the same period are called strongly correlated if the knowledge of one, within reasonable time, determines the other. The opposite case, they are said to be weakly correlated.*

Definition 8. *We say that two binary strings S and S' of the same period K are weakly correlated if:*

$$D'(S,S') \simeq D'(S,\overline{S'}).$$

Propriety 1. *For all S and S' in Γ, we say that two binary strings are weakly correlated.*

The proof of this proposition relies on Proposition 3 and on Definition 6.

Corollary 2. *If $D'(S,S') \ll 0.5$, we say that S and S' are highly correlated. If $D'(S,S') \gg 0.5$, then $D'(S,\overline{S'}) \ll 0.5$, we say S and $\overline{S'}$ that are highly correlated.*

Proposition 4. *Let $S_{m,N}$ be the set of binary strings such that its waist is between m and $m+N$.*

1) The cardinal of $S_{m,N}$ is $\#S_{m,N} = 2^m(2^{N+1}-1)$.
2) If the elements of $S_{m,N}$ are equiprobable then for all $S \in S_{m,N}$, we get $P(S) = \frac{1}{\#S_{m,N}}$.

Proof. We know that the number of binary strings of length k is 2^k, therefore:

$$\begin{aligned} \#S_{m,N} &= \sum_{k=m}^{m+N} 2^k \\ &= 2^m \sum_{S=0}^{N} 2^S \\ &= 2^m(2^{N+1}-1). \end{aligned}$$

We hence get Proposition 4. □

4.2 Behavioral Study of RGSCS Algorithm

After explaining the principals and the advantages of each component process of the *RGSCS* algorithm, a behavioral study dedicates to highlight its characteristics: The distribution of lengths of primitive signals and distances of the regenerated binary sequences.

4.2.1 The Lengths Distribution of Primitive Signals

In this section, we study the components functions of *RGSCS* according to the lengths of their primitive signals for one hundred, two hundred and three hundred iterations.

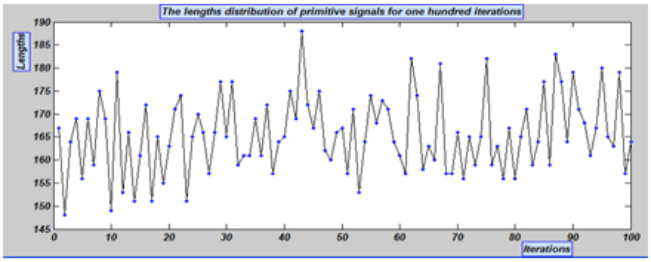


Figure 2: The lengths distribution of primitive signals for one hundred iterations

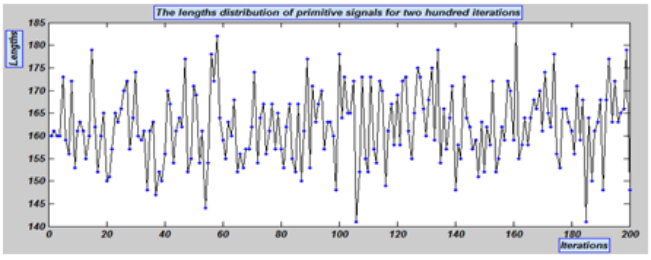


Figure 3: The lengths distribution of primitive signals for two hundred iterations

From the Figures 2, 3, 4 and Proposition 4, we deduce that the lengths distribution of primitive signals generated is random and unpredictable over time. The range of lengths of sequences is enough large and more subtle (between 140 and 185 bits).

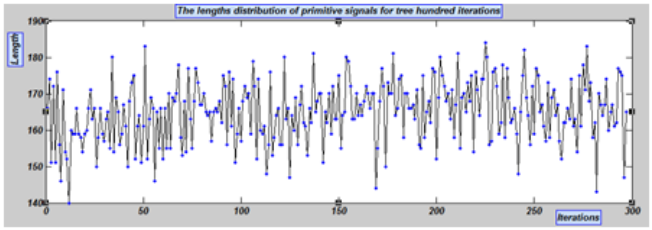


Figure 4: The lengths distribution of primitive signals for three hundred iterations

4.2.2 The Distances Distribution Between Binary Sequences

In this section, we examine the distribution of standardized three classes of distance sequences, a class of one hundred, two hundred and three hundred observers by computing the normalized distance between these sequences. Let S_i and S_j be tow elements of a given class. Set $d_{ij} = D(S_i, S_j)$ for $i, j \in \{1, ..., m\}$. The symmetric square matrix $(d_{ij})_{1 \leq i,j \leq m}$ called distance matrix for its class.

The analysis of Hamming distance matrix [8] associated to each given class will give an estimation of the complexity, correlation and coverage of its sequences. The above figures show the histograms of distance matrix of three classes: One hundred, two hundred and three hundred iterations.

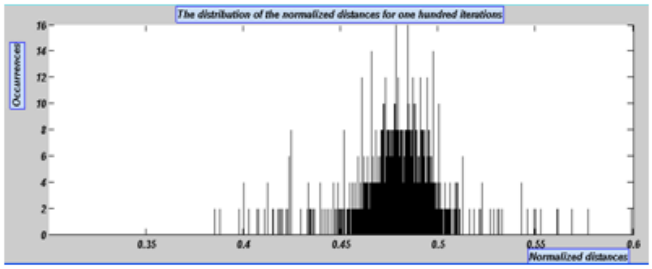


Figure 5: The distribution of normalized distances for one hundred iterations

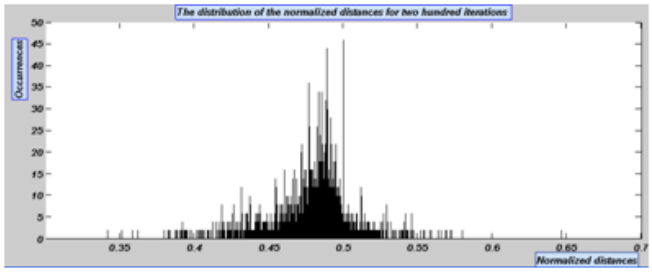


Figure 6: The distribution of normalized distances for two hundred iterations

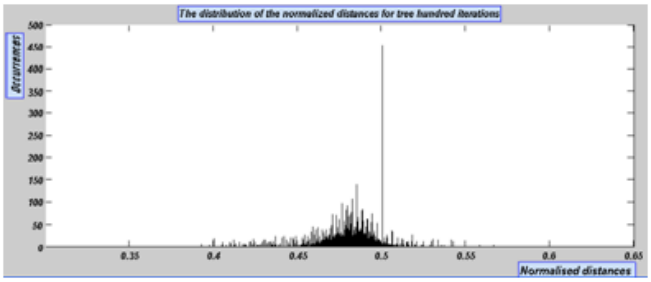


Figure 7: The distribution of normalized distances for three hundred iterations

From these histograms (5, 6, 7), we can divide regions of interest in three periods:

- From 0.35 to 0.45: in this portion, the distribution of the normalized distances phenomenon seems chaotic.
- Between 0.45 and 0.52: In this portion, we have an accumulation of normalized distances. But with a distribution seems a bit like Gaussian curve followed by small peaks. So, we do have the not correlation of generated primitive signals able to withstand the collision problem.
- Between 0.52 and 0.6: almost the same as the first portion.

The results obtains are almost identical in all three histograms. The only difference is the apparition of a peak nearest 0.5 percent for the three hundred iterations. This is normal because we have normalized between binary functions and the theory of distances required to have this peak. Hence, our purpose has unpredictable characteristics, witch is recommended by $NIST$ [14]. This enables us to ensure the cryptographic nature of the $RGSCS$ algorithm. Finally, we can summarize these features as follows:

- The distribution of lengths and periods are random.
- The primitive signals are unpredictable.
- The integrity of all OTS is provided by CRC of variable lengths.

5 Implementation of RGSCS Algorithm

Our $RGSCS$ algorithm can be executed in different types of authentication system especially banking systems and Web applications, more generally, in all the systems of cyberspace. We aim, in this work, to evolve the cryptographic quality passwords against various types of attacks. In particular, the attacks which found on the usurpation of the private data during their transmissions or their storages or on the limits of the users related to choices, memorization and storage of the passwords [1, 5]. The robustness of an authentication system is the measure of its ability to deal with all vulnerabilities, to resist against various types of attacks degrading the level of security and also to innovate an authentication system that meets the limits user. Thus, according to the theoretical and behavioral study of our $RGSCS$ algorithm, the cryptographic quality of the primitive signals regenerated is assured. Likewise, the originality and validity of any regenerated salt is provided to avoid any falsifications or perturbations unexpected of OTS primitive signals during execution. The execution of our model is done in a transparent manner. Furthermore, the portability is ensured to facilitate the movement of the internet users to a specific browser (Portability of authentication system) and avoid the risks related with the problems of storing sensitive data on the client side. For greater security, the integrity of salts exchanged between the communicating entities is also insured by the integration of a technique of errors detection CRC of variables lengths which adapts itself with all polynomials generator regenerated during any session. The interest to introduce this control mechanism of integrity aims at avoid the problem of collision of code CRC of fixed length (two primitive signals giving the same checksum), also, to meet the needs of our architecture which regenerates polynomials generator of the variables lengths.

The implementation of our proposed scheme to regenerate safes one time salts $SOTS$ specific any session opened by a user. The regenerated salts cannot be guess by the previous values. They are unfalsifiable, uncorrelated random and unpredictable.

In the following example, we have regenerated three safe one time salts by using the programming language PHP.

We aim by this work to evolve at the authentication systems based on the virtual passwords. For this interest, we have checked during the conception of our $RGSCS$ algorithm on the cryptographic quality and the integrity control of salts OTS regenerated. A priori, this mechanism is designed to preserve the validity of salts against any modifications or perturbations unexpected. Figure 8 shows three safe one time salt regenerated for three different successive sessions.

- **The binary representation of one time salts OTS:** It is the binary representation of the salts regenerated. According to these results, the one time salts regenerated are neither periodic nor the same length.
- **The real representation of one time salts OTS:** It is the $ASCII$ code representation of the primitive signals of any salt regenerated. The chain of the characters returned consists of very difficult random characters which can be memorized or guessed. They exceed the capacity of encoding information of the browsers. For this, we rewrote the characters in hexadecimal seen that the most supported by mod-

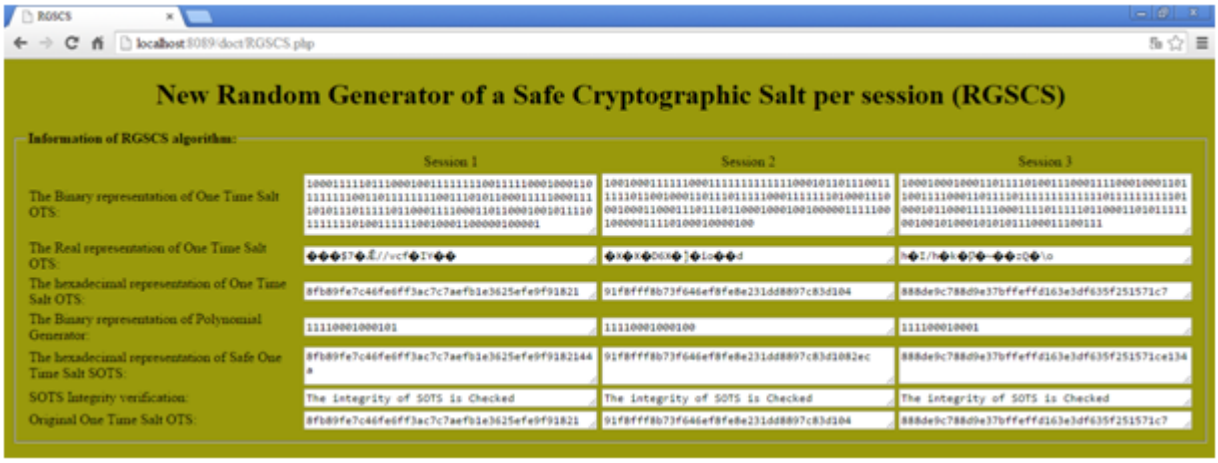


Figure 8: Implementation of RGSCS algorithm

ern browsers. This result reassures once again the cryptographic quality of our regenerator.

- **The hexadecimal representation of one time salts** OTS**:** It is the hexadecimal representation of primitive signals of any salt regenerated.
- **The binary representation of polynomials generator:** It is the binary representation of the polynomials generator which will be used to calculate the cyclic checksum CRC specific to any primitive signal OTS and to verify their integrity.
- **The hexadecimal representation of safe one time salts SOTS:** It is concatenation of the one time salt and its calculated cyclic checksum CRC.
- **SOTS integrity verification:** The primitive signals specific to any salts can undergo to falsifications or perturbations unexpected during their transitions on the thread. For this, we have to reapply this mechanism of errors detection CRC on the $SOTS$ primitive signal. If the cyclic checksum CRC is zero, then the integrity of $SOTS$ is checked, otherwise, the validity of $SOTS$ has been altered.
- **Original one time salts** OTS**:** If the integrity verification of $SOTS$ is successful, then, we deduct the original primitive signal. For this, we should remove the cyclic checksum CRC of SOTS. This OTS will be used for the regeneration of a new virtual password.

Mathematically, the CRC code is a surjective function, which means we can have the same checksum for several different primitive signals. Whence, an attacker can seek to change a primitive signal in order to have same checksum without need to modify the polynomial generator. But, further to the dynamic cryptographic nature of the $SOTS$ and to the polynomials generative which depend on the complexity of the SOTS, this attack remains very distant especially for the most connected users.

6 Conclusion

Awareness about the impact of computer sciences security on the quality of applications and websites, has leaded us to the development of a new $RGSCS$ algorithm. This paper has come in order to strengthen and improve user authentication based on passwords and a safe one time salts.

Certainly in terms of security, authentication, integrity, simplicity, predictability, transparency and complexity all play an important role. Subjectively, our purpose based on simple and programmable operations in most programming languages. Hence, we associate a random primitive signal to a salt. Then there are almost impossible to divine its through successive iterations. And to make sure of their integrities, we adopt an error detection code mechanism CRC that can adapt with all polynomials generator. However, $RGSCS$ algorithm is able to detect any changes on any primitive signal constituting its salt. Thus, we develop new authentication architecture that can completely deform the password or digital signatures in general and improve the level of security against multiple types of attacks: dictionary, brute force, phishing, collision, spyware, and rainbow table attacks. Finally, we summarize its characteristics as follows:

- The length and period of generated binary sequences are random.
- The nature of the generated primitive signal is pseudo-random and in some situations seems chaotic.
- The integrity of OTS is ensured by integration mechanism CRC error detection of variables lengths.
- The complexity of the $RGSCS$ algorithm comes from the unpredictable nature of any generated primitive signal. However, for an attack, the divination of the following strings becomes very complicated or impossible.

References

[1] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in *The Ninth Workshop on the Economics of Information Security*, pp. 1–48, 2010.

[2] D. Boyd, *Answers to Questions from Twitter on Teen Practices*, Technical Report, Apophenia, 2009.

[3] N. Chou, R. Ledesma, Y. Teraguchi, and J. Mitchell, "Client-side defense against web-based identity theft," in *Proceedings of Network and Distributed Systems Security (NDSS'04)*, pp. 1–16, 2004.

[4] P. Dourish, E. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the wild: User strategies for managing security as an everyday, pactical problem," *Personal Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[5] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*, pp. 657–666, Dalian, China, 2007.

[6] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proceedings of the Second Symposium on Usable Privacy and Security*, pp. 44–55, 2006.

[7] J. A. Halderman, B.Waters, , and E. Felten, "A convenient method for securely managing passwords," in *Proceedings of the 14th International World Wide Web Conference*, pp. 471–479, 2005.

[8] R. W. Hamming, "Error-detecting and error-correcting codes," *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[9] Matasano, Javascript Cryptography Considered Harmful, 2011. (`http://www.matasano.com/articles/javascript-cryptography`)

[10] B. Miller, L. Huang, A. D. Joseph, and J. D. Tygar, *I Know Why You Went to the Clinic: Risks and Realization of https Traffic Analysis*, Technical Report, arXiv preprint arXiv: 1403.0297, 2014.

[11] R. Morris and K. Thompson, "Password security: A case history," *Communication of ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[12] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," in *Seventh Australasian Information Security Conference*, pp. 71–78, 2009.

[13] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," in *Proceedings of the 14th conference on USENIX Security Symposium (SSYM'05)*, vol. 14, pp. 2, 2005.

[14] A. Rukhin, et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Technical Report, NIST Special Publication - 800-22 (Revision 1a), 2010.

[15] A. Sabour and and A. Lbekkour A. Asimi, "Genetic regenerator of pseudo-random sequences RA NMJ," *International Journal of Computer Science and Network Security*, vol. 7, no. 1, pp. 594–597, 2007.

[16] A. Sabour, A. Asimi, and A. Lbekkouri, "The three states functions: Theoretical foundations and estimated complexity," in *The 3rd International Conference on Information Technology*, pp. 1–9, 2007.

[17] S. K. Sanadhya and P. Sarkar, "New collision attacks against upto 24-step sha-2," in *Advances in Cryptology (Indocrypt'08)*, LNCS 5365, pp. 91–103, Springer, 2008.

[18] D. Seguy and P. Gamache, *Security PHP 5 et MySQL*, Eyrolles, 2007.

[19] C. Shiflett, *Essential PHP Security*, O'Reilly, 2005.

[20] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Password sharing: Implications for security design based on social practice," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 895–904, 2007.

[21] W. Steinmetz and B. Ward, *PHP Clés En Main*, 76 scripts efficaces pour enrichir vos sites web, 2008.

[22] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Advances in Cryptology (Crypto'05)*, LNCS 3621, pp. 17–36, Springer, 2005.

[23] X. Wang and H. Yu, "How to break MD5 and other hash functions", in *Advances in Cryptology (EUROCRYPT'05)*, LNCS 3494, pp. 19–35, Springer, 2005.

Younes Asimi received his Master's degree in Computer Science and Distributed Systems in 2012 from Departments of Mathematics and Computer Sciences, Faculty of Science, University Ibn Zohr, Agadir,Morocco. He is currently pursuing Ph.D in Departments of Mathematics and Computer Sciences, Information Systems and Vision Laboratory,Morocco. His research interests include Authentication Protocols, Computer and Network Security and Cryptography.

Abdallah Amghar is a Professor in the Physics Department, Faculty of Science, University Ibn Zohr, Morocco. He received his DEA and DES degree in 1994 from Department of Physics, Faculty of Science, University Hassan II, Morocco. In January 2002, he has Ph.D degree in microelectronic from Department of Physics, Faculty of Science, University Ibn Zohr, Morocco. His areas of research interests include Cryptography, DNT, embedded systems and microelectronic.

Ahmed Asimi received his PhD degree in Number theory from the University Mohammed V - Agdal in 2001. His research interest includes Number theory, Code theory, and Computer Cryptology and Security. He is a full professor at the Faculty of Science at Agadir since 2008.

Yassine Sadqi received his Master in the field of Computer Science and Distributed Systems at the Ibn Zoher University in 2012. He is currently a Ph.D. candidate of the Ibn Zoher University, Agadir, Morocco. His main field of research interest is computer security, cryptography and authentication in Web applications.

Security Analysis on "Secure Untraceable Off-line Electronic Cash System"

Feng Wang[1,2], Chin-Chen Chang[2], and Changlu Lin[3]
(Corresponding author: Chin-Chen Chang)
College of Mathematics and Physics, Fujian University of Technology[1]
Fuzhou, Fujian, 350118, China
Department of Information Engineering and Computer Science, Feng Chia University[2]
100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
College of Mathematics and Computer Science, Fujian Normal University[3]
Fuzhou, Fujian, 350117, China
(Email: alan3c@gmail.com)
(Received Aug. 29, 2013; revised and accepted Feb. 18 & Aug. 12, 2014)

Abstract

In 2013, Baseri et al. proposed an untraceable off-line electronic cash scheme from the RSA cryptosystem. They used a method that injects the expiration date and the spenders identity onto the coin to prevent double spending. The authors claimed that the scheme provides the properties of anonymity, unforgeability, double spending detection, and date attachability. Unfortunately, we find that there are security flaws in terms of verifiability, unreuseablity, and unforgeability. First, the verifiable method of e-cash in their scheme is not correct according to Euler's Theorem. Second, malicious spenders can inject a false identity in the withdrawal phase due to the homomorphic property of modular operation. Therefore, coins can be doubly spent without being detected. Finally, a malicious spender or merchant can forge valid coins using existing coins.

Keywords: Electronic cash, off-line, unforgeability, unreuseablity, verifiability

1 Introduction

Electronic cash (e-cash) is a more convenient method of payment in electronic commerce compared with traditional paper cash. In general, there are three entities involved in an e-cash scheme: the bank, the spender, and the merchant. The spender withdraws the e-cash from his/her account and then pays it to the merchant for some goods or services. The merchant sends his/her e-cash to the bank and deposits it in his/her account. An e-cash scheme should have the properties of unforgeability, untraceable, verifiability, unreuseability [12] and might have properties such as divisibility, transferability, anonymity revocation, and so on. Depending on whether the bank attends to the transaction between the spender and the merchant, the e-cash scheme can be classified into two categories: on-line and off-line. In an on-line scheme [2, 8, 10], the bank must attend the transaction to detect double spending; thus, it exhausts the most resources of the bank. An off-line scheme is more efficient, because the bank does not attend the transaction. Therefore, the off-line e-cash scheme is a more attractive research area.

Since Chaum et al. [3] proposed the first off-line e-cash scheme, numerous such schemes have been presented [1, 4, 6, 7, 13]. Unfortunately, there is not a globally acceptable off-line scheme, and many existing schemes have security flaws [1, 5, 9]. For example, in 2013, Baseri et al. [1] found that Eslami and Talebi's scheme [6] had three faults: attacking double spender detection, forging the expiration, and cheating on exchange protocol. They proposed a secure untraceable off-line electronic cash scheme from the RSA cryptosystem. In order to prevent double spending, they injected the expiration date and the spender's identity onto the coin in withdrawal phase. In [1], it was claimed that the author's scheme provides the properties of anonymity, unforgeability, double spending detection, and date attachability. However, we find that Baseri et al.'s scheme has some security flaws such as verifiability, double spending detection, and unforgeability. First, the verifiable method of e-cash in this scheme is not correct according to Euler's Theorem [11], and we revise the flaw in Subsection 3.1. Second, malicious spenders can withdraw coins without injected their actual identities using the homomorphic property of modular operation. Therefore, the bank cannot detect their identities when double spending occurs. Finally, a malicious spender or merchant can forge valid coins using existing coins due to the homomorphic prop-

erty of modular operation.

The rest of the paper is organized as follows. In Section 2, we review Baseri et al.'s scheme [1]. We describe the flaws of Baseri et al.'s scheme in detail in Section 3, and the conclusion is given in Section 4.

2 Review of Baseri et al.'s Scheme

Baseri et al.'s [1] scheme has four participants: a central authority, the bank, the spender, and the merchant. It also has six phases: initialization, opening an account, withdrawal, payment, deposit, and exchange. We describe them as follows, excluding the exchange phase for simplification.

2.1 Initialization

The central authority (CA) selects two distinct large primes p and q, computes $n = p \cdot q$ and $\varphi(n) = (p-1)\cdot(q-1)$, picks two random numbers $g_1, g_2 \in_R Z_n^*$ with the same large prime order l. Next, he/she picks two random numbers $e'_B, e_B \in_R Z^*_{\varphi(n)}$ such that $e'_B < e_B$ and $\gcd(e'_B, \varphi(n)) = \gcd(e_B, \varphi(n)) = 1$, computes $1/e'_B$ and $1/e_B$ such that $e'_B \cdot (1 \setminus e'_B) = e_B \cdot (1 \setminus e_B) = 1(\bmod \varphi(n))$. Then, CA selects a one-way hash function H, publishes $(g_1, g_2, n, e'_B, e_B, H)$ and keeps $(1/e'_B, 1/e_B, \varphi(n))$ secretly.

2.2 Opening an Account

Step 1. Spender → Bank: ID_C and a zero knowledge proof that he/she knows u.

The spender selects $u \in_R Z^*_{e_B}$, computes $ID_C = g_1^u (\bmod\ n)$ such that $g_1^u \cdot g_2 \neq 1 (\bmod\ n)$, and generates a zero knowledge proof that he/she knows the discrete logarithm of ID_C.

Step 2. Bank → Spender: O_1.

The bank checks the zero knowledge proof and computes $A = ID_C \cdot g_2 (\bmod\ n)$, and $O_1 = A^{1/e_B} (\bmod\ n)$.

2.3 Withdrawal

Step 1. Spender → Bank: (ω_1, ω_2, t).

The spender chooses $x_1, x_2 \in_R Z^*_{e'_B}$ and $s, b_1, b_2 \in_R Z_n^*$. Then, the spender computes $A' = A^s (\bmod\ n)$, $B = g_1^{x_1} \cdot g_2^{x_2} (\bmod\ n)$, $\omega_1 = B \cdot b_1^{e'_B} (\bmod n)$, and $\omega_2 = (A' + B) \cdot b_2^{(e_B * t)} (\bmod\ n)$.

Step 2. Bank → Spender: (O_2, O_3), where $O_2 = \omega_1^{1/e'_B} (\bmod\ n)$, and $O_3 = \omega_2^{1/(e_B * t)} (\bmod\ n)$.

Step 3. The spender stores $(A', B, s_1, s_2, s_3, t)$ as his/her $Coin$, where $s_1 = O_1^s (\bmod n)$, $s_2 = O_2/b_1 (\bmod n)$, and $s_3 = O_3/b_2 (\bmod\ n)$.

Note that s_1, s_2, and s_3 are signatures of A', B, and $A' + B$, respectively, with the private keys $1/e_B$, $1/e'_B$, and $1/(e_B * t)$, respectively.

2.4 Payment

Step 1. Spender → Merchant: $Coin$, where $Coin = (A', B, s_1, s_2, s_3, t)$.

Step 2. Merchant →Spender: d.

The merchant checks whether $A' \neq 0$, and s_1, s_2, and s_3 are valid signatures of A', B, and $A' + B$, respectively, and computes $d = H(A', B, ID_M, date||time)$.

Step 3. Spender → Merchant: (r_1, r_2), where $r_1 = d \cdot u \cdot s + x_1 (\bmod\ e_B)$, and $r_2 = d \cdot s + x_2 (\bmod\ e_B)$.

Step 4. The merchant accepts the $Coin$ if equation $g_1^{r_1} \cdot g_2^{r_2} = (A')^d \cdot B (\bmod\ n)$ holds.

2.5 Deposit

Step 1. Merchant → Bank: $(Coin, r_1, r_2)$.

Step 2. The bank checks the merchant's identity and the validity of the $Coin$. If valid, he/she checks whether the $Coin$ is in the bank's database; if not, he/she stores the $Coin$. If there is another $(Coin, r'_1, r'_2)$ in the bank's database, then the bank can detect the identity of the malicious spender by $u = \frac{r_1 - r'_1}{r_2 - r'_2} (\bmod\ e_B)$, and $ID_C = g_1^u (\bmod\ n)$.

3 Security Analysis of Baseri et al.'s Scheme

3.1 Dissatisfying Verifiability

In Steps 3 and 4 of the payment phase, the spender sends $r_1 = d \cdot u \cdot s + x_1 (\bmod e_B)$, and $r_2 = d \cdot s + x_2 (\bmod e_B)$ to the merchant, who accepts the $Coin$ if $g_1^{r_1} \cdot g_2^{r_2} = (A')^d \cdot B (\bmod n)$ holds. In order to ensure that $g_1^{r_1} \cdot g_2^{r_2} = (A')^d \cdot B (\bmod n)$ holds, the r_1 and r_2 should be revised as $r_1 = d \cdot u \cdot s + x_1 (\bmod \varphi(n))$ and $r_2 = d \cdot s + x_2 (\bmod \varphi(n))$, respectively, according to Euler's theorem [11], which states that if n and a are coprime positive integers, then $a^{\varphi(n)} = 1 (\bmod n)$. However, the spender does not know the value $\varphi(n)$. Thus, we can only adopt an inefficient method to revise them into $r_1 = d \cdot u \cdot s + x_1$, $r_2 = d \cdot s + x_2$. Furthermore, the value in Step 2 of the deposit phase must be modified as $u = (\frac{r_1 - r'_1}{r_2 - r'_2} (\bmod \varphi(n))) (\bmod\ e_B)$.

3.2 Attacking Double Spending Detection

A malicious spender can forge one identity in the withdrawal phase to avoid being detected when he/she doubly spends the e-cash. Suppose that the malicious spender

changes his/her identity ID_C into ID_C^*. When double spending occurs, the bank cannot find who doubly spends the e-cash even if he/she has computed ID_C^*. There are two methods to forge the spender's identity, as described in the following.

3.2.1 Forging Identity Independently

We first describe how to forge one identity without any help from a third party.

Step 1. The malicious spender executes the withdrawal phase similar to Baseri et al.'s scheme except that he/she changes ω_1 and ω_2 into $\omega_1 = g_1 \cdot b_1^{e'_B} (\bmod n)$, and $\omega_2 = g_1 \cdot b_2^{(e_B * t)} (\bmod n)$. Of course, the coin that he/she obtained is not a valid coin, but he/she can obtain $s_2 = O_2/b_1 (\bmod n) = g_1^{1/e'_B}$, $s_3 = O_3/b_2 (\bmod n) = g_1^{1/(e_B * t)}$. Then, he/she computes $g_1^{1/e_B} = s_3^t (\bmod n)$, and denotes $\alpha_1 = g_1^{1/e_B} (\bmod n)$, $\beta_1 = g_1^{1/e'_B} (\bmod n)$, and $\gamma_1 = g_1^{1/(e_B * t)} (\bmod n)$. Similarly, he/she can obtain $\alpha_2 = g_2^{1/e_B} (\bmod n)$, $\beta_2 = g_2^{1/e'_B} (\bmod n)$, and $\gamma_2 = g_2^{1/(e_B * t)} (\bmod n)$.

Step 2. The spender executes the withdrawal phase similar to Baseri et al.'s scheme except that he/she changes A' into $A'^* = g_1^{a_1} \cdot g_2^{a_2} (\bmod n)$, where $a_1, a_2 \in_R Z_{e'_B}^*$. Then, he/she computes $s_1^* = \alpha_1^{a_1} \cdot \alpha_2^{a_2} (\bmod n)$. This is a valid signature of A'^*, because $(s_1^*)^{e_B} = (\alpha_1^{a_1} \cdot \alpha_2^{a_2})^{e_B} = ((g_1^{1/e_B})^{a_1} \cdot (g_2^{1/e_B})^{a_2})^{e_B} = g_1^{a_1} \cdot g_2^{a_2} = A'^* (\bmod n)$. Furthermore, he/she can change r_1 and r_2 into $r_1^* = d \cdot a_1 + x_1$ and $r_2^* = d \cdot a_2 + x_2$, respectively, in the payment phase and can pass all verifications, because $g_1^{r_1^*} \cdot g_2^{r_2^*} = g_1^{d \cdot a_1 + x_1} \cdot g_2^{d \cdot a_2 + x_2} = (g_1^{a_1} \cdot g_2^{a_2})^d \cdot g_1^{x_1} \cdot g_2^{x_2} = (A'^*)^d \cdot B (\bmod n)$.

Thus, the spender withdraws a valid coin $(A'^*, B, s_1^*, s_2, s_3)$ without being injected his/her identity. If he/she doubly spends the coin, the bank can obtain (r_1^*, r_2^*) and $(r_1^{*\prime}, r_2^{*\prime})$ with identical coin $(A'^*, B, s_1^*, s_2, s_3)$ and compute $u^* = \frac{r_1^* - r_1^{*\prime}}{r_2^* - r_2^{*\prime}} = (\frac{a_1}{a_2} \bmod \varphi(n)) (\bmod e_B)$. However, the coin does not contain the identity of spender, and the bank cannot find out who doubly spends the coin with the value u^*.

3.2.2 Forging Identity Jointly

We give a method for constructing one forging identity if two malicious spenders collaborate. The attack succeeds due to the homomorphic property of modular operation.

Step 1. Two malicious spenders C_1 and C_2 execute the opening an account phase. At the end of this phase, they have their identities $ID_{C_1} = g_1^{u_1} (\bmod n)$, and $ID_{C_2} = g_1^{u_2} (\bmod n)$, respectively, and the values $A_1, A_2, O_{C_1,1}, O_{C_2,1}$.

Step 2. The spenders execute the withdrawal phase similar to Baseri et al.'s scheme, except that they work together to compute $A'^* = A_1^{a_1} \cdot A_2^{a_2} (\bmod n)$ instead of A' for some $a_1, a_2 \in_R Z_n^*$, and $s_1^* = O_{C_1,1}^{a_1} \cdot O_{C_2,1}^{a_2} (\bmod n)$ instead of s_1. Here, s_1^* is a valid signature of A'^*, because $(s_1^*)^{e_B} = (O_{C_1,1}^{a_1} \cdot O_{C_2,1}^{a_2})^{e_B} = (O_{C_1,1}^{e_B})^{a_1} \cdot (O_{C_2,1}^{e_B})^{a_2} = A_1^{a_1} \cdot A_2^{a_2} = A'^* (\bmod n)$. Furthermore, they work together to compute $r_1^* = d \cdot (a_1 \cdot u_1 + a_2 \cdot u_2) + x_1$ and $r_2^* = d \cdot (a_1 + a_2) + x_2$ instead of r_1 and r_2 in the payment phase and can pass all verifications since $g_1^{r_1^*} \cdot g_2^{r_2^*} = g_1^{d \cdot (a_1 \cdot u_1 + a_2 \cdot u_2) + x_1} \cdot g_2^{d \cdot (a_1 + a_2) + x_2} = ((g_1^{u_1} \cdot g_2)^{a_1} (g_1^{u_2} \cdot g_2)^{a_2})^d \cdot g_1^{x_1} \cdot g_2^{x_2} = (A'^*)^d \cdot B (\bmod n)$.

Thus, they can withdraw a valid coin $(A'^*, B, s_1^*, s_2, s_3)$ without being injected their actual identities. If they doubly spend the coin, the bank can obtain (r_1^*, r_2^*) and $(r_1^{*\prime}, r_2^{*\prime})$ with identical coin $(A'^*, B, s_1^*, s_2, s_3)$ and compute $u^* = \frac{r_1^* - r_1^{*\prime}}{r_2^* - r_2^{*\prime}} = (\frac{a_1 \cdot u_1 + a_2 \cdot u_2}{a_1 + a_2} \bmod \varphi(n))) (\bmod e_B)$. However, the coin does not contain the identity of spender, and the bank cannot find who doubly spend the coin with the value u^*.

3.3 Attacking Unforgeability

Suppose a malicious spender has a valid coin (A', B, s_1, s_2, s_3). He/she can forge valid coins independently. Furthermore, a malicious merchant can forge a valid coin by cheating the spender or with the help of the spender.

3.3.1 Forging Coins Independently

We first forge a valid coin by a malicious spender independently.

Step 1. This is identical to Step 1 in Subsection 3.2.1.

Step 2. With coin (A', B, s_1, s_2, s_3), the spender picks two random values $a_1, a_2 \in_R Z_{e'_B}^*$ and computes $A'^* = A' \cdot g_1^{a_1} \cdot g_2^{a_2} (\bmod n)$, $B^* = B \cdot g_1^{a_1} \cdot g_2^{a_2} (\bmod n)$, $s_1^* = s_1 \cdot \alpha_1^{a_1} \cdot \alpha_2^{a_2} (\bmod n)$, $s_2^* = s_2 \cdot \beta_1^{a_1} \cdot \beta_2^{a_2} (\bmod n)$, and $s_3^* = s_3 \cdot \gamma_1^{a_1} \cdot \gamma_2^{a_2} (\bmod n)$. In the payment phase, the spender computes $r_1^* = d \cdot (u \cdot s + a_1) + x_1 + a_1$, and $r_2^* = d \cdot (s + a_2) + x_2 + a_2$ because he/she knows the value of (u, s, x_1, x_2).

Obviously, s_1^*, s_2^*, and s_3^* are valid signatures of A'^*, B^*, and $A'^* + B^*$, respectively. We can verify by the following equations: $(s_1^*)^{e_B} = (s_1 \cdot \alpha_1^{a_1} \cdot \alpha_2^{a_2})^{e_B} = (s_1 \cdot (g_1^{1/e_B})^{a_1} \cdot (g_2^{1/e_B})^{a_2})^{e_B} = A' \cdot g_1^{a_1} \cdot g_2^{a_2} = A'^* (\bmod n)$, $(s_2^*)^{e'_B} = (s_2 \cdot \beta_1^{a_1} \cdot \beta_2^{a_2})^{e'_B} = B \cdot g_1^{a_1} \cdot g_2^{a_2} = (s_2 \cdot (g_1^{1/e'_B})^{a_1} \cdot (g_2^{1/e'_B})^{a_2})^{e'_B} = B \cdot g_1^{a_1} \cdot g_2^{a_2} = B^* (\bmod n)$, and $(s_3^*)^{(e_B * t)} = (s_3 \cdot \gamma_1^{a_1} \cdot \gamma_2^{a_2})^{(e_B * t)} = (s_3 \cdot (g_1^{1/(e_B * t)})^{a_1} \cdot (g_2^{1/(e_B * t)})^{a_2})^{(e_B * t)} = (A' + B) \cdot g_1^{a_1} \cdot g_2^{a_2} = (A'^* + B^*) (\bmod n)$. Furthermore, the spender can compute (r_1^*, r_2^*) which satisfies $g_1^{r_1^*} \cdot g_2^{r_2^*} = g_1^{d \cdot (u \cdot s + a_1) + x_1 + a_1} g_2^{d \cdot (s + a_2) + x_2 + a_2} = ((g_1^{u \cdot s} \cdot g_2^s) \cdot (g_1^{a_1} \cdot g_2^{a_2}))^d \cdot ((g_1^{x_1} \cdot g_2^{x_2}) \cdot (g_1^{a_1} \cdot g_2^{a_2})) =$

$(A' \cdot g_1^{a_1} \cdot g_2^{a_2})^d \cdot (B \cdot g_1^{a_1} \cdot g_2^{a_2}) = (A'^*)^d \cdot B^* (\mathrm{mod}\, n)$. Thus, the coin $(A'^*, B^*, s_1^*, s_2^*, s_3^*)$ is valid and can be spent with any merchant.

3.3.2 Forging Coins by Cheating the Spender

The malicious merchant also can generate a valid coin by cheating the spender. We describe the detailed process as follows.

Step 1. This is same as Step 1 in Subsection 3.2.1.

Step 2. In the payment phase, when the malicious merchant obtains a valid coin (A', B, s_1, s_2, s_3), he/she computes $A'^* = A' \cdot g_1^{a_1} \cdot g_2^{a_2} (\mathrm{mod} n)$, $B^* = B \cdot g_1^{a_1} \cdot g_2^{a_2} (\mathrm{mod} n)$, $d^* = H(A'^*, B^*, ID_M, date||time)$, and sends d^* to the spender. The spender sends $r_1 = d^* \cdot u \cdot s + x_1 (\mathrm{mod} e_B)$, and $r_2 = d^* \cdot s + x_2 (\mathrm{mod} e_B)$ to the merchant. Then, it is claimed by the merchant that the value d^* is not correct or there is a network fault and stops the transaction. Next, the merchant computes $r_1^* = r_1 + d \cdot a_1 + a_1$, and $r_2^* = r_2 + d \cdot a_2 + a_2$. If the spender is honest, the (r_1^*, r_2^*) is valid, because $g_1^{r_1^*} \cdot g_2^{r_2^*} = g_1^{r_1 + d^* \cdot a_1 + a_1} \cdot g_2^{r_2 + d^* \cdot a_2 + a_2} = (g_1^{r_1} \cdot g_2^{r_2}) \cdot (g_1^{a_1} \cdot g_2^{a_2})^{d^*} \cdot g_1^{a_1} \cdot g_2^{a_2} = (A' \cdot g_1^{a_1} \cdot g_2^{a_2})^{d^*} (B \cdot g_1^{a_1} \cdot g_2^{a_2}) = (A'^*)^{d^*} \cdot B^* (\mathrm{mod} n)$. Then, he/she computes $s_1^* = s_1 \cdot \alpha_1^{a_1} \cdot \alpha_2^{a_2} (\mathrm{mod} n)$, $s_2^* = s_2 \cdot \beta_1^{a_1} \cdot \beta_2^{a_2} (\mathrm{mod} n)$, and $s_3^* = s_3 \cdot \gamma_1^{a_1} \cdot \gamma_2^{a_2} (\mathrm{mod} n)$.

According to Step 2 in Subsection 3.3.1, s_1^*, s_2^*, and s_3^* are valid signatures of A'^*, B^*, and $A'^* + B^*$ respectively. Thus, the coin $(A'^*, B^*, s_1^*, s_2^*, s_3^*)$ with (r_1^*, r_2^*) is valid for the merchant and can be later deposited in the bank. Furthermore, the spender cannot detect the cheating, because that he/she can spend his/her coin (A', B, s_1, s_2, s_3) normally.

3.3.3 Forging Coins with the Help of the Spender

If there is a malicious merchant colluding with a malicious spender, they also can forge a valid coin by following the same process described in Subsection 3.3.2.

4 Conclusions

We review Baseri et al.'s [1] off-line electronic cash scheme and find three flaws. First, the scheme cannot satisfy verifiability. Second, malicious spenders can withdraw coins independently or jointly without being injected his/her identity, therefore, the bank cannot detect the coins owner when double spending occurs. This violates the property of unreuseability. Finally, a malicious spender can forge valid coins using existing coins, and a malicious merchant can forge valid coins by cheating or colluding with a spender. This violates the property of unforgeability. From above, the Baseri et al.'s scheme is not secure. Presently, we are investigating how Baseri et al.'s method can be greatly modified to defend all possible kinds of attacks.

References

[1] Y. Baseri, B. Takhtaei, and J. Mohajeri, "Secure untraceable off-line electronic cash system," *Scientia Iranica*, vol. 20, no. 3, pp. 637–646, June 2013.

[2] D. Chaum, "Blind signatures for untraceable payments," in *Proceedings of Advances in Cryptology (CRYPTO'82)*, pp. 199–203, Santa Barbara, California, USA, 1982.

[3] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proceedings of Advances in Cryptology (CRYPTO'88)*, pp. 319–327, Santa Barbara, California, USA, 1988.

[4] X. F. Chen, F. G. Zhang, and S. L. Liu, "ID-based restrictive partially blind signatures and applications," *Journal of Systems and Software*, vol. 80, no. 2, pp. 164–171, Feb. 2007.

[5] Y. Chen, and J. S. Chou, "On the Privacy of 'User efficient recoverable off-line e-cash scheme with fast anonymity revoking'," *International Journal of Network Security*, vol. 17, no. 6, pp. 708–711, Nov. 2015.

[6] Z. Eslami, and M. Talebi, "A new untraceable off-line electronic cash system," *Electronic Commerce Research and Applications*, vol. 10, no. 1, pp. 59–66, Feb. 2011.

[7] C. I. Fan, S. V. Huang, and Y. C. Yu, "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 227–237, Jul. 2013.

[8] C. I. Fan, B. W. Lin, and S. M. Huang, "Customer efficient electronic cash protocol," *Journal of Organizational Computing and Electronic Commerce*, vol. 17, no. 3, pp. 259–281, Dec. 2007.

[9] X. M. Hu, and S. T. Huang, "Analysis of id-based restrictive partially blind signatures and applications," *Journal of Systems and Software*, vol. 81, no. 11, pp. 1951–1954, Nov. 2008.

[10] W. S. Juang, and H. T. Liaw, "A practical anonymous multi-authority e-cash scheme," *Applied Mathematics and Computation*, vol. 147, no. 3, pp. 699–711, Jan. 2004.

[11] W. Mao, *Modern Cryptography: Theory and Practice*, Ch. 6, pp. 186, Publishing House of Electronics Industry, 2004.

[12] Z. W. Tan, "An off-line electronic cash scheme based on proxy blind signature," *The Computer Journal*, vol. 54, no. 4, pp. 505–512, Apr. 2011.

[13] H. Wang, J. L. Cao, and Y. C. Zhang, "A flexible payment scheme and its role-based access control," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 3, pp. 425–436, Mar. 2005.

Feng Wang was born in Shandong province, China, in 1978. He received his B.S. degree in Mathematics from Yantai Normal University (now named Ludong University), Yantai, in 2000 and the M.S. degree in Applied Mathematics from the Guangzhou University, Guangzhou, in 2006. Currently, he is a Lecturer in the College of Mathematics and Physics at Fujian University

of Technology and a visiting scholar in Department of Information Engineering and Computer Science at Feng Chia University. His research interests include computer cryptography and information security.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

Changlu Lin received the BS degree and MS degree in mathematics from the Fujian Normal University, P.R. China, in 2002 and in 2005, respectively, and received the Ph.D degree in information security from the state key laboratory of information security, Graduate University of Chinese Academy of Sciences, P.R. China, in 2010. He works currently for the College of Mathematics and Computer Science, and the Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University. He is interested in cryptography and network security, and has conducted research in diverse areas, including secret sharing, public key cryptography and their applications.

A Taxonomy of Attacks in RPL-based Internet of Things

Anthéa Mayzaud[1,2], Rémi Badonnel[2], and Isabelle Chrisment[2]
(Corresponding author: Anthéa Mayzaud)
Inria Grand Est - Nancy, France[1]
TELECOM Nancy, Université de Lorraine, LORIA, UMR 7503, France[2]
(Email: anthea.mayzaud@inria.fr)
(Received June 23, 2015; revised and accepted July 30 & Aug. 12, 2015)

Abstract

The growing interest for the Internet of Things is contributing to the large-scale deployment of Low power and Lossy Networks (LLN). These networks support communications amongst objects from the real world, such as home automation devices and embedded sensors, and their interconnection to the Internet. An open standard routing protocol, called RPL, has been specified by the IETF in order to address the specific properties and constraints of these networks. However, this protocol is exposed to a large variety of attacks. Their consequences can be quite significant in terms of network performance and resources. In this paper, we propose to establish a taxonomy of the attacks against this protocol, considering three main categories including attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic. We describe these attacks, analyze and compare their properties, discuss existing counter-measures and their usage from a risk management perspective.
Keywords: Internet of things, LLN, RPL, security

1 Introduction

The Internet of Things defines a new paradigm that is increasingly growing in the context of pervasive networks and services. It consists in the extension of the Internet to objects from the real world which are interacting with each other in order to reach common goals. The high interest for this paradigm has resulted in the large-scale deployment of Low power and Lossy Networks (LLN), such as wireless sensor networks and home automation systems. These networks have strong resource constraints (energy, memory, processing) and their communication links are by nature characterized by a high loss rate and a low throughput. Moreover, the traffic patterns are not simply defined according to a point-to-point schema. In many cases, the devices also communicate according to point-to-multipoint and multipoint-to-point patterns. Existing routing protocols are not suitable to deal with these requirements [19]. Therefore a complete stack of standardized protocols has been developed including the IEEE 802.15.4 standard protocol for the communication layers in wireless personal area networks (WPAN) and the 6LowPAN protocol which defines encapsulation and header compression mechanisms between IPv6 and 802.15.4. At the routing layer, the ROLL[1] working group has proposed a protocol called RPL (Routing Protocol for Low power and Lossy Networks) based on IPv6 [31]. Due to their constrained nature RPL-based networks may be exposed to a large variety of security attacks [27]. Even if cryptographic mechanisms are used in first defense, they only prevent external attacks. When nodes are compromised and become as a result internal attackers, cryptographic techniques become unavailing and can no longer protect the network.

Many studies have been conducted on security issues regarding mobile ad-hoc networks [1, 5] and wireless sensor networks [29]. Current published surveys regarding the RPL protocol have been focused on performance evaluation [8] and a few on some specific security aspects. The security threat analysis [27] provided by the ROLL working group is probably the most complete study on possible RPL security issues. The attacks are classified according to a regular CIAA model (confidentiality, integrity, authentication and availability). Guidelines and recommendations are provided to counteract these attacks. However, this analysis is a general framework on generic threats. It does not detail how the attacks are instantiated using the RPL protocol. In [14], authors performed a study of security in 6LowPAN networks including the routing protocol RPL but only mentioned three attacks regarding the routing protocol. The authors of [23] performed a survey of some existing attacks targeting the RPL protocol and the 6LoWPAN protocol with no classification, they also provided a discussion on different types of IDS such as [24] and [14]. Also, other studies [16, 28, 24, 25] present some attacks targeting the

[1]Routing Over Low power and Lossy networks

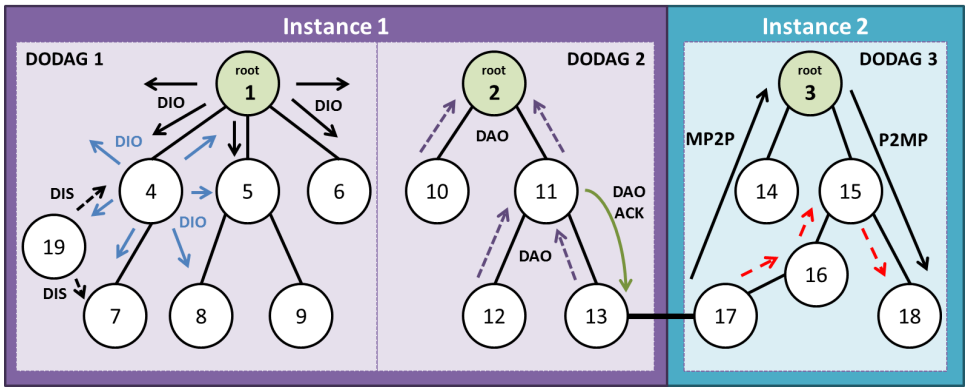


Figure 1: Example of a RPL network composed of two instances and three DODAGs

RPL protocol, but their main contribution consists in an intrusion detection system (IDS) whose goal is to detect these attacks. In [17], the authors presented an evaluation in the emulation environment Cooja using the contiki OS[2] of four attacks targeting the RPL protocol mostly mentioned in [14].

In this paper, our objectives are the identification and classification of the different attacks against the RPL network protocol while providing details on how those attacks can take place. This novel approach classifies the attacks according to the attacker's goal and means considering the specific properties of RPL networks. This classification allows us to prioritize attacks depending on the damages they cause to the network and can be used in a risk management perspective. We also describe in this taxonomy existing security solutions we have found in the literature.

The rest of the paper is consequently organized as follows. Section 2 overviews the RPL protocol and identifies its security issues. We then introduce our taxonomy of attacks related to the RPL protocol. In the following sections, we analyse each category of the proposed taxonomy. Section 3 focuses on security attacks targeting the network resources of RPL devices. Section 4 details security attacks targeting the topology and Section 5 addresses security attacks on network traffic. In Section 6, we show the utilization of the classification as a support for risk management and highlight benefits from a risk management perspective through an illustrative example. Finally, Section 7 concludes the paper and points out future research perspectives.

2 RPL Concepts and Security Concerns

The RPL protocol is a distance-vector routing protocol based on IPv6. The RPL devices are interconnected according to a specific topology which combines mesh and tree topologies called Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG graph is built from a root node which is the data sink of the graph. A network can operate one or more RPL instances which consist of multiple DODAG graphs as shown in Figure 1. Each RPL instance is associated to an objective function which is responsible for calculating the best path depending on a set of metrics or constraints. For instance, this function can minimize energy consumption or simply compute the shortest path. A RPL node can join several instances at the same time, but it can only join one DODAG graph per instance such as nodes 13 and 17 in Figure 1. These multiple instances enable the RPL protocol to perform different optimizations, such as quality-of-service ones. The RPL packets can be forwarded according to three traffic patterns as shown in the third DODAG of Figure 1: (i) multipoint-to-point traffic (MP2P) from leaves to the root via upward routes; (ii) point-to-multipoint traffic (P2MP) from the root to leaves using downward routes; and (iii) point-to-point traffic (P2P) illustrated by red doted arrows using both up and downward routes.

2.1 DODAG Building and Maintenance

The DODAG graph is built in a step by step manner. The root initially broadcasts a DIO message (*DODAG Information Object*) as depicted in Figure 1. This message contains the information required by RPL nodes to discover a RPL instance, get its configuration parameters, select a parent set, and maintain the DODAG graph. Upon receiving a DIO message, a node adds the sender of the message to its parents list and determines its own rank value by taking into account the objective function referred in the DIO message. The rank value of a node corresponds to its position in the graph with respect to the root and must always be greater than its parents' rank in order to guarantee the acyclic nature of the graph. It then forwards updated DIO messages to its neighbors. Based on its parents list, the node selects a preferred parent which becomes the default gateway to be used when data has to be sent toward the DODAG root. At the end of this process, all the nodes participating in the DODAG graph have an upward default route to the DODAG root. This route is composed of all the preferred parents. The

[2]http://www.contiki-os.org

DIO messages are periodically sent according to a timer set with the trickle algorithm [18] which optimizes the transmission frequency of control messages depending on the network state. A new node may join an existing network by broadcasting a DIS message (*DODAG Information Solicitation*) in order to solicit DIO messages from its neighbors. The DAO messages (*Destination Advertisement Object*) are used to build downward routes. Depending on the mode of operation specified by the root in the DIO messages, routing tables can be maintained by router nodes. In the storing mode, the child unicasts a DAO message to the selected parent which records it. The parent aggregates the routes received from other DAO messages and sends the information to its parent recursively through a DAO message. In the non-storing mode, DAO messages are unicasted to the DODAG root. Intermediate nodes do not store routing information but simply insert their own address to the message in order to complete the reverse path. The DAO messages can be acknowledged with DAO-ACK messages (*Destination Advertisement Object Acknowledgement*).

2.2 Loops, Inconsistencies and Repairs

The RPL protocol integrates mechanisms to avoid loops, detect inconsistencies and repair DODAGs. Count-to-infinity phenomena occur when a parent increases its rank value and selects its child as a new parent and the child do the same because it cannot re-attach to another node and so on. Then, the rank value of both parent and child does not stop to increase. To prevent this, the RPL protocol limits the maximum rank value allowed within the graph. DODAG loops appear when a node does not respect the rank property which means that the DODAG is no longer acyclic. To prevent this, a leaving node must poison its sub-DODAG by advertising an infinite rank. The leaving node has also the possibility to use a detaching mechanism, which consists in forming an intermediary DODAG and rejoining the main DODAG later. The RPL protocol can also detect inconsistencies using datapath validation mechanism. Routing information is included in data packets within a RPL Option carried in the IPv6 Hop-by-Hop header. Several flags are defined: (i) the Down 'O' flag indicates the expected direction up or down of a packet. If a router sets this flag, the packet should be forwarded to a child node using downward routes, otherwise it should be sent to a parent with a lower rank toward the DODAG root; (ii) the Rank-Error 'R' flag indicates that a rank error is detected. It occurs when a mismatch is observed between the rank values and the direction of a packet indicated by the Down flag, (iii) the Forwarding-Error 'F' flag indicates the inability of a node to forward the packet toward the destination in case of downward packets [31].

When inconsistencies are detected, the RPL nodes should trigger repair mechanisms. These mechanisms contribute also to the topology maintenance when node and link failures happen. The local repair mechanism consists in finding an alternative path to route the packets when the preferred parent is not available. The node chooses another parent in its parent list. It is also possible to route packets via a sibling node e.g. node with the same rank. This alternative path may not be the most optimized one. According to [12], this local repair mechanism is effective and enables the network to converge again within a reasonable time. When the local repair mechanisms fail due to multiple inconsistencies, the DODAG root can initiate a global repair by incrementing the version number of the DODAG graph. The RPL network is then completely rebuilt.

2.3 Security Concerns

The RPL protocol is exposed to a large variety of security attacks. The characteristics of LLN networks such as resource constraints, lack of infrastructure, limited physical security, dynamic topology and unreliable links make them particularly vulnerable and difficult to protect against attacks. These ones can be specific to the RPL protocol, but can also be applied to wireless sensor networks or even to wired networks. The RPL protocol defines several mechanisms that contribute to its security. As previously mentioned, it integrates local and global repair mechanisms as well as loop avoidance and detection techniques. It also defines two security modes to encrypt data packets. However, typical deployments of such networks base their security on link layer and transport/application layer [3]. In the following of the paper we assume that an attacker is able to bypass security at the link layer by either exploiting a vulnerability or gaining access to a shared key. The attacker can also be a misconfigured or faulty node whose behavior can disturb network functioning.

In this paper, we propose to establish a taxonomy of routing attacks against the RPL protocol. This one takes into account the goals of the attack and what element of the RPL network is impacted. The taxonomy is depicted in Figure 2 and considers three categories of security attacks. The first category covers attacks targeting the exhaustion of network resources (energy, memory and power). These attacks are particularly damaging for such constrained networks because they greatly shorten the lifetime of the devices and thus the lifetime of the RPL network. The second category includes attacks targeting the RPL network topology. They disturb the normal operation of the network: the topology may be sub-optimized in comparison with a normal convergence of the network or a set of RPL nodes may be isolated from the network. The third category corresponds to attacks against the network traffic, such as eavesdropping attacks or misappropriation attacks.

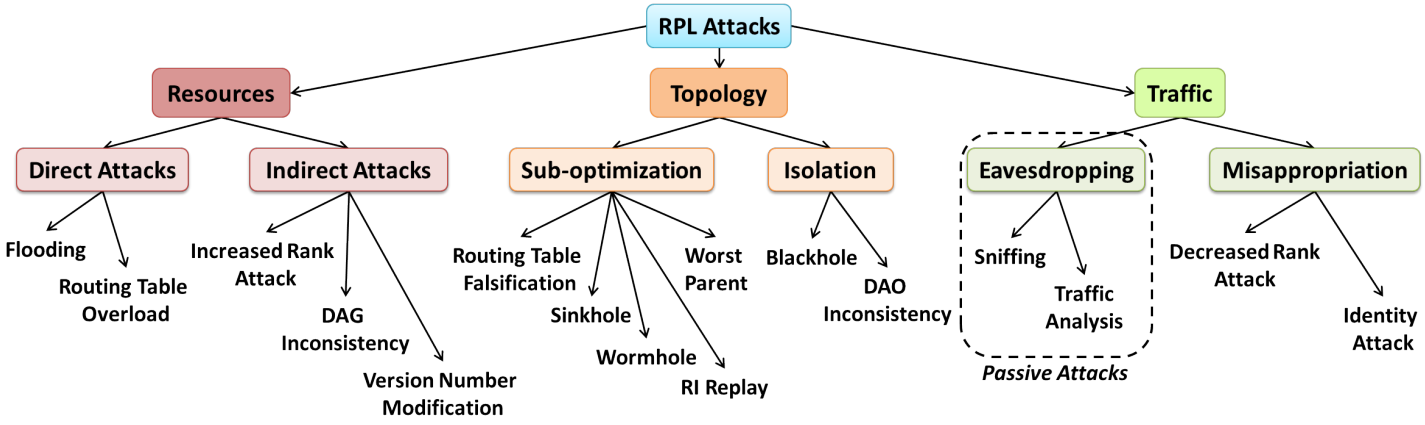


Figure 2: Taxonomy of attacks against RPL networks

3 Attacks Against Resources

Attacks against resources typically consists in making legitimate nodes perform unnecessary processing in order to exhaust their resources. This category of attacks aims at consuming node energy, memory or processing. This may impact on the availability of the network by congesting available links and therefore on the lifetime of the network which can be significantly shortened.

We distinguish two subcategories of attacks against resources. The first one gathers direct attacks where a malicious node will directly generates the overload in order to degrade the network. The second one contains indirect attacks where the attackers will make other nodes generate a large amount of traffic. For instance, such an attack can be performed by building loops in the RPL network so that make other nodes produce traffic overhead.

3.1 Direct Attacks

In case of direct attacks, the attacker is directly responsible for resource exhaustion. This can typically be done by performing flooding attacks or by executing overloading attacks with respect to routing tables, when the storing mode is active.

3.1.1 Flooding Attacks

Flooding attacks consist in generating a large amount of traffic in a network and make nodes and links unavailable. These attacks can be performed by an external or internal attacker. They exhaust the resources of all the network nodes in the worst case. More specifically, using solicitation messages to perform the flooding is called an HELLO flood attack. In RPL networks, an attacker can either broadcast DIS messages to its neighboring nodes which have to reset their trickle timer, or, unicast DIS message to a node which has to reply with a DIO message. In both cases, this attack leads to network congestion and also to the saturation of the RPL nodes. The consequences of such attacks has been studied in [17], the authors show that the control message overhead significantly increased but the delivery ratio is not affected. However no solution especially designed for RPL has been proposed.

3.1.2 Routing Table Overload Attacks in Storing Mode

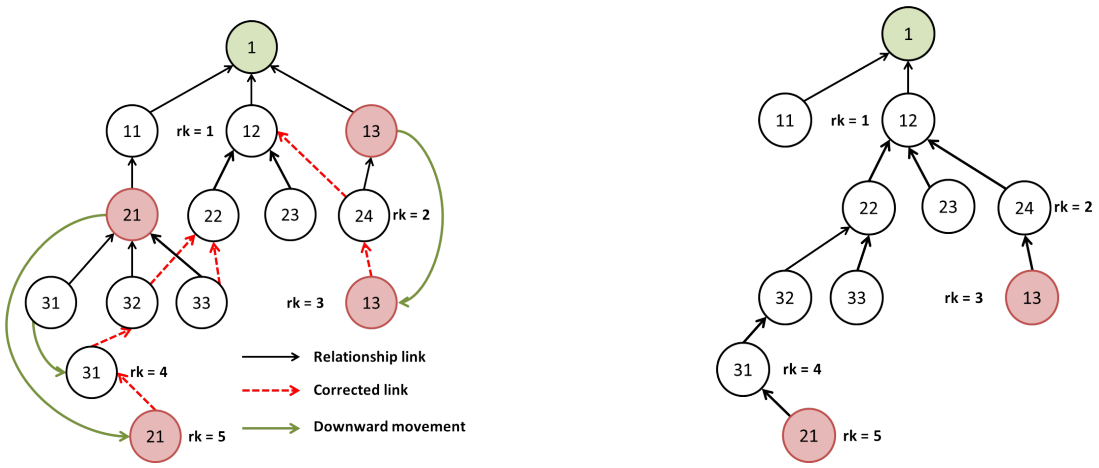
It is also possible to perform direct attacks against resources by overloading the RPL routing tables. The RPL protocol is a proactive protocol. This means that the RPL router nodes build and maintain routing tables when the storing mode is enabled for those nodes. The principle of routing table overload is to announce fake routes using the DAO messages which saturate the routing table of the targeted node. This saturation prevents the build of new legitimate routes and impacts network functioning. It may also result in a memory overflow. Let us consider the example of the DODAG 2 graph described in Figure 1 and assume that node 12 plays the role of the attacker. Nodes 12 and 13 send a DAO message in order to add the corresponding entries in the routing table of node 11. The attacker, node 12 sends multiple forged DAO messages to node 11 with false destinations. As a consequence, node 11 builds all the corresponding entries in its routing table. Afterwards, when the other nodes including node 13 are sending legitimate DAO messages with respect to new routes, the node 11 is no longer able to record them because its routing table is overloaded. This attack is not specifically mentioned in the literature but it is part of overload attacks more generally [25].

3.2 Indirect Attacks

Indirect attacks correspond to attacks where the malicious node makes other nodes generate an overload for the network. It includes: increased rank attacks, DAG inconsistency attacks and version number attacks.

3.2.1 Increased Rank Attacks

The increased rank attack consists in voluntarily increasing the rank value of a RPL node in order to generate



(a) Initial State (b) Final State

Figure 3: Rank increased attack in a RPL network

loops in the network. This attack has been studied in [32] through ns-2 simulations. The authors showed that their loop avoidance mechanisms costed more than the attack itself. Concretely, in a RPL network, a rank value is associated to each node and corresponds to its position in the graph structure according to the root node. As previously mentioned, the node rank is always increasing in the downward direction in order to preserve the acyclic structure of the DODAG. When a node determines its rank value, this one must be greater than the rank values of its parents. If a node wants to change its rank value, it has first to update its parents list by removing the nodes having a higher rank than its new rank value. Once a node has established the set of parents in a DODAG, it selects its preferred parent from this list in order to optimize the routing cost when transmitting a packet to the root node. A malicious node advertises a higher rank value than the one it is supposed to have. Loops are formed when its new preferred parent was in its prior sub-DODAG and only if the attacker does not use loop avoidance mechanisms. In that case, two attack scenarios are possible as illustrated in Figure 3. In the first scenario, the attacker is node 13 and the new preferred parent (node 24) has already a substitute parent (node 12) to re-attach to. The node 13 increases its rank value to 3 and chooses node 24 as the new preferred parent. This operation generates a routing loop in the DODAG graph, because the node 24 was in the prior sub-DODAG of node 13. The formed loop is composed of nodes 13 and 24 and is easily repaired because the node 24 can re-attach to node 12 after sending few control messages. However, this attack becomes more problematic when the node does not have a substitute parent such as node 31 in the second scenario. As depicted in Figure 3, the attacker increases its rank value which requires node 31 to also increase its own in order to find a new parent. Meanwhile nodes 32 and 33 have to connect to a substitute parent (node 22) so node 31 selects node 32 as new preferred parent. At the end, node 21 increases its rank value to 5 in order to add node 31 as its preferred parent. The count-to-infinity problem is avoided because of the limitation of the maximum rank value advertised for a DODAG, as seen in Section 2.2. The increased rank attack is more damaging in this second scenario, because more routing loops are built at the neighborhood. In that case, the loop repair mechanism requires to send many DIO messages (resets of the trickle timer) and requires a longer convergence time. The more the number of affected nodes increases, the longer the convergence time is. We consider this attack as part of the resource consumption attacks because the churn is exhausting node batteries and is congesting the RPL network.

To mitigate this attack, the number of times a RPL node is increasing its rank value in the DODAG graph should be monitored to determine if a node can be considered as malicious or misconfigured. It is important to notice that a node can legitimately increase its rank value if it no longer matches the objective function and/or cannot manage the amount of received traffic. However, it must use the loop prevention techniques or it can wait for a new version of the DODAG graph. Also, thanks to the data path validation mechanism, the RPL protocol is able to deal with these loops even if resources are consumed to repair them [31].

3.2.2 DAG Inconsistency Attacks

A RPL node detects a DAG inconsistency when it receives a packet with a Down 'O' bit set from a node with a higher rank and vice-versa [31] e.g. when the direction of the packet does not match the rank relationship. This can be the result of a loop in the graph. The Rank-Error 'R' bit flag is used to control this problem. When an inconsistency is detected by a node, two scenarios are possible: (i) if the Rank-Error flag is not set, the node sets it and the packet is forwarded. Only one inconsistency along the path is not considered as a critical situation for the RPL network, (ii) if the 'R' bit is already set, the node discards

Table 1: Summary of attacks on resources

Attacks	I/E	A/P	Prerequisites	Impact	CIA	Mitigation/ Protection	Overhead
Flooding	I/E	A	-	Link/Battery	A	None	None
Routing Table Overload	I	A	Storing Mode	Memory/Battery	A/I	None	None
Increased Rank Attack	I	A	-	Battery/Link	A	RPL loop detection and avoidance mechanisms [31]	None (by default in RPL)
DAG Inconsistency Attack	I	A	Option Header	Battery/Link	A/I	Limitation of timer resets [10, 26, 22]	Low (for both solutions)
Version Number Attack	I	A	-	Battery/Link	A/I	VersionNumber and Rank Authentication [7], TRAIL [13]	Low (for both solutions)

the packet and the timer is reset [18]. As a consequence, control messages are sent more frequently. A malicious node has just to modify the flags or add new flags to the header. The immediate outcome of this attack is to force the reset of the DIO trickle timer of the targeted node. In that case, this node starts to transmit DIO messages more frequently producing local instability in the RPL network. This also consumes the battery of the nodes and impacts the availability of links. All the neighbourhood of the attacker is concerned by the attack, since it has to process unnecessary traffic. Moreover, by modifying legitimate traffic, all the packets are discarded by the targeted node. This causes a blackhole and isolates segments of the network. To mitigate the flooding induced by this attack, [10] proposes to limit the rate of trickle timer resets due to an RPL Option to no greater than 20 resets per hour. In our previous works [26] and [22], we proposed instead of a fixed threshold two solutions that takes into account network characteristics. The first solution presented in [26] is an adaptive threshold with fixed parameters that we improved in a dynamic approach [22] where node's specific parameters are used instead. We showed that these approaches are more effective than the fixed threshold while preserving energy consumption of the nodes. Also another variant of a similar attack is described by the authors of [16] and [14]. Their attack termed as rank attack consists in not checking the rank relationship for a malicious node. The attacker does not set the 'R' flag if an inconsistency is detected. The difference with the DAG inconsistency is that the attacker does not manipulate flags to build "fake loops" but chooses to not solve "real loops" if they occur but the consequences are still similar.

3.2.3 Version Number Attacks

The version number is an important field of each DIO message. It is propagated unchanged down the DODAG graph and is incremented by the root only, each time a rebuilding of the DODAG is necessary which is also called global repair. An older value indicates that the node has not migrated to the new DODAG graph and cannot be used as a parent node. An attacker can change the version number by illegitimately increasing this field of DIO messages when it forwards them to its neighbors. Such an attack causes an unnecessary rebuilding of the whole DODAG graph. We showed in [21] that this attack can create many loops and as a consequences loss of data packets. Also the successive unnecessary rebuildings of the graph increase significantly controle message overhead exhausting nodes resources and congesting the network. Dvir et al. [7] proposed a security mechanism called VeRa (standing for Version Number and Rank Authentication) that prevents compromised nodes from impersonating the root and from sending an illegitimate increased VersionNumber. The solution uses authentication mechanisms based on hash operations. In that case, a node can easily check if the VersionNumber has been modified by the root node or by another malicious node, which can no longer usurp the identity of the DODAG root. Also, authors of [13] proposed an improvement of the previous solution solving some issues they discovered in VeRA.

3.3 Analysis

We discuss in this section the properties of the identified attacks as well as methods and techniques to address them. Table 1 summarizes attacks against resources. A first property to be analysed is the internal (I) or external (E) nature of the attacks. Internal attacks are initiated by a malicious or compromised node of the RPL network. External attacks are performed by nodes that do not belong to the RPL network or are not allowed to access it. We can observe that only the flooding can be performed externally because the attacker does not need to join the graph to perform the DIS flooding since DIS message are used to discover the DODAG. For the rest of the attacks, the malicious node needs to be part of the DODAG to have enough knowledge in order to launch its attacks.

A second property is to determine if the attack is passive (P) or active (A). Passive attacks do not modify the behavior of the network. On the contrary, active attacks

require the node to perform operations that are observable by other nodes in the network. They are usually more critical than passive attacks which mainly target data confidentiality or topology information. Attacks targeting the resources are all active since the attacker has to send packets.

A third property is the prerequisites property. The prerequisites are the required conditions to initiate the attack besides the internal/external nature of the attack, such as particular configuration of the network. The storing mode which means maintaining routing table has to be enabled to launch routing table overload and the RPL option header has to be implemented to run DAG inconsistency attacks.

The next property corresponds to the impact of the attacks. The objective is to quantify the consequences of a successful attack on the network.

The impact in this category is evaluated as the type of over-consumed resources (e.g. memory, battery, link availability). We observe that all the attacks consume node battery as they imply additional processing for the nodes. Most of the time, the link availability is also impacted since the attack requires sending a large number of control messages. The memory is also over-consumed in case of routing table overload attacks.

The fifth property corresponds to the CIA acronym standing for confidentiality, integrity and availability, and refers to a security reference model. In the context of the RPL protocol, confidentiality means the protection of routing information and exchanges. Integrity involves the protection of routing information from unauthorized modification, and availability requires that forwarding services and routing information exchanges are accessible for the nodes. Regarding the identified attacks targeting resources, they systematically impact network availability. Indeed, these attacks involve that the attacker jeopardizes resources of the network (battery, memory, processing, link availability). The integrity is also impacted when the result of the attack supposes that a legitimate resource or legitimate traffic is corrupted e.g. routing table of legitimate nodes is altered during routing table overload attacks. Version number modifications and DAG inconsistency attacks induce that the integrity of packets is jeopardized.

The two last columns of tables indicate respectively the possible security mechanisms to address the attacks, and their overhead (according to their authors). We saw that RPL provides internal mechanisms which contribute to counter attacks. For instance, the loop avoidance mechanisms prevent increased rank attacks. The protocol also proposes an optional mitigation mechanism that limits inconsistency attacks impact [10]. Specific approaches have been designed for the RPL protocol. The VeRa [7] and the TRAIL [13] approaches address version number modifications. In many cases, it is difficult to evaluate the overhead induced by the security mechanisms because they are still at a conceptual level. Moreover, we cannot really consider that the mechanisms which are inherent to the RPL protocol operation introduce an overhead. Also in [24] and [16], authors proposed an IDS to detect different security threats.

4 Attacks on Topology

Attacks against the RPL protocol can also target network topology. We distinguish two main categories amongst these attacks: sub-optimization and isolation.

4.1 Sub-optimization Attacks

In case of sub-optimization attacks, the network will not converge to the optimal form (i.e optimal paths) inducing poor performance.

4.1.1 Routing Table Falsification Attacks in Storing Mode

In a routing protocol, it is possible to forge or modify routing information to advertise falsified routes to other nodes. This attack can be performed in the RPL network by modifying or forging DAO control messages in order to build fake downward routes. This can only be done when the storing mode is enabled. For instance, a malicious node advertises routes toward nodes that are not in its sub-DODAG. Targeted nodes have then wrong routes in their routing table causing network sub-optimization. As a result, the path can be longer inducing delay, packet drops or network congestion. This has not been studied yet in the context of the RPL protocol.

4.1.2 Sinkhole Attacks

An alternative attack consists in building a sinkhole. Such an attack takes place in two steps. First, the malicious node manages to attract a lot of traffic by advertising falsified information data (for instance, up and downward links of superior quality). Then, after having received the traffic in an illegitimate manner, it modifies or drops it. In RPL networks, the attack can be easily performed through the manipulation of the rank value as shown in Section 5.2.1. Because of this falsified advertisement, the malicious node is more frequently chosen as preferred parent by the other nodes, while it does not provide better performance. Thus, the routes are not optimized for the network. The attack modifies the topology and degrades network performance. Moreover, if the attacker decides to drop all the traffic, it also performs a blackhole attack as described in 4.2.1.

This attack was studied in [28] and [24], the authors proposed an IDS to counter it. A functionality of this IDS is to build a global view of the network and as a consequence the possiblity to detect incoherences in the network such as sinkholes. In [30], the authors investigated defence techniques against sinkholes. The first technique is called Rank verification and restricts the possibility for

the attacker to decrease its rank value. It allows legitimate nodes to check if another node along the path has a fake rank. The second technique is called parent fail-over and operates as an end-to-end acknowledgement. When a root node does not receive enough traffic from a node (according to a certain threshold value), it adds this node's address in a DIO message field. When the node receives the DIO message with its own identity, it blacklists its parent and selects another one. The authors show that a combination of these two techniques provides efficient results in a RPL network.

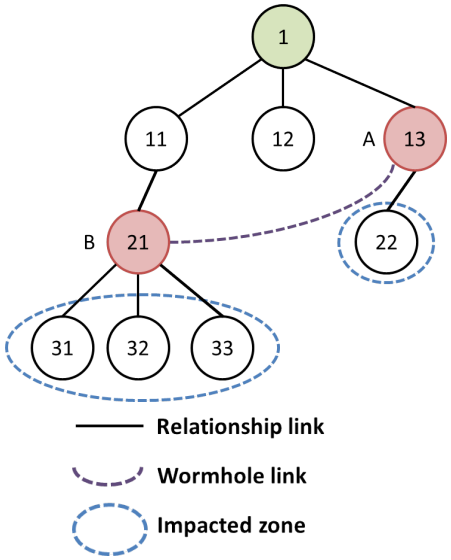


Figure 4: A wormhole attack in a RPL network

4.1.3 Wormhole Attacks

Wormhole attacks are defined as the use of a pair of RPL attacker nodes, nodes A and B, linked via a private network connection. An example is depicted in Figure 4. In this scenario, every packet received by node 13 is forwarded through the wormhole to node 21 in order to be replayed later. Since the roles are interchangeable, node 21 may perform the same operations than node 13. In the case of wireless networks, it is easier to perform this attack because the attacker can send through the wormhole the traffic addressed to himself as well as all the traffic intercepted in the wireless transmissions. The wormhole attack distorts the routing path and is particularly problematic for RPL networks. If an attacker tunnels routing information to another part of the network, nodes which are actually distant, see each other as if they are in the same neighbourhood. As a result, they can create non-optimized routes according to the objective function.

This attack was studied in [28] which showed that the RPL protocol cannot solve this attack by itself. The authors explained that countering this type of attack is a research challenge if one node of the wormhole is in the Internet. If both attackers are in the RPL networks, the authors suggested to use geographical data and different cryptographic keys at the mac layer for different segments to solve this threat issue. Also the authors of [11] proposed to prevent this attack by using Merkel trees to authenticate nodes and paths.

4.1.4 Routing Information Replay Attacks

A RPL node can also perform routing information replay attacks. It records valid control messages from other nodes and forwards them later in the network. In case of dynamic networks, this attack is quite damaging because the topology and the routing paths are often changed. Replay attacks cause nodes to update their routing tables with outdated data resulting in a false topology. The RPL protocol uses some sequence counters to ensure the freshness of the routing information such as the Version Number for DIO messages or the Path Sequence present in the Transit Information option of DAO messages [31]. This attack is mentioned in [25] however the authors neither study the consequences of such attack nor explained how it can takes place in RPL networks.

4.1.5 Worst Parent Attacks

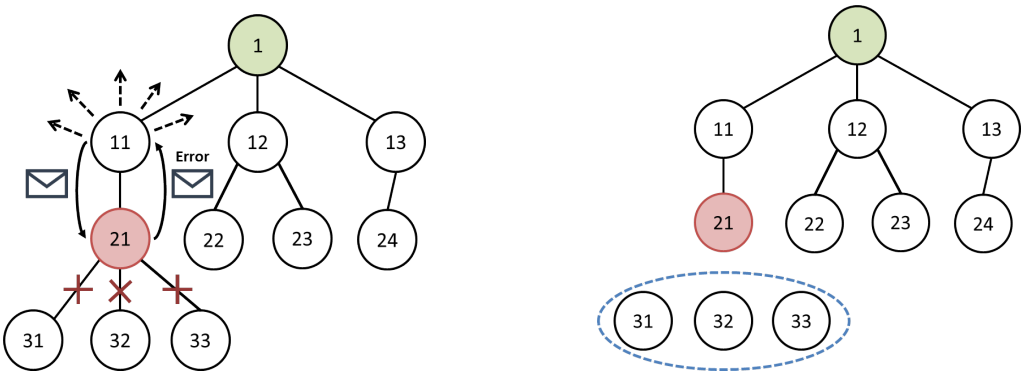
This attack described in [15] and termed as "Rank attack" consists in choosing systematically the worst preferred parent according to the objective function. The outcome is that the resulting path is not optimized inducing poor performance. This attack cannot be easily tackled because children node rely on their parent to route packets and this attack cannot be monitored by neighbors. However, using a security solution which rebuilds a global view of the graph based on nodes information should detect this attack such as the proposed solution in [24].

4.2 Isolation Attacks

The attacks against the topology also serve as a support for isolating a node or a subset of nodes in the RPL network which means that those nodes are no longer able to communicate with their parents or with the root.

4.2.1 Blackhole Attacks

In a blackhole attack, a malicious intruder drops all the packets that it is supposed to forward. This attack can be very damaging when combined with a sinkhole attack causing the loss of a large part of the traffic. It can be seen as a type of denial-of-service attack. If the attacker is located at a strategic position in the graph it can isolate several nodes from the network. There is also a variant of this attack called gray hole (or also selective forwarding attack) where the attacker only discards a specific subpart of the network traffic. Chugh et al.[4] investigated the consequences of blackhole attacks in RPL networks through a set of Cooja simulations. They highlighted different indicators to detect these attacks such as rate and frequency of DIO messages, packet delivery ratio, loss



(a) Initial State (b) Final State

Figure 5: Illustration of a DAO inconsistency attack

percentage and delay. The IDS SVELTE proposed in [24] was designed to detect selective forwarding attacks in such networks.

4.2.2 DAO Inconsistency Attacks in Storing Mode

DAO inconsistencies occur when a node has a downward route that was previously learnt from a DAO message, but this route is no longer valid in the routing table of the child node [31]. RPL provides a mechanism to repair this inconsistency, called DAO inconsistency loop recovery. This optional mechanism allows the RPL router nodes to remove the outdated downward routes using the Forwarding-Error 'F' flag in data packets which indicates that a packet can not be delivered by a child node. The packet with the 'F' flag is sent back to the parent in order to use another neighbour node, as depicted in Figure 5. Once a packet is transmitted downward, it should normally never go up again. When it happens the router sends the packet to the parent that passed it with the Forwarding-Error 'F' bit set and the Down 'O' bit left. When the parent receives the packet with 'F' set it removes the corresponding routing state, clear the 'F' bit, and try to send the packet to another neighbor. If the alternate neighbor still has an inconsistent state the process reiterates. In this scenario, the malicious node is represented by node 21. It uses the 'F' flag to make RPL routers remove legitimate downward routes and thus isolate nodes from the DODAG graph. Each time node 21 receives a packet from node 11, it only changes the RPL 'F' flag and sends it back to node 11. As a consequence, the other nodes of the network (nodes 31 to 33) are isolated from the graph. The objective of this attack is to make router nodes discard available downward routes. This makes the topology of the DODAG graph sub-optimal. One possible consequence of this attack is to isolate the sub-DODAG bound to the attacker which can no longer receive packets, as in our example. This also leads to additional congestion (if the packets are forwarded through sub-optimal paths), partitions and instabilities in the network. The consequences for the children nodes include starvation and delay [2]. To reduce the effects of this attack on the network, RFC 6553 proposes to limit the rate of the downward routing entries discarded due to an 'F' flag to 20 per hour [10].

4.3 Analysis

Table 2 synthesizes attacks targeting the topology. We notice that the attacker has to be both internal and active for these attacks. Indeed, the malicious node has to join the graph to manipulate the topology.

The attacks related to routing tables such as routing table falsifications and DAO inconsistency attacks need the storing mode to be enabled to be performed. Also the RPL option header has to be implemented for the second attack since the malicious node misuses the data path validation which relies on this header. At least two malicious intruders are required to perform the wormhole attack.

In this table, the impact characterizes how the network is affected (modified or isolated) and what type of traffic is concerned (e.g. downward (D) or upward traffic (U)). We consider two main areas that may be impacted: (1) the neighbourhood of a RPL node corresponding to nodes in the direct vicinity such as parents, children, and siblings nodes, and (2) the subnet of a node. We can observe in that table that the routing table falsification attack and the DAO inconsistency attacks are characterized by a similar impact. Indeed, these two attacks corrupt the routing tables of the target. Only downward traffic is concerned because routing tables are only used for downward routing. Therefore, the subnet of the target is modified but the upward traffic is not disturbed. All the other attacks can have consequences on both upward and downward traffic since they concern all types of packets. In that case, both the subnet and/or the neighbourhood can be damaged. These attacks do not target a specific node but try to impact on the overall network traffic in general, even if some filtering is also be performed.

Regarding the next property, the availability is im-

Table 2: Summary of attacks on topology

Attacks	I/E	A/P	Prerequisites	Impact	CIA	Mitigation/ Protection	Overhead
Routing Table Fals.	I	A	Storing Mode	Target's Subnet, D	A/I	None	None
Sinkhole	I	A	-	Attacker's Subnet and Neighbourhood, D/U	A/I	SVELTE [24], Rank verification [7] and Parent fail-over [30]	Low, No evaluation
Wormhole	I	A	2 intruders min.	Attackers Subnet, D/U	A/I	Geographical data [28], Merkel trees [11]	No evaluation (for both)
Routing Information Replay	I	A	-	Attacker's Neighbourhood, D/U	A/I	Sequence Number [31]	None (by default in RPL)
Worst Parent	I	A	-	Attacker's Subnet, D/U	A/I	None	None
Blackhole	I	A	-	Attacker's Subnet, D/U	A/I	Monitoring of counters [4], Parent fail-over [30], SVELTE[24]	Depends on the solution, No evaluation
DAO Inconsistency	I	A	Storing Mode, Option Header	Target's Subnet, D	A/I	Limitation of discarding routing state [10]	Low

pacted in all attacks because the malicious node modifies the topology and then isolates nodes or degrades network performance through sub-optimization. The integrity is also impacted by attacks targeting topology. For instance, routing table falsification attacks and DAO inconsistency attacks alter routing table. Decreased rank attacks induce that the integrity of packets is jeopardized. Moreover, the routing information held by legitimate nodes such as parent identity, freshness or routing path are corrupted during routing information replay, sinkhole, wormhole, blackhole and worst parent attacks.

Replay attacks can be countered by sequence numbers implemented by default in the RPL protocol; also the optional mechanism proposed in RFC 6553 mitigates the effects of DAO inconsistency. The cost of this mitigation is low because it consists in implementing a fixed threshold. Different authors proposed several counter-measures to topology attacks such as the Rank verification [7], the Parent fail-over [30] or Merkel trees [11], however the costs of these solutions have not been evaluated yet. Chugh et al. [4] have defined methods for efficiently detecting blackholes in these networks. The SVELTE IDS [24] is also designed to detect the sinkhole and blackhole attacks. We notice that there is no solution for routing table falsification since this attack has not been studied in the context of the RPL protocol. The worst parent attack also does not have any counter-measures although this threat has been studied [15].

5 Attacks on Traffic

This third category concerns the attacks targeting the RPL network traffic. It mainly includes eavesdropping attacks on the one hand, and misappropriation attacks on the other hand.

5.1 Eavesdropping Attacks

The pervasive nature of RPL networks may facilitate the deployment of malicious nodes performing eavesdropping activities such as sniffing and analysing the traffic of the network.

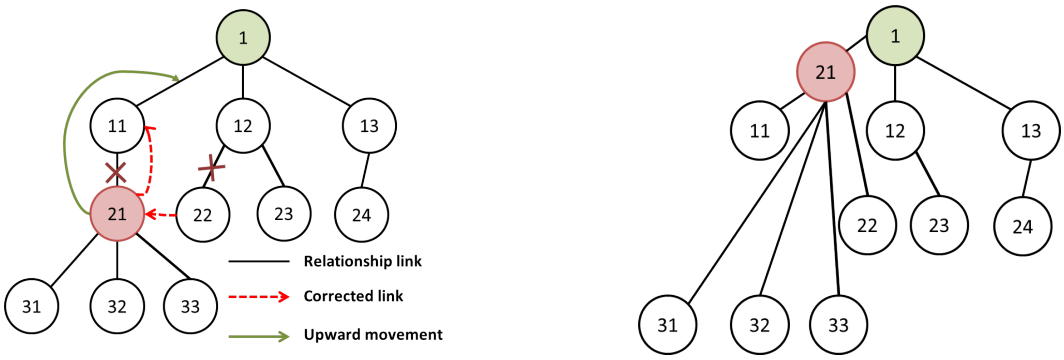
5.1.1 Sniffing Attacks

A sniffing attack consists in listening the packets transmitted over the network. This attack is very common in wired and wireless networks and compromises the confidentiality of communications. An attacker can perform this attack using a compromised device or directly capture the packets from the shared medium in case of wireless networks.

The information obtained from the sniffed packets may include partial topology, routing information and data content. In RPL networks, if an attacker sniffs control messages, it can access information regarding the DODAG configuration such as DODAG ID, Version Number, ranks of the nodes located in the neighborhood. By sniffing data packets, the attacks can not only discover packet content but also have a local view of the topology in the eavesdropped area by looking at source/destination addresses. This attack is difficult to be detected due to its passive nature. The only way to prevent sniffing is encryption of messages when the attacker is external. Even if RFC 6550 mentions encryption of control messages as an option, the technical details are left out from the specification making implementation difficult.

5.1.2 Traffic Analysis Attacks

Traffic analysis aims at getting routing information by using the characteristics and patterns of the traffic on a link. This attack can be performed even if the packets



(a) Initial State (b) Final State

Figure 6: Illustration of a decreased rank attack

are encrypted. The objective is, like sniffing attacks, to gather information about the RPL network such as a partial view of the topology by identifying parent/children relationships. Thanks to this attack, a malicious node can possibly perform other attacks with the gathered information. The consequences depend on the rank of the attacker. If this one is close to the root node, it can process a large amount of traffic and therefore can get more information than when the node is located on the edge of a sub-DODAG.

5.2 Misappropriation Attacks

In misappropriation attacks, the identity of a legitimate node is usurped or performance are overclaimed. These attacks are not so damaging for the RPL network per se. However, they are often used as a first step for other attacks such as those seen in the previous two main categories. They allow the attacker to gain a better understanding of the network and its topology, to gain better access or to intercept a large part of the traffic.

5.2.1 Decreased Rank Attacks

In a DODAG graph, the lower the rank is, the closer the node is to the root and the more traffic this node has to manage. When a malicious node illegitimately advertises a lower rank value, it overclaims its performance. As a result, many legitimate nodes connect to the DODAG graph via the attacker. This results in the attraction of a large part of the traffic, as shown in Figure 6. Thanks to this operation, the malicious node is capable of performing other attacks such as sinkhole and eavesdropping attacks. In the RPL protocol, an attacker can change its rank value through the falsification of DIO messages. The VeRa [7] solution as well as the Rank verification method [30] described in Sections 4.1.2 and 3.2.3 are able to address this issue. However authors in [13] have shown that VeRa is not sure regarding rank authentication and they proposed improvements to address this issue called TRAIL. They also showed another way to perform this attack by replaying the rank of the attacker's parent which allows it to decrease its rank by one. Since SVELTE [24] can detect sinkhole attacks it can also detect the decreased rank attack.

5.2.2 Identity Attacks

Identity attacks gather both spoofing and sybil attacks. A spoofing attack also called Clone ID attack occurs when a malicious node pretends to be a legitimate existing node. In RPL networks, the root node plays a key role in a DODAG graph. It builds and maintains the topology by sending routing information. An attacker may sniff the network traffic to identify the root node. Once this identification is performed, it can spoof the address of the DODAG root and take the control over the network. During sybil attacks [6], one malicious node uses several logical entities on the same physical node. Identity attacks are used as a premise to perform other operations. They were studied in [28], the authors showed that the RPL protocol cannot solve this issue by itself and proposed to consider geographical data to detect such attacks.

5.3 Analysis

As we can observe in Table 3, eavesdropping attacks can be performed externally. They are usually exploited to gain access to the internal network. As for the other categories, the attacker has to be an insider to perform misappropriation attacks. Only the eavesdropping attacks have been classified as passive attacks. All the other identified attacks induce that the attacker generates or modifies packets. Passive attacks are quite difficult to detect, in particular in RPL networks which are often supported by wireless links. There is no particular prerequisite for attacks on traffic.

Regarding attacks on traffic, Table 3 describes the cases where the consequences can be considered as critical for the RPL network. The effect of eavesdropping attacks depends on the nature of the listened data. For instance, data content may be of high importance for patients in the area of healthcare sensor networks, while the criticality is lower when the objective of the RPL network is

Table 3: Summary of attacks on traffic

Attacks	I/E	A/P	Pre.	Impact	CIA	Detection/ Protection	Overhead
Sniffing	I/E	P	-	Critical data	C	Encryption [31]	Depends on the algorithms
Traffic Analysis	I/E	P	-	Critical data	C	None	None
Decreased Rank	I	A	-	Node's rank	I	VeRA [7], TRAIL [13], Rank verification [30], SVELTE [24]	Low, Low, Not evaluated, Low
Identity attack	I	A	-	Node's rank	I	None	None

simply to collect weather temperatures. In case of misappropriation attacks, the consequences are determined by the location of the malicious or spoofed node. Indeed, when the malicious node has a lower rank, it is closer to the root. It is therefore capable of intercepting a larger amount of data and the opportunities to attack the RPL network are bigger.

The next property to be discussed is the classification according to the CIA model. The confidentiality aspect concerns eavesdropping attacks, where the goal of the attacker is to obtain information about the network configuration. Due to the nature of misappropriation attacks, the integrity property is affected in these cases.

The only way to prevent sniffing is to use encryption however in our security model we assumed that the attacker is able to break the cryptography due to the physical constraints of RPL networks. As mentioned previously, even if cryptographic mechanisms are suggested in the standard, it is difficult to implement them because important feature like key-management are left out by the RFC. Moreover, cryptographic algorithms are known to occupy the most memory and take many CPU cycles, thereby greatly affecting the performance of constrained devices. Current RPL implementations, as such, do not enable secure operation modes. There is no current existing solution to prevent traffic analysis and identity attacks in RPL networks. However, the decreased rank attack has been widely studied because it is also used in sinkhole attacks 4.1.2 and several counter-measures has been proposed.

6 Exploitation for Risk Management

This taxonomy provides an overview of the main attacks that the RPL protocol therefore the Internet of Things is currently facing and details their properties. It shows that most of the studies within the area are proof of concepts and that mature security mechanisms are far from being fully deployed. The classification is conceived in a way it is easily expendable with possible future attacks in RPL networks. Our objective is to give a view of the different possibilities. We design this taxonomy so it can be exploited for risk management which consists in identifying, evaluating and treating the risks that a network or an information system faces. The attacks, their consequences and their security mechanisms are considered separately but it is likely that a real attacker combines several of these attacks. Existing approaches from similar networks such as MANETs (Mobile Ad-hoc NETwork) and WSNs (Wireless Sensor Networks) could be investigated. However, they are often too expensive or too difficult to deploy in such highly constrained networks.

6.1 Risk Management

In this context, risk management offers new perspectives to dynamically activate or deactivate security mechanisms in RPL-based networks, in order to prevent attacks while maintaining network performances [20]. We propose in this section to investigate risk management methods and techniques to address the trade-off between security and cost in the Internet of Things. The risk level is defined by Equation (1) [9].

$$\mathcal{R}(a) \quad = \quad P(a) \times E(a) \times C(a). \tag{1}$$

Let consider a security attack noted a. The risk level $R(a)$ depends on the potentiality $P(a)$ of the attack, the exposure $E(a)$ of the RPL network, and the consequences $C(a)$ on the network if the attack succeeds. Risk management is a process consisting in monitoring, prioritizing and controlling risks. For instance, when this process observes a high potentiality $P(a)$, it may activate security mechanisms (being aware of their costs) to reduce the exposure $E(a)$ and maintain the risk level $R(a)$ to a low value.

As depicted in Figure 7, risk management process is composed of two main activities: risk assessment and risk treatment. Risk assessment consists in quantifying the potentiality of attacks. For that, it is necessary to evaluate the performance of detection techniques (based on anomalies or known signatures) in these RPL environments, and to identify the network nodes able to perform this activity. Risk assessment aims also at quantifying the consequences of successful attacks. The objective is to assess the relative importance of nodes in the RPL network, and to analyze how the attack against a given node may impact on the functioning of the overall network.

The risk treatment activity consists then in selecting and applying the security mechanisms that are needed having the cost of the solution in mind.

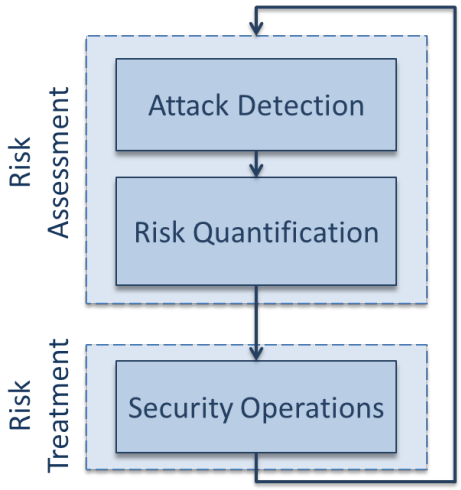


Figure 7: Risk management process

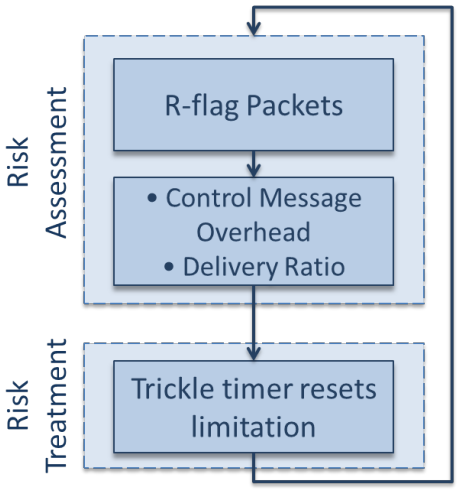


Figure 8: Risk management process applied to the DAG inconsistency attack

6.2 Instantiation

In this section, we propose to show how risk management can be applied to a particular attack. We choose the DAG Inconsistency attack from Section 3.2.2 that we studied in [26]. Risk assessment is composed of quantification of potentiality and consequences of an attack. To quantify the potentiality of an attack we need to define a metric allowing us to detect it. In the DAG inconsistency attack case, an efficient metric is the number of 'R'-flag packets. An attack is detected if this value reach a threshold defined in [26]. To quantify the consequences of this attack, we can use interesting metrics such as control message overhead and delivery ratio.

Regarding the risk treatment, in order to reduce the impact of such attack in the network, several countermeasures can be considered and applied. We already mentioned the solution proposed in the RFC 6553 [10] which is to limit at 20 per hour the number of trickle timer resets due to DAG inconsistency detection. The other countermeasures that we proposed are also to limit the number of trickle timer resets but using an adaptive or a dynamic threshold instead of fixed one. Our approaches are able to adapt according to the aggressiveness of the attacker. The adaptive threshold relies on set values and the dynamic is based on node's specific parameters. Figure 8 summarizes the risk management process applied to the DAG inconsistency attack.

This process can be applied to each attack we described in this taxonomy. For that purpose, each attack has to be accurately studied (with detection metrics and techniques highlighted) and security countermeasures developed or identified. The classification can help prioritizing the risks according to which main network resources are harmed.

7 Conclusions

The Internet of Things relies on the deployment of Low power and Lossy networks in order to support communications amongst objects and their interconnection to the Internet. These networks are characterized by scarce resources in terms of energy, processing and memory. Their development has led to the specification by the IETF ROLL working group of a dedicated routing protocol called RPL. Considering the nature of these networks composed of devices from the real life, it is a mandatory to identify and analyse the security attacks to which this protocol is exposed.

We have therefore proposed in this paper a taxonomy in order to classify the attacks against the RPL protocol in three main categories. The attacks against resources reduce network lifetime through the generation of fake control messages or the building of loops. The attacks against the topology make the network converge to a sub-optimal configuration or isolate nodes. Finally, attacks against network traffic let a malicious node capture and analyse large part of the traffic. Based on this taxonomy, we have compared the properties of these attacks and discuss methods and techniques to avoid or prevent them. While the RPL specification mentions two possible security modes, it does not define how they might be implemented nor how the management of keys could be performed. Most of the security solutions in the area are still at a proof-of-concept level. Moreover, while several solutions from wired and wireless networks are available, they might significantly degrade network performance, which are limited in the Internet of Things. Risk management mechanisms provide new perspectives with respect to this issue. They could typically serve as a support for dynamically selecting the security modes and the protection techniques to be considered for a given context. The context including the potentiality of attacks and the network

properties (size, nature of devices). This adaptive configuration of RPL networks is a major challenge for addressing the trade-off between the level of security required by applications and the overhead induced by countermeasures.

Acknowledgment

This work was funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

References

[1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communication Surveys & Tutorials*, vol. 10, no. 4, pp. 78–93, Oct. 2008.

[2] A. Barbir, S. Murphy, and Y. Yang, *Generic Threats to Routing Protocols*, RFC 4593 (Informational), Internet Engineering Task Force, Oct. 2006.

[3] A. Brandt, E. Bacceli, R. Cragie, and P. van der Stok, *Applicability Statement: The Use of the RPL Protocol Set in Home Automation and Building Control*, May 2014. (`https://tools.ietf.org/html/draft-brandt-roll-RPL-applicability-home-building-04`)

[4] K. Chugh, L. Aboubaker, and J. Loo, "Case study of a black hole attack on 6lowpan-RPL," in *Proceedings of the SECURWARE Conference*, pp. 157–162, Aug. 2012.

[5] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communication Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[6] J. R. Douceur, "The sybil attack," in *First International Workshop on Peer-to-Peer Systems (IPTPS'01)*, pp. 251–260, London, UK, 2002.

[7] A. Dvir, T. Holczer, and L. Buttyán, "Vera - version number and rank authentication in RPL," in *Proceedings of Mobile Adhoc and Sensor Systems Conference (MASS'11)*, pp. 709–714, 2011.

[8] O. Gaddour and A. Koubâa, "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, Sept. 2012.

[9] B. Guttman and E. A. Roback, *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12, NIST, 1995.

[10] J. Hui and J. Vasseur, *The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams*, RFC 6553 (Proposed Standard), Internet Engineering Task Force, Mar. 2012.

[11] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based lln network," in *Fifth International Conference on Ubiquitous and Future Networks (ICUFN'13)*, pp. 149–154, July 2013.

[12] K. D. Korte, A. Sehgal, and J. Schönwälder, "A study of the RPL repair process using contikirpl," in *Proceedings of Dependable Networks and Services*, LNCS 7279, pp. 50–61, Springer, 2012.

[13] M. Landsmann, H. Perrey, O. Ugus, M. Wählisch, and T. C. Schmidt, "Topology authentication in RPL," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'13)*, pp. 73–74, 2013.

[14] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: A study on qos security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[15] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors*, vol. 13, no. 10, pp. 3685–3692, 2013.

[16] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing RPL from topology attacks," in *Wireless Days*, pp. 1–3, 2011.

[17] A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance.," in *IEEE Symposium on Computers and Communications (ISCC'13)*, pp. 789–794, 2013.

[18] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, *The Trickle Algorithm*, RFC 6206 (Proposed Standard), Internet Engineering Task Force, Mar. 2011.

[19] P. Levis, A. Tavakoli, and S. Dawson-Haggerty, *Overview of Existing Routing Protocols for Low Power and Lossy Networks*, Internet Engineering Task Force (IETF) Internet Draft: draft-ietf-roll-protocols-survey-07, April 2009. (`http://tools.ietf.org/html/draft-levis-roll-overview-protocols-00`)

[20] A. Mayzaud, R. Badonnel, and I. Chrisment, "Monitoring and security for the internet of things," in *Emerging Management Mechanisms for the Future Internet*, LNCS 7943, pp. 37–40, Springer, 2013.

[21] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL dodag version attacks," in *Monitoring and Securing Virtualized Networks and Services*, LNCS 8508, pp. 92–104, Springer, 2014.

[22] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," *International Journal of Network Management*, 2015.

[23] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6lowpan in IOT," in *International Conference on Pervasive Computing (ICPC'15)*, pp. 1–6, Jan. 2015.

[24] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[25] A. Rghiout, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6lowpan-RPL networks: Issues and practical solutions," *Journal of Advanced Computer Science & Technology*, vol. 3, no. 2, pp. 143–153, 2014.

[26] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, "Addressing DODDAG inconsistency attacks in RPL networks," in *Proceedings of Global Information Infrastructure and Networking Symposium (GIIS'14)*, pp. 1–8, 2014.

[27] T. Tsao, R. Alexander, M. Dohler, V. Daza, A Lozano, and M. Richardson, *A Security Threat Analysis for Routing Protocol for Low-power and Lossy Networks (RPLs)*, RFC 7416, Internet Engineering Task Force, 2015.

[28] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-11, 2013.

[29] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[30] K. Weekly and K. S. J. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *Proceedings of the 20th IEEE International Conference on Network Protocols (ICNP'12)*, pp. 1–6, 2012.

[31] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, *RPL: IPv6 routing protocol for low-power and lossy networks*, RFC 6550, IETF, 2012.

[32] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "Routing loops in dag-based low power and lossy networks," in *Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 888–895, Washington, USA, 2010.

Anthéa Mayzaud is a researcher at the MADYNES Team at Inria, France and a third year PhD student at the University of Lorraine, France. She received her M. D. in Computer Science at TELECOM Nancy, France. Her main research interests are security issues in the Internet of Things mostly based on the RPL protocol and lightweight security solutions based on risk management.

Rémi Badonnel is an Associate Professor at TELECOM Nancy and a research staff member of the MADYNES Research Team at Inria. Previously he worked on change management methods and algorithms at IBM T.J. Watson in USA and on autonomous systems at the University College of Oslo in Norway. His research interests include network and service management, dynamic and autonomic environments, security and defence techniques.

Isabelle Chrisment is currently a Professor at TELECOM Nancy, University of Lorraine. She received her PhD in Computer Science in 1996 from University of Nice-Sophia Antipolis and her Habilitation Degree in 2005 from University of Lorraine. Head of the MADYNES Reseach team at Inria, her research activities focus on network monitoring and security within dynamic networks.

Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation

Arindom Ain[1], Monowar H. Bhuyan[1], Dhruba K. Bhattacharyya[2] and Jugal K. Kalita[3]
(Corresponding author: Monowar H. Bhuyan)

Department of Computer Science & Engineering, Kaziranga University[1]
Jorhat-785006, Assam, India
Department of Computer Science & Engineering, Tezpur University[2]
Tezpur-784028, Assam, India
Department of Computer Science, University of Colorado[3]
Colorado Springs, Co 80918, USA
(Email: {ainarindom, monowar.tezu}@gmail.com, dkb@tezu.ernet.in, jkalita@uccs.edu)
(Received Nov. 26, 2014; revised and accepted May 15 & July 4, 2015)

Abstract

A low-rate distributed denial of service (DDoS) attack has the ability to obscure its traffic because it is very similar to legitimate traffic. It can easily evade current detection mechanisms. Rank correlation measures can quantify significant differences between attack traffic and legitimate traffic based on their rank values. In this paper, we use two rank correlation measures, namely, Spearmen Rank Correlation (SRC) and Partial Rank Correlation (PRC) to detect low-rate DDoS attacks. These measures are empirically evaluated using three real-life datasets. Experimental results show that both measures can effectively discriminate legitimate traffic from attack traffic. We find that PRC performs better than SRC in detection of low-rate DDoS attacks in terms of spacing between malicious and legitimate traffic.

Keywords: DDoS attack, low-rate, network traffic, rank correlation

1 Introduction

With the rapid growth in the number of applications on Internet-connected computers and the devices and the rise in the sophistication of attacks on the application, early detection of Internet-based attacks is essential to reduce damage to legitimate user's traffic. A DDoS attack is a DoS attack that uses multiple distributed attack sources. Typically, attackers use a large number of compromised computers, also called zombies, to launch a DoS attack against a single target or multiple targets with the intention of making one or more services unavailable to intended users [4]. Botnets have become a powerful way to control a large number of hosts, allowing the launching of sophisticated and stealth DDoS attack on target host(s) quickly [3, 7].

In the recent past, botnets have become more intelligent and capable, and as a consequence the amount of attack traffic has increased targeting servers and components of Internet infrastructure such as firewalls, routers, DNS servers as well as network bandwidth. Regardless of how well secured the victim system may be, its susceptibility to DDoS attacks depends on the state of security in the rest of the global Internet [1, 10]. A lot of different tools are used by attackers to bypass security systems, and as a result, researchers have to upgrade their approaches to handle new attacks simultaneously. Some defense mechanisms concentrate on detecting an attack close to the victim machine, because the detection accuracy of these mechanisms is high. Network traffic comes in a stream of packets and it is difficult to distinguish legitimate traffic from attack traffic. More importantly, the volume of attack traffic can be much larger than the system can handle. The behavior of network traffic is reflected by its statistical properties [13] because such properties summarize behavior. Correlation measures can be used on the traffic summary to identify malicious traffic.

A network or host can be compromised with DDoS attacks using two types of traffic, namely, high-rate DDoS traffic and low-rate DDoS traffic. High-rate traffic is similar to flash crowd, i.e., when a large amount of unexpected legitimate traffic comes to a smallest server, and on the other hand, low-rate traffic is similar to legitimate traffic. So, it is very difficult to identify and mitigate either type of DDoS attack within a short time period [2].

Correlation coefficient is a measure that can be used to identify linear relationship between malicious and legitimate traffic. In this paper, we attempt to use rank corre-

lation to detect low-rate DDoS attacks. We use, two rank correlation techniques, namely, SRC and PRC.

The rest of the paper is organized as follows: Section 2 provides related work and observations. Section 3 presents the detection mechanism for low-rate DDoS attacks using rank correlation. Experimental results are reported in Section 4. Section 5 presents concluding remarks and future work.

2 Related Work

A DoS attack is characterized by an explicit attempt to prevent the legitimate use of a service [10]. A DDoS attack deploys multiple attacking entities to attain this goal. Much research has been devoted to the detection of DDoS attacks [11]. Wei et al. [14] propose a rank correlation based approach to detect reflection DDoS attacks. Once suspicious flows are found, it estimates the rank correlation between flow pairs and generates a final alert according to preset thresholds. Sheng et al. [12] discuss a measure based on Hurst coefficient to detect low-rate DDoS attacks. Bhuyan et al. [2] present an empirical evaluation of the suitability of various information metrics to detect both low-rate and high-rate DDoS attacks. Jin and Yeung [5] propose a covariance analysis model for detecting SYN flooding attacks. The method can accurately detect DDoS attacks with different intensities. It can also detect DDoS attacks which are similar to legitimate traffic. Mathew and Katkar [9] propose a light-weight software-based approach for low-rate DoS (LDoS) attack detection, and integrated it with an existing intrusion detection system. It does not require any change in existing infrastructure and protocol. Xiang et al. [15] present a generalized information metric to detect both low-rate and high-rate DDoS attacks. They consider the spacing between legitimate traffic and attack traffic in terms of an information distance measure. We observe the following based on literature survey.

- Although a large number of methods have been introduced to detect high-rate DDoS attacks, the number of methods to detect low-rate DDoS attacks is small. Most methods to detect low-rate DDoS attacks suffer from significant large percentage of false alarms.
- Most published detection methods, attempt to detect at the packet level for low-rate DDoS attacks. Though NetFlow traffic analysis is faster than packet level analysis.

3 Rank Correlation for Low-rate DDoS Attack Detection

Rank correlation has been found suitable as a potential metric to differentiate legitimate traffic from attack traffic [14]. Low-rate attacks exploit TCP retransmission time-out (RTO) to slowly reduce network throughput. An attacker causes legitimate TCP flow by entering the RTO state repeatedly. In a compromised host, it reduces the throughput significantly also reducing the bandwidth of the network simultaneously. A low-rate DDoS attack strategy is given in Figure 1. T is the total time interval for a period. T_w indicates the height of the attack burst, i.e., the strength of the attack traffic and T_x represents the burst length that indicates the pulse width. T_y is the time interval between two consecutive attack pulses, i.e., RTO + 2 round trip time (RTT). T_z is the interval between two pulses of high-rate traffic, i.e., legitimate traffic, N_a, N_b, and finally A_a, A_b, A_c are the high-rate attack traffic pulses towards a target from common effort of different attackers. The average volume of attack traffic can be calculated as $T_w * T_x/T$, which is much less than the legitimate TCP traffic [8]. So, it is difficult to detect attack traffic within short interval of time. In this work, two measures are used to detect low-rate DDoS attack, namely, Spearmen rank correlation and Partial rank correlation. Table 1 describes the symbols used to describe the method.

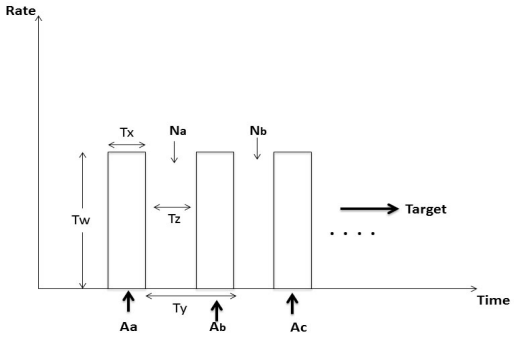


Figure 1: A low-rate DDoS attack strategy

3.1 Spearmen Rank Correlation

Spearman's correlation coefficient (SRC) measures the strength of association between two random variables better [14]. Spearman rank correlation coefficient between two random variables X and Y is computed as

$$r_{X,Y} = \frac{E(X,Y) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}}. \quad (1)$$

The coefficient $r_{X,Y}$ is the covariance value normalized by standard deviation, and E is the expected value. The use of rank measure correlation using characteristics that cannot be expressed quantitatively but that lend themselves to being ranked. A perfect linear relationship between the ranks yields a rank correlation coefficient of +1 for positive relationship (or -1 for a negative relationship) and no linear relationship between the ranks yields a rank correlation coefficient of 0.

Table 1: Symbol used

Symbols	Definition
T	time interval for processing
T_w	strength of the attack traffic
T_y	burst length that indicates pulse width
T_x	time interval between two consecutive attack pulse
T_z	interval between two pulses of high-rate traffic
N_a, N_b	legitimate traffic
A_a, A_b, A_c	high-rate attack traffic
t_i	i^{th} time interval within T
x_i	i^{th} instance within x
δ	threshold for attack detection
S	sample traffic
N	total number of packets within full time interval T
n	represents number of packets within the smaller time interval t within T

3.2 Partial Rank Correlation

Partial rank correlation (PRC) computes correlation between two random variables keeping one or more variables constant. The partial correlation between X and Y with a given set of n controlling variables Z = $Z_1, Z_2, Z_3, ., Z_n$, written as $r_{xy.z}$, is the correlation between residual r_x and r_y resulting from the linear regressions of X with Z and of Y with Z, respectively [6].

$$r_{xy.z} = \frac{r_{xy} - r_{xz}r_{yz}}{\sqrt{(1 - r_{xz}^2)(1 - r_{yz}^2)}} \quad (2)$$

where r_{xy} denotes the correlation between X and Y with Z constant. The rank correlation coefficient values vary from -1 to +1, where +1 indicates complete linear relationship, -1 indicates a negative linear relationship and 0 indicates no relationship. Partial correlation is a measure of the degree of association between two random variables keeping the third variable constant. The steps for rank correlation-based low-rate DDoS attack detection method is reported in Algorithm 1.

As stated in Algorithm 1, the sample period T considered for experimentation is divided into n intervals with, N being the total time interval. Three different network traffic instances, namely, x_i, x_j and x_k are considered. Rank correlation coefficient is calculated for each sample using Equation (1) or (2) within a sampling period T of the ith sample based on source IP, destination IP and protocol. If the rank correlation of x_i and x_j is greater than threshold $\geq \delta_1$ or rank correlation of x_i, x_j, x_k is greater than threshold $\geq \delta_2$, an alarm will be generated, else the router will send the packet to the next level of routers.

Algorithm 1 The low-rate DDoS attack detection

Input: x represents network traffic with respect to time window T and thresholds δ_1 and δ_2.
Output: alarm information (attack or legitimate).
Steps:

1) initialization: sample period T = $t_1, t_2, t_3, ..., t_N$ where N is the full time interval. x_i, x_j, x_k represent three different network traffic instances
2) sample the network traffic x received from upstream router R based on sampling period T
3) compute rank correlation coefficient using Equation (1) or (2) for each sample within T sampling period of ith sample based on traffic features (i.e., source IP, destination IP and protocol).
4) Check whether $RC(x_i, x_j) \geq \delta_1$ or $RC(x_i, x_j, x_k) \geq \delta_2$, if so generate alarm; otherwise, router sends the packets to the next level routers.
5) go to Step 2.

3.3 Complexity Analysis

Both spearman rank correlation and partial rank correlation work in quadratic time, $O(n^2T)$, where n is the number of traffic instances within a sample, T is the time interval. Though the complexity is high the rank correlation reveals that:

1) It can discriminate legitimate traffic from attack traffic correctly.
2) PRC can significantly identify low-rate DDoS attack with high linear correlation value.

4 Experimental Analysis

In this section, experimental results are presented for both the rank correlation measures using benchmark datasets.

4.1 Datasets

The evaluation of any detection method is extremely important before deployment in a real-time network. Two different datasets are used, namely: (i) MIT Lincoln Laboratory and (ii) CAIDA DDoS 2007 dataset. The MIT dataset contains pure legitimate traffic in tcpdump format. It does not contain any attack traffic. Even though it is old it is still useful and widely used [11]. The CAIDA DDoS 2007 dataset contains 5 minutes of anonymized traffic from a DDoS attack on August 4, 2007. This traffic trace contains only traffic to the victim and responses from the victim. If more than 10,000 attack packets per second are forwarded to the victim machine, it is known as high-rate attack traffic [11]. If up to 1000 attack packets per seconds are forwarded to the victim machine, it is

considered low-rate attack traffic [11]. So, low-rate attack may be similar in nature with legitimate traffic.

4.2 Results

Initially the total time interval is splits into 10 second sub-intervals. Three packet attributes are used during the experiment, namely, source IP, destination IP and protocol. For a victim-end based detection system, source IP is important, especially to find source hosts even though they may be spoofed. The destination IP is also important to identify and to estimate the traffic flowing to a particular target. The attribute protocol is added to identify the attack type. Each sample is processed one at a time. The rank correlation measure is applied to find the linear relationship between legitimate and attack traffic.

Figures 2 and 3 show the probability density of legitimate and attack traffic when using the MIT dataset as legitimate traffic and the CAIDA dataset as attack traffic. Following Xiang et. al [15], the MIT dataset is considered legitimate traffic in our experiment. Spearmen rank correlation and partial rank correlation are computed on the two different datasets, namely, MIT legitimate and CAIDA attack dataset. These attack traffic instances are assumed to satisfy the low-rate attack properties. Results for both legitimate and attack traffic instances are reported for both rank correlation measures in Figures 4, 5, and 6 for PRC and 7, 8 and 9 for SRC. Correlation values for legitimate traffic and attack traffic are reported in Table 2. While using Spearmen rank correlation and partial rank correlation, Figures 10 and 11 report results for mixed traffic (i.e. both legitimate and attack traffic). We see that PRC can discriminate effectively legitimate traffic from attack traffic with rank correlation with min = 0.8 and max = 1.0. Figure 10 reports the attack and legitimate traffic rank values when using SRC and PRC. Figure 11 shows the spacing between legitimate traffic and attack traffic when using SRC and PRC. It seems that PRC has higher spacing than SRC. Better results are observed for those ranges of rank correlation values and are reported in Table 2, when detecting low-rate DDoS attacks.

Table 2: Ranges of correlation values

Rank correlations	Traffic type	Minimum	Maximum
PRC	normal-normal	-0.2	1.0
SRC	normal-normal	-2.7	0.8
PRC	attack-attack	0.8	1.0
SRC	attack-attack	0.89	1.0
PRC	normal-attack	-0.2	1.0
SRC	normal-attack	-2.8	0.9

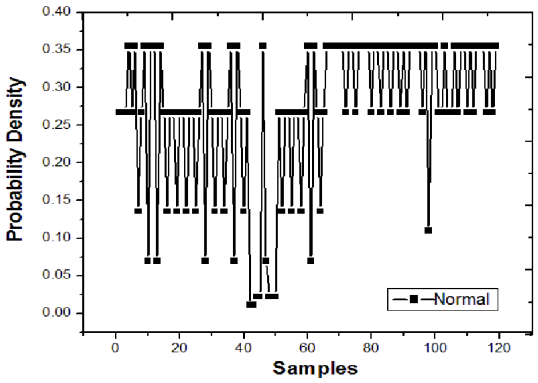


Figure 2: Probability density for legitimate traffic

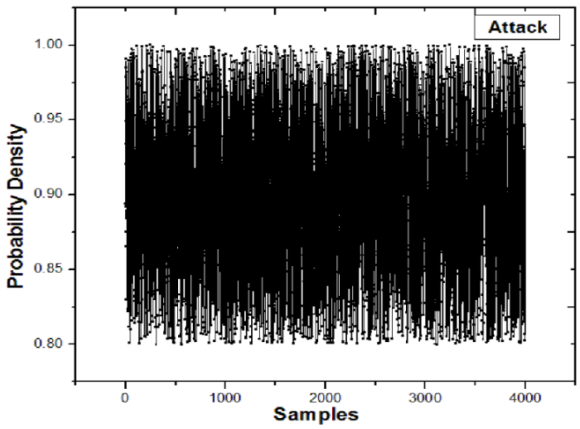


Figure 3: Probability density for attack traffic

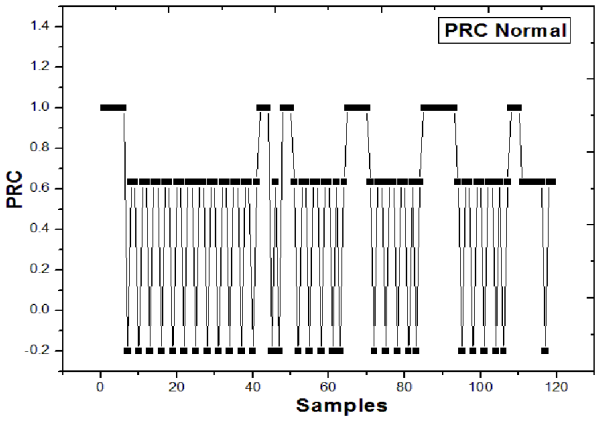


Figure 4: Partial rank correlation for legitimate traffic

4.3 Discussion

Based on the analysis, we make the following observations.

1) SRC uses a small number of parameters to estimate rank correlation.

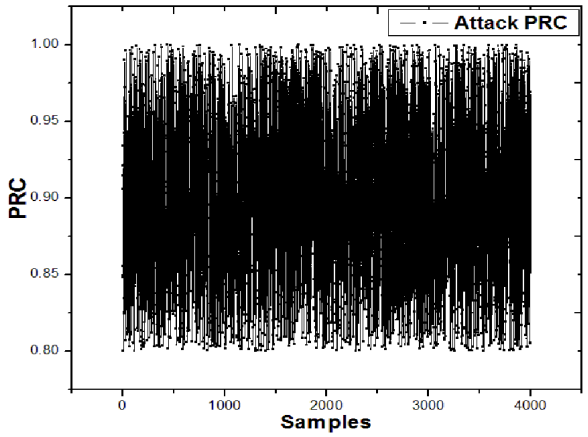


Figure 5: Partial rank correlation of attack traffic

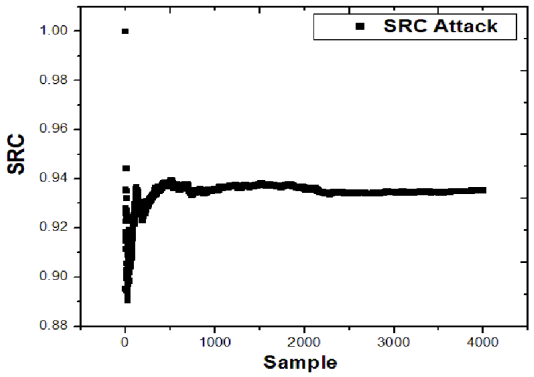


Figure 8: Spearmen rank correlation for attack traffic

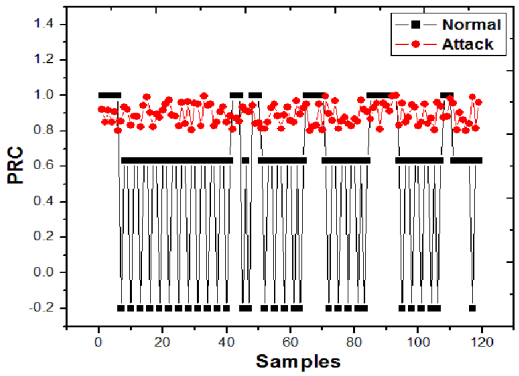


Figure 6: Partial rank correlation of legitimate and attack traffic

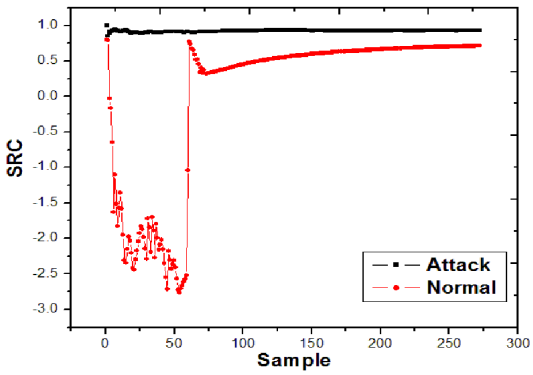


Figure 9: Spearmen rank correlation of legitimate and attack traffic

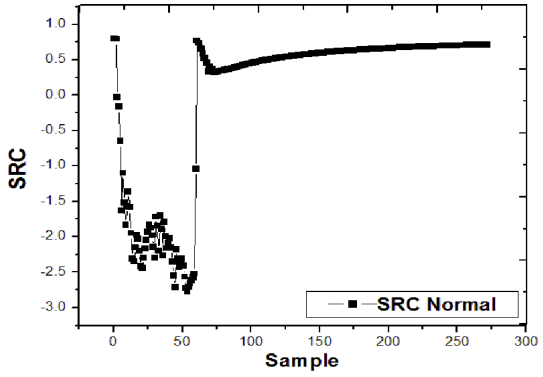


Figure 7: Spearmen rank correlation for legitimate traffic

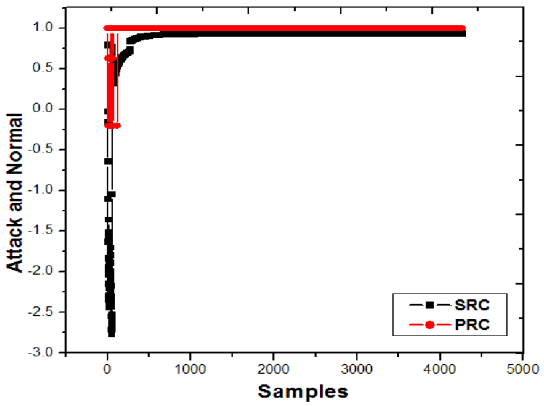


Figure 10: Rank correlation for attack and legitimate traffic using SRC and PRC

2) Both correlation measures are capable of differentiating legitimate traffic from malicious traffic correctly.

3) The partial rank correlation measure is effective in reducing false alarms in a victim-end defence system. It is due to higher spacing between legitimate and attack traffic.

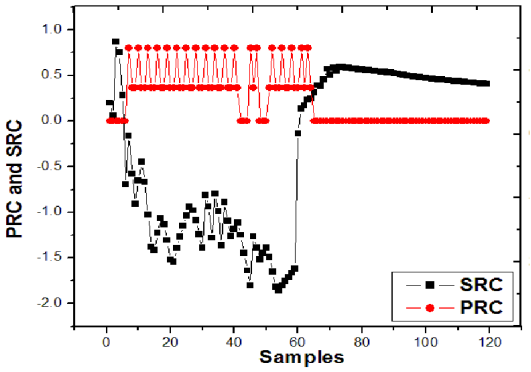


Figure 11: Shows difference between PRC and SRC

5 Conclusion

In this paper, we have presented an empirical study of rank correlation used to detect low-rate distributed DoS attacks. PRC and SRC both are used to effectively differentiate legitimate traffic from malicious traffic. Our experimental study, show that PRC is more effective than SRC in differentiating legitimate traffic from attack traffic. Development of a traceback mechanism to support low-rate DDoS attack is underway.

References

[1] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Information metrics for low-rate DDoS attack detection: A comparative evaluation," in *Seventh IEEE International Conference on Contemporary Computing (IC3'14)*, pp. 80–84, 2014.

[2] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection," *Pattern Recognition Letters*, vol. 51, pp. 1–7, 2015.

[3] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting distributed denial of service attacks: Methods, tools and future directions," *The Computer Journal*, vol. 57, no. 4, pp. 537–556, 2013.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys and Tutorials*, vol. 16, pp. 303–336, 2014.

[5] S. Jin and D. S. Yeung, "A covariance analysis model for DDoS attack detection," in *IEEE International Conference on Communications*, vol. 4, pp. 1882–1886, 2004.

[6] M. G. Kendall, "Partial rank correlation," *Biometrika*, vol. 32, no. 3/4, pp. 277–283, 1942.

[7] H. Liu and M. S. Kim, "Real-time detection of stealthy DDoS attacks using time-series decomposition," in *IEEE International Conference on Communications (ICC'10)*, pp. 1–6, 2010.

[8] G. Maciá-Fernández, J. E. Díaz-Verdejo, and P. García-Teodoro, "Mathematical model for low-rate DoS attacks against application servers," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 519–529, 2009.

[9] R. Mathew and V. Katkar, "Software based low rate DoS attack detection mechanism," *International Journal of Computer Applications*, vol. 20, no. 6, pp. 14–18, 2011.

[10] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[11] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115–139, 2006.

[12] Z. Sheng, Z. Qifei, P. Xuezeng, and Z. Xuhui, "Detection of low-rate DDoS attack based on self-similarity," in *Second International Workshop on Education Technology and Computer Science*, pp. 333–336, Washington, DC, USA, 2010.

[13] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denial-of-service attack detection based on multivariate correlation analysis," in *Neural Information Processing*, pp. 756–765, 2011.

[14] W. Wei, F. Chen, Y. Xia, and G. Jin, "A rank correlation based detection against distributed reflection DoS attacks," *IEEE Communications Letters*, vol. 17, no. 1, pp. 173–175, 2013.

[15] Y. Xiang, Ke Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426–437, 2011.

Arindom Ain received his Master's degree in Computer Application from Dibrugarh University, Assam, India in 2011. He is System Administrator at Kaziranga University, India. He is pursuing his Ph.D. from Sikkim Manipal University.

Monowar H. Bhuyan is an assistant professor in the Department of Computer Science and Engineering at Kaziranga University, Jorhat, Assam, India. He received his Ph.D. in Computer Science & Engineering from Tezpur University in 2014. His research areas include data and web mining, cloud security, computer and network security. He has published 20 papers in international journals and referred conference proceedings. Dr. Bhuyan has one book that will be published by Springer International, Germany.

Dhruba K. Bhattacharyya received his Ph.D. in Computer Science from Tezpur University in 1999. Currently, he is a Professor in the Computer Science & Engineering Department at Tezpur University. His research areas include data mining, network security and bioinformatics. Prof. Bhattacharyya has published 220 research papers in leading international journals and conference proceedings. Dr. Bhattacharyya also has written/edited 10 books.

Jugal K. Kalita is a professor of Computer Science at the University of Colorado at Colorado Springs. He received his Ph.D. from the University of Pennsylvania in 1990. His research interests are in natural language processing, machine learning, artificial intelligence, bioinformatics and applications of AI techniques to computer and network security. He has published 150 papers in international journals and referred conference proceedings and has written two technical books.

An ElGamal Encryption with Fuzzy Keyword Search on Cloud Environment

Yilei Wang[1], Wenyi Bao[1], Yang Zhao[1], Hu Xiong[1,2], and Zhiguang Qin[1]
(Corresponding author: Hu Xiong)
School of Information and Software Engineering, University of Electronic Science and Technology of China[1]
No. 4, North Jianshe Road, Chenghua District, chengdu, Sichuan 610054, China
State Key Laboratory of Information Security, Institute of Software & Chinese Academy of Sciences[2]
No. 19, Yuquan Road, Shijingshan District, Beijing 100190, China
(Email: xionghu.uestc@gmail.com)
(Received June 17, 2015; revised and accepted Aug. 12 & Aug. 24, 2015)

Abstract

With the continuous development of cloud computing, more and more sensitive data needs to be centrally stored in the cloud storage. For protecting the privacy of data, sensitive data must be encrypted before being outsourced to the server. The traditional PEKS (Public Encryption Keyword Search) enables users to search data by using keywords in the condition of encryption, however, it not only needs the security channel but also tolerates the huge pairing-computation. Although the pairing-free public key encryption with keyword search has been proposed, it can not support fuzzy keyword search and this drawback greatly reduces the usability of the system. In this paper, the proposed scheme features three good aspects: First, the keywords and data have been encrypted under the server's public key and thus the secure channel of the keywords transmission has been eliminated in the sense that the outside attackers cannot obtain any information related to the keywords without the knowledge of the server's private key. Second, our scheme not only supports accurate keyword search encryption but also supports the search when the keywords input have any spelling mistakes or format inconsistencies, which significantly improved the availability of the system. Finally, the proposed scheme is constructed on the El Gamal encryption instead of the bilinear-pairing encryption, which greatly improve the computational efficiency.

Keywords: Cloud environment, free secure-channel, fuzzy keywords

1 Introduction

With the development of cloud computing, more and more confidential documents will be stored in the cloud environment. But Clients also worry about the trust rank of the server, so the data stored in the cloud server will be encrypted. Clients can download the all data and decrypt it, then they will search what they want by keywords, however, the process will expend a lot of time and cost. So, it's more and more important to propose an effective searchable encryption scheme.

Boneh et al. propose the keyword search scheme under the condition of public key encryption for the first time in [2]. But a secure channel is established between the server and receiver to transmit data. As all we know, the computing overhead of bilinear pairings is very huge. Thokozani et al. propose a pairing-free PEKS scheme in [14] and it greatly reduces the computational cost. However, this scheme only allows exact keyword search, that is to say, the searching keywords can not tolerate any incorrect spellings and formats. The obvious drawbacks seriously reduces the availability of it.

In this paper, we propose a pairing-free public key encryption with fuzzy keyword search scheme, it does not need to establish a secure channel between the server and receiver. For creating a PEKS ciphertext, the sender will use the server's public key and his own public key. Meanwhile the scheme also supports fuzzy keyword search and don't need to encrypt keywords by bilinear pairings needing much computing cost. When the keyword input by users exactly match the defined keyword, the server will return the related files containing it directly. When the exact match fails, according to the similar semantics of keywords, the server will return the most likely similar matching files. More accurately, this paper will use the similar semantics in [8] and specifically use edit distance to quantify the similarity of the keywords. We will use the wildcard technology to solve the problem of the creation of fuzzy keyword sets. There is no need to list all keywords, and the number of fuzzy keyword sets greatly decrease by utilizing wildcard technology. Compared with the previous schemes, ours meets the three requirements:

1) Secure channel-free;

2) Pairing-free;

3) Fuzzy keyword search.

1.1 Related Work

The earliest PEKS scheme was proposed in [2], in which the user can send a secret key to the server, the server can identify all of the data files which contain keywords searched but he can't get any information about the data files. An secure channel-free PEKS scheme was proposed by Baek in [1], the basic idea of it is that the server has its own public key and private key, the data owner creates a PEKS ciphertext by using the server's public key and their own, then the receiver can send a trapdoor to retrieve files through a public channel because the outside attacker that has not obtained the server's private key cannot make any decisions about the PEKS ciphertexts even though the attacker gets all the trapdoors for the keywords that it holds. Fuzzy keyword search over encrypted was first proposed in [8], the scheme use edit distance to quantify the similarity of the keyword and use wildcard technology to create fuzzy keyword sets, the server can return the IDs of files by matching the index of similar keywords, but, its trapdoor is unsafe and vulnerable to keyword guessing attack. Most PEKS proposed so far are based on the bilinear pairings. Thokozani et al. proposed a pairing-free PEKS in [14] and it improved computational efficiency greatly, but this scheme can't support fuzzy keyword search.

Rhee et al. point out that the SCF-PEKS scheme suffers from keyword guessing attack and proposed a scheme which satisfies the property of trapdoor indistinguishability without using an additional secure channel in [11]. For achieving a more effective search, a similar "index" technology was proposed in [9], in which a single index of encrypted hash table is established for the whole file storage. In the index table, each item is made up of the trapdoor of keywords and the encrypted collection of identify numbers of the files which contain relevant keywords. Both of the two schemes only support exact keyword search. Min-Shiang Hwang et al. propose a Study of PEKS in [4] which is a summary of PEKSs and show an overview of six existing security models of PEKS/SCF-PEKS scheme and conclude five security requirements that must satisfy to construct a secure PEKS/SCF-PEKS scheme.

A scheme supports secure keyword ranking was proposed in [15] and returned the ranking of searching files through an effective technology, which enhances the usability of searching system. In [10], an efficient PEKS scheme was proposed, which allows the server to participate in the decipherment, and to return only files containing certain keywords specified by the users, so as to reduce both the computational and communication overhead in decryption for users, on the condition of preserving user data privacy and user querying privacy. Shih-Ting Hsu et al. propose a study of CKSS in [5] and examine six security models by concluding the secret-key setting and public-key setting, and sum up six security requirements that must satisfy to construct a secure conjunctive keyword searchable scheme.

1.2 The Advantages of Our Scheme

According to [1, 2, 8], most PEKSs schemes cannot support the public key encryption with fuzzy keyword search. For example, after sending the encrypted messages along with the corresponding keywords into the cloud server, the data owner cannot perform the keyword searching in case the exact passwords has been forgotten, which usually happens when many files has been outsourced in the remote cloud server.

In the addition, most PEKSs need to encrypt keyword ciphertext by bilinear pairings needing much computing cost which will reduce the efficiency of schemes. Although Thokozani et al. proposed a pairing-free PEKS in [14] and it improved computational efficiency greatly. However, there are some obvious drawbacks in the scheme. First the scheme can't decrypt the ciphertext to get the correct messages because its decryption algorithm has some mistakes. Second, it uses the server's public key to encrypt the trapdoor instead of the keyword ciphertext, so, it needs a secure channel to transport the trapdoor.

Different from previous schemes, our proposed scheme provides a promising solution to this problem by supporting public key encryption with keywords search. In this way, only part of keywords or the keywords with some spelling errors can be used to perform the keyword search. Furthermore, our scheme is constructed on the ElGamal instead of bilinear pairings to encrypt keywords, which significantly improve the efficiency.

1.3 Organization

The organization of this paper is as follows. Some preliminaries are given in Section 2. The proposed ElGamal encryption with fuzzy keyword search on cloud environment are given in Section 3. The comparison of efficiency is given in Section 4. Its security analyse is given in Section 5. The conclusions will be made in Section 6.

2 Preliminaries

In this section, we will review the traditional PEKS, the creating method of fuzzy keyword sets and the definition of some relevant knowledge.

2.1 The Sets of Fuzzy Keyword

For proposing an effective and practical fuzzy keyword search scheme, the concept of edit distance is introduced into the solution. If the editing operation is in the same position of a keyword, all relevant keywords will be listed. Using wildcards represents the same position of editing operation in [8].

Edit Distance. There are some methods to quantize the similarity of strings. A known edit distance is proposed in [6], $ed(w_1, w_2)$(denoting the edit distance of w_1 and w_2) means the number of operations which one keyword becoming another similar keyword needs.

The editing operation is made up of three parts:

1) Substitution: changing one character to another in a word;

2) Deletion: deleting one character from a word;

3) Insertion: inserting a single character into a word. Given a keyword w.

The wildcard-based fuzzy keyword set of w_i with edit distance d is denoted as $S_{w_i,d} = \{S'_{w_i,0}, S'_{w_i,1}, ..., S'_{w_i,d}\}$, where $S'_{w_i,\tau}$ denotes the set of words w'_i with τ wildcards. For example,assuming that edit distance $d = 1$ for the keyword "while", its wildcard-based fuzzy keyword set can denote $S_{while,1} = \{while, *while, *hile, w*ile, \cdots, whil*, while*\}$.

Fuzzy Keyword Search. Given a set of n encrypted data files $C = (F_1, F_2, ..., F_N)$ stored in the cloud server, a set of different keywords $W = w_1, w_2, ..., w_p$, given the edit distance d, a search input (w, k) (w denotes a keyword, $k(k \leqslant d)$ denotes the input of the edit distance). The server will return IDs of files after the execution of fuzzy keyword search and IDs whose corresponding the data files may contain the keyword w, denoting FID_{w_i}: if $w = w_i \in W$, return FID_{w_i} immediately; Or if $w \notin W$, return the IDs' set FID_{w_i} for $ed(w, w_i \leqslant k)$.

2.2 The First PEKS Scheme

As being described in [2], this search system is made up of a data owner, a data receiver, a server. The Data owner creates some data and then send the encrypted data and keywords to the server. When the server receives them, he can execute the search operating by obtaining the trapdoor from the data receiver. The Data receiver creates the trapdoor and send it to the server to search what he wants.

We review 4 steps of the public-key encryption search (PEKS) algorithm:

1) $KeyGen(s)$: Taking secure parameter s, then the algorithm generates the common public key and private key (pk, sk) of data owner and data receiver.

2) $PEKS(pk, W)$: Taking pk and a keyword W, the algorithm generates a PEKS ciphertext $S = PEKS(pk, W)$.

3) $Trapdoor(sk, W')$: Taking sk and a keyword W' input, the algorithm generates a search trapdoor $T_{w'}$.

4) $Test(pk, S, T_{w'})$: Taking the public key pk, the PEKS ciphertext S and the search trapdoor $T_{w'} = trapdoor(sk, W')$, the algorithm matches if $W = W'$, output "YES", otherwise output "NO".

Data owner executes $KeyGen$ algorithm to generate public-private key pairs. Then data receiver uses the algorithm $Trapdoor$ to generate the trapdoor $T_{W'}$ for a keyword W' input by him. After the server receives the trapdoor, he will execute $Test$ algorithm to determine whether these data files contain the keyword W'.

2.3 ElGamal Encryption

ElGamal encryption algorithm is a relatively common encryption algorithm and it is based on public key cryptosystem and elliptic curve encryption system which are proposed in 1984. Its security depends on elliptic curve discrete logarithm problem over the finite fields. The algorithm description is in [13] as follows:

KeyGen: First select a prime p and obtain primitive root g, a random element $x \in F_q$ in which both x and g are less than p, then computes $y = g^x$. The user's public key is y and private key is x.

Encryption: For encrypting a file F, pick a random element $r \in F_q$ and computes $c_1 = g^r, c_2 = F(g^x)^r$, then obtain the ciphertext $c_F = (c_1, c_2)$.

Decryption: Given $c_F = (c_1, c_2)$, recover the file by computing $c_2/c_1^x = F$.

2.4 Discrete Logarithm Problem

Discrete Logarithm Problem: Given a prime number p and a primitive element $a \in \mathbb{Z}_p(\mathbb{Z}_p$ is a finite field),for a integer $b \in \mathbb{Z}_\text{ı}$, finding the unique integer c make $a^c \equiv b(modp)$ is a difficult problem if selecting p carefully.

At present, there is not a polynomial time algorithm of computing discrete logarithm problem.

3 Construction

In the section, we will propose our scheme which not only support fuzzy keyword search but also encrypt keywords and data files by ElGamal instead of bilinear pairings, and needn't an additional secure channel to exchange a trapdoor.

Some public system parameters will be generated by first algorithm such as server's public key and private key, the sender's public key and private key.

1) $KeyGen(\gamma_1, \gamma_2)$: Taking the security parameters γ_1 and γ_2, this algorithm will generate public key $y = g^x$, private key x for the sender and public key $S = g^z$, private key z for the server.

   We suppose the value of edit distance is d, and suppose the keyword set $\{w_1, w_2, w_3, ..., w_i\}$ of every encrypted file in the cloud server. For setting up an index for each keyword w_i, first the sender will create a fuzzy keyword set of index $S_{w_i,d}$ ($S_{w_i,d}$ has been explained in Section 2). each element of $S_{w_i,d}$

is the keyword which uses wildcard technology. Every wildcard denotes an editing operation. Then the sender will encrypt each $w_i' \in S_{w_i,d}$. The description of PEKS algorithm is as follows.

2) $PEKS(y, S, w_i')$: To encrypt the keyword w_i', this algorithm first computes $c_i = h_1(w_i')$ and $C_{w_i'} = S \cdot y^{c_i}$ by using one-way hash function. Then the sender sends $C_{w_i'}$ to the server for storage.

   The data user needs to input (w, k) ((w, k) has been explained in Section 2) for searching files, and he will computes all trapdoors $\{T_{w'}\}_{w' \in S_{w,k}}$. the algorithm's description of computing every fuzzy keyword trapdoor based on wildcard-keyword is as follows.

3) $Trapdoor(x, w')$: To retrieve the data files which the user wants, the user chooses a dynamic random element a and computes two trapdoors $T'_{w'} = (g^{h_1(w')})^x \cdot g^a$ and $T''_{w'} = g^a$.

   The algorithm generates the trapdoor $T_{w'} = (T'_{w'}, T''_{w'})$, and when the user computes all fuzzy keyword trapdoors, he sends the trapdoor set $\{T_{w'}\}_{w' \in S_{w,k}}$ to the server for returning what he wants. the description of matching algorithm is as follows.

4) $Test(T'_w, z, C_{w_i'})$: First the server uses its private key to compute $C_w = (C_{w_i'}) \cdot g^{-z} = y^{c_i}$, then test whether $T'_{w'} = T''_{w'} \cdot C_w$. If $w_i' = w'$, the algorithm outputs "YES", then return the corresponding data files or else if $w_i' \neq w'$, the algorithm outputs "NO".

Our proposed scheme needn't a secure channel to transport the trapdoor because of the server's public key $S = g^z$ to encrypt the PEKS $C_{w_i'} = S \cdot y^{c_i}$, and can resist keyword guessing attack. By using El Gamal encryption instead of bilinear pairings encryption and supporting fuzzy keyword search, it improves the efficiency and usability significantly.

4 Comparison

In the section, the efficiency and usability analyse of our scheme and the others are compared as follows:

We compare our approach with Li et al. in [10], Baek et al. in [1], Rhee et al. in [11], Boneh et al. in [2], Thokozani et al. in [14] in term of the computation cost. To achieve the similar level of security for our pairing-free approach, the Koblitz elliptic curve $y^2 = x^3 + ax^2 + b$ can be used. The running time of the cryptographic operation listed in Table 1 can be derived using the standard cryptographic library. MIRACAL [12], and the hardware and OS for the experiment is PIV 3 GHZ processor with 512 M bytes storage capacity, and the Windows XP operating system respectively [3]. Bilinear pairings is the most expensive computation operation while scalar multiplication is the next and modular exponentiation is the third, hash function is the least.

Table 1: Cryptographic operation time in milliseconds

Operations	Time
ECC-based scalar multiplication	0.83
Exponential in $\mathbb{F}_{p^2}$	11.20
Pairing-based scalar multiplication	6.38
Pairing	20.01

Table 2: Frequency of each operation

Scheme	PA	SM	EX	HF
Li et al. in [10]	3	-	5	3
Baek et al. in [1]	2	2	1	1
Rhee et al. in [11]	3	3	3	3
Boneh et al. in [2]	1	3	1	3
Thokozani et al. in [14]	-	3	6	1
Our scheme	-	4	5	1

The number of keywords affects the space efficiency of the existing approaches and ours at the most extent. For example, we implement the experiment that there are 5000 keywords needed to be stored , a keyword takes up two bytes in average and each keyword has 50 corresponding fuzzy keywords. So all of keywords will take $5000 \times 2 \times 50 = 500000B \approx 488KB$. We can know that our scheme needs a little space to save keywords and rarely reduces the space efficiency.

Next,we can analyse the computation cost of our scheme that there are 4 scalar multiplications($S \cdot y^{c_i}$, $(g^{h_1(w')})^x \cdot g^a$, $(C_{w_i'}) \cdot g^{-z}$, $T''_{w'} \cdot C_w$), 5 exponentiations(y^{c_i}, $g^{h_1(w')}$, $(g^{h_1(w')})^x$, g^a, g^{-z}), 1 hash function($h_1(w_i')$). Also, we can analyse the computational overhead of the other five approaches in the Table 2.

In the Table 2, Let PA, SM, EX and HF be the abbreviate for the Pairing, Scalar Multiplication, Exponentiation and Hash Function, respectively. The comparison focuses on the operation implemented by the sender or the receiver with the server to have sufficient communication capability.

Thus, the computation efficiency is evaluated based on the method proposed in [7]. For example, in the algorithm of Baek et al.'s in [4], 2 PAs , 2 SMs , 1 EX, 1 HF are needed, and the computation time is $2 \times 6.38 + 2 \times 20.01 + 1 \times 11.20 = 63.98$ms(the computation cost of hash function can be ignored.). In the same way, we can calculate the other four existing schemes and ours($59.32ms$). Observing the comparison results listed in Chart 1, although, the computation cost of scheme in [2] is less than ours, it needs a extra secure channel to transport its trapdoor which reduce its efficiency. From the above, our scheme is more efficient than the existing schemes for implementing each exact keyword search.

When a user implements fuzzy keyword search, we denote the size of a fuzzy keyword set by n, n is a constant and he/she can compute n by some searching software quickly and cost $m = 59.32n$ ms for searching, so m is

Table 3: Comparison of usability assumption

Scheme	CT Ind	Trap Ind	SC	FKS
Li et al. in [10]	Satisfied	Not satisfied	Required	unsupported
Baek et al. in [1]	Satisfied	Not satisfied	Not Required	unsupported
Rhee et al. in [11]	Satisfied	Satisfied	Not Required	unsupported
Boneh et al. in [2]	Satisfied	Not satisfied	Required	unsupported
Thokozani et al. in [14]	Satisfied	Satisfied	Not Required	unsupported
Our scheme	Satisfied	Satisfied	Not Required	supported

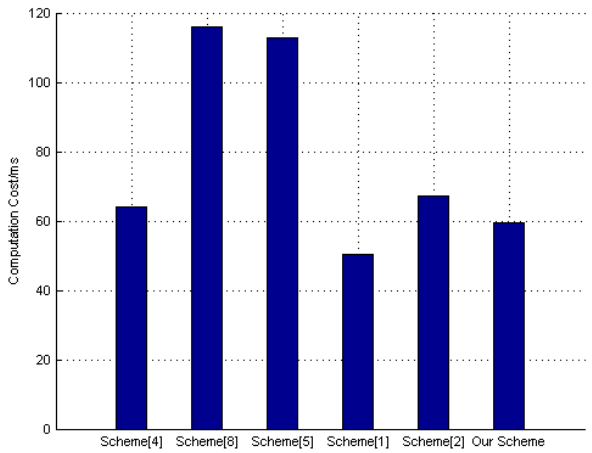


Figure 1: Comparison of the Existing Schemes on Computation Cost

also a constant and can be accepted.

In Table 3, we use CT Ind, Trap Ind, SC, FKS as abbreviations for the meaning of PEKS Ciphertext Indistinguishability, Trapdoor Indistinguishability, Secure Channel between a sender and server, and Fuzzy Keyword Search,respectively.

Our proposed scheme uses the lighter operation of exponentiation because the security bases of it are on the intractability of elliptic curve discrete logarithm problem and ElGamal encryption.

5 Security Analyse

The security of our proposed scheme will be discussed in the section.

As all we know, the first PEKS scheme in [2] is a non-interactive searchable encryption scheme semantically secure against a chosen keyword attack in the random oracle model. But in [2], a certain keyword corresponds to a constant trapdoor. Therefore, an outside attacker who intercepts and captures the communications can statistics the frequency of occurrences of these trapdoors, and then he can choose the highest frequency trapdoor to attack. Once the attack is successful, an attacker may know users privacy interests. So it is not against a keyword guessing attack.

Theorem 1. *Our pairing-free scheme satisfies the property of trapdoor indistinguishability which can be against a keyword guessing attack in the random oracle.*

Proof. As a malicious server or an outside attacker, he can not distinguish whether two trapdoors are from the same keyword. the trapdoor is changed each time because of the difference of the random element a we chooses. If the a is changed, $T'_{w'} = (g^{h_1(w')})^x \cdot g^a$ and $T''_{w'} = g^a$ will be also changed. So the trapdoor can not be distinguished. □

Theorem 2. *Our pairing-free scheme satisfies the property of keyword security in the random oracle.*

Proof. Even though an outsider attacker or a malicious server knows that two trapdoors are generated by the same keyword and intercept them, they can't do anything about the trapdoors. Suppose an outsider attacker captures the sender's private key x , the trapdoor $T_{w'}$ and g^a., then he will compute $g^{h_1(w')}$ through $T'_{w'}$ captured. Due to elliptic curve discrete logarithm problem, he can't compute $g^{h_1(w')}$. So he can't obtain any information about the trapdoor. □

6 Conclusion

In this paper, we propose an ElGamal encryption with fuzzy keyword search scheme on cloud environment. It not only supports accurate keyword search encryption but also supports the search when the keywords which are input have any spelling mistakes or format inconsistent situations. For bilinear pairings free, our scheme is more efficient than most others, and it can satisfies the property of trapdoor indistinguishability and keyword security in the random oracle based on the intractability of elliptic curve discrete logarithm problem and ElGamal encryption. Finally it is also a SCF-PEKS. How to reduce the size of a fuzzy keyword set effectively is our future master expectation.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61003230,

Grant 61370026, and Grant 61202445, in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2013J073, in part by the Applied Basic Research Program of Sichuan Province under Grant 2014JY0041, in part by the National High Technology Research and Development Program of China (863) under Grant 2015AA016007 and in part by the science and technology foundation of Sichuan Province under Grant 2014GZ0109.

References

[1] J. Baek, R. Safavi-Naini, W. Susilo, "Public key encryption with keyword search revisited," in *The 8th International Conference of Computational Science and Its Applications (ICCSA'08)*, pp. 1249–1259, Perugia, Italy, 2008.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovskyl, "Public key encryption with keyword search," in *The 22th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04)*, pp. 506–522, Heidelberg, Berlin, 2004.

[3] X. Cao, W. Kou, X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[4] S. T. Hsu, C. C. Yang, M. S. Hwang, "A study of public key encryption with keyword search," *International Journal of Network Security*, vol. 2, no. 15, pp. 71–79, 2013.

[5] C. C. Lee, S. T. Hsu, M. S. Hwang, "A study of conjunctive keyword searchable schemes," *International Journal of Network Security*, vol. 5, no. 15, pp. 321–330, 2013.

[6] V. Levenstein, "Binary codes capable of correcting spurious insertions and deletions of ones," *Problems of Information Transmission*, vol. 1, no. 1, pp. 8–17, 1965.

[7] J. Li, H. Du, Y. Zhang, T. Li, "Provably secure certificate-based key-insulated signature scheme," *Concurrency and Computation Practice and Experience*, vol. 26, no. 8, pp. 1546–1560, 2014.

[8] J. Li, Q. Wang, and C. Wang, "Fuzzy keyword search over encrypted data in cloud computing," in *The 29th Conference on Computer Communications (INFOCOM'10)*, pp. 1–5, San Diego, USA, Mar. 2010.

[9] M. Li, S. Yu, K. Ren, and W. Lou, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security (ACM'06)*, pp. 79–88, New York, NY, USA, 2006.

[10] Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 927–933, 2012.

[11] H. S. Rhee, J. H. Park, W. Susilo, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," *Journal of Systems and Software*, vol. 83, no. 5, pp. 763–771, 2010.

[12] M. Scott, *Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*, CertiVox Ltd, Aug. 2015. (`https://www.certivox.com/miracl`)

[13] Y. Tsiounis, M. Yung, "On the security of elgamal based encryption," in *The First International Workshop on Practice and Theory in Public Key Cryptography (PKC'98)*, pp. 117–134, Pacifico Yokohama, 1998.

[14] T. F. Vallent and H. Kim, "A pairing-free public key encryption with keyword searching for cloud storage services," in *The 5th International Conference of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (AFRICOMM'13)*, pp. 70–78, Kampala, Uganda, 2014.

[15] C. Wang, N. Cao, J. Li, "Secure ranked keyword search over encrypted cloud data," in *The IEEE 30th International Conference on Distributed Computing Systems (ICDCS'10)*, pp. 253–262, Genoa, Italy, 2010.

Yilei Wang is pursuing his Ph.D. degree in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). He received his B.S. degree from School of Communication and Information, UESTC, in 2008. He received his M.S. from Faculty of Engineering, Lund University of Sweden,in 2011. His research interests include security and application of mobile network data.

Wenyi Bao received his B.S. degree in the China University of Mining and Technology (CUMT) in 2009. He is currently pursing his M.S. degree in the School of Information and Software Engineering, UESTC. His research interests include: public key encryption with (fuzzy) keyword search.

Yang Zhao is an associate professor at the School of Computer Science and Engineering, UESTC. His research interests are in the area of networking security and e-commerce protocol.

Hu Xiong is an associate professor at the School of Information and Software Engineering, UESTC. He received his Ph.D degree from UESTC in 2009. His research interests include: cryptography and network security.

Zhiguang Qin is the dean and professor in the School of Information and Software Engineering, UESTC. He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.

Linear Complexity of a Family of Pseudorandom Discrete Logarithm Threshold Sequences

Chenhuang Wu[1,2], Xiaoni Du[3], and Zhengtao Jiang[4]
(Corresponding author: Chenhuang Wu)
School of Mathematics, Putian University[1]
Putian, Fujian 351100, P.R. China
School of Information Science and Technology, University of Science and Technology of China[2]
Hefei, Anhui 230000, P.R. China
(Email: ptuwch@163.com)
School of Mathematics and Information Science, Northwest Normal University[3]
Lanzhou, Gansu 730070, P.R. China
School of Computer Science, Communication University of China[4]
Chaoyang District, Beijing 100024, P.R. China
(Received Jan. 6, 2015; revised and accepted July 4 & Aug. 12, 2015)

Abstract

We discuss the linear complexity of a family of binary threshold sequence defined by the discrete logarithm of integers modulo a large prime. It is proved that the linear complexity is at least the half of their period and under some special conditions the linear complexity can achieve maximal.

Keywords: Binary threshold sequences, discrete logarithm, linear complexity

1 Introduction

A typical design approach to N-periodic sequences is application of cosets (or cyclotomic classes) via a subgroup of the group of invertible elements modulo N. Well-known basic examples are the Legendre and Jacobi sequences and their generalizations, which are related to discrete logarithm, see [4, 6, 8, 9, 10, 11, 12, 13] and references therein.

Let p be an odd prime. The *Legendre sequence* [9, 11, 16] $S_p = \{s_0, s_1, \ldots, s_{p-1}\}$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ is defined as

$$s_u = \begin{cases} 0, & \text{if } \left(\frac{u}{p}\right) = 1 \text{ or } p|u, \\ 1, & \text{otherwise,} \end{cases} \qquad u \geq 0$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Let g be a (fixed) primitive root modulo p and $\mathrm{ind}(n)$ be the discrete logarithm of n modulo p (to the base g) so that

$$g^{\mathrm{ind}(n)} \equiv n \pmod{p}, \quad p \nmid n, \quad 1 \leq \mathrm{ind}(n) \leq p-1.$$

Then we get an equivalent definition of S_p:

$$s_u = \begin{cases} 0, & \text{if } \mathrm{ind}(u) \equiv 0 \pmod 2 \text{ or } p|u, \\ 1, & \text{otherwise,} \end{cases} \qquad u \geq 0.$$

Legendre sequences have strong pseudorandom properties: equidistribution, optimal correlation, high linear complexity and k-error linear complexity, see [1, 2, 8, 9, 11, 16].

In particular, Sárközy studied in [19] the following binary sequence $E_p = \{e_0, e_1, \ldots, e_{p-1}\}$, which is called *discrete logarithm threshold sequence* in [3], over $\mathbb{F}_2$ defined by

$$e_u = \begin{cases} 0, & \text{if } 1 \leq \mathrm{ind}(u) \leq (p-1)/2, \\ 1, & \text{if } (p+1)/2 \leq \mathrm{ind}(u) \leq p-1 \text{ or } u = 0. \end{cases} \tag{1}$$

Gyarmati later extended this construction in [15]. (Note that [15, 19] actually dealed with the sequences $E'_p = \{e'_0, \ldots, e'_{p-1}\} \in \{-1, 1\}^p$ defined by $e'_n = (-1)^{e_n}$, $0 \leq n \leq p-1$.)

Sárközy estimated the well-distribution measure and the correlation measure of order k (see [17] for the notions) for E_p in [19] and Brandstätter and Winterhof estimated a lower bound on linear complexity profile of E_p in terms of the correlation measure of order k in [3]. In this short article, we will view E_p as a p-periodic sequence and consider its *linear complexity* (see below for the notion) under some special conditions. Below we consider this problem in a general way.

Let $p - 1 = 2df$ for large prime p. The cyclotomic classes of order $2d$ give a partition of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ defined by

$$D_l = \{g^{2di+l} \pmod{p} | i = 0, 1, \ldots, f-1\},$$

where $l = 0, 1, \ldots, 2d-1$. Then one can define binary sequences $\{e_u\}_{u\geq 0}$ of period p by setting

$$e_u = \begin{cases} 0, & \text{if } u \pmod p \in D_1 \cup \cdots \cup D_d, \\ 1, & \text{if } u \pmod p \in D_{d+1} \cup \cdots \cup D_{2d-1} \cup D_0, \\ 1, & \text{if } p|u, \end{cases} \tag{2}$$

where $u \geq 0$.

If $d = 1$, $\{e_u\}_{u\geq 0}$ is the complement of Legendre sequence. If $d = (p-1)/2$, $\{e_u\}_{u\geq 0}$ is the discrete logarithm threshold sequence E_p (viewing E_p as a p-periodic sequence) defined in Equation (1). The k-error linear complexity (over $\mathbb{F}_p$) of $\{e_u\}_{u\geq 0}$ was investigated in [1]. Certain pseudo-random measures of $\{e_u\}_{u\geq 0}$ were investigated in [6]. Below we consider the linear complexity (over $\mathbb{F}_2$) of $\{e_u\}_{u\geq 0}$ and hence obtain the linear complexity of E_p as a corollary in some special cases.

2 Linear Complexity

We recall that the *linear complexity* $L(\{s_t\}_{t\geq 0})$ of an N-periodic sequence $\{s_t\}_{t\geq 0}$ over $\mathbb{F}_2$ is the least order L of a linear recurrence relation over $\mathbb{F}_2$,

$$s_{t+L} = c_{L-1}s_{t+L-1} + \cdots + c_1 s_{t+1} + c_0 s_t \quad \text{for } t \geq 0$$

which is satisfied by $\{s_t\}_{t\geq 0}$ and where $c_0 = 1, c_1, \ldots, c_{L-1} \in \mathbb{F}_2$. The polynomial

$$M(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0 \in \mathbb{F}_2[x]$$

is called the *minimal polynomial* of $\{s_t\}_{t\geq 0}$. The *generating polynomial* of $\{s_t\}_{t\geq 0}$ is defined by

$$S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1} \in \mathbb{F}_2[x].$$

It is easy to see that

$$M(x) = (x^N - 1)/\gcd\left(x^N - 1,\ S(x)\right),$$

hence

$$L(\{s_t\}_{t\geq 0}) = \deg(M(x)) = N - \deg\left(\gcd(x^N - 1,\ S(x))\right), \tag{3}$$

see, e.g. [18] for details.

Lemma 1. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$, if $a \pmod p \in D_\ell$ for some $0 \leq \ell \leq 2d-1$, then we have*

$$aD_l = \{an \pmod p | n \in D_l\} = D_{l+\ell \pmod{2d}},$$

where $0 \leq l \leq 2d-1$.

Proof. Since $a \pmod p \in D_\ell$, there exists an integer $k_0 : 0 \leq k_0 < f$ such that $a \equiv g^{2dk_0+\ell} \pmod p$. Then we have

$$\begin{aligned} aD_l &= \left\{g^{2dk_0+\ell} \cdot g^{2dk+l} \pmod p |\ 0 \leq k < f\right\} \\ &= \left\{g^{2d(k_0+k)+(\ell+l)} \pmod p |\ 0 \leq k < f\right\} \\ &= D_{l+\ell \pmod{2d}}. \end{aligned}$$

□

For $0 \leq l \leq 2d-1$, define

$$D_l(x) = \sum_{n\in D_l} x^n \in \mathbb{F}_2[x]$$

and

$$U(x) = 1 + D_0(x) + D_{d+1}(x) + \cdots + D_{2d-1}(x), \tag{4}$$

which is the generating polynomial of $\{e_u\}_{u\geq 0}$ in Equation (2).

Lemma 2. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$, if $a \pmod p \in D_\ell$ for some $0 \leq \ell \leq 2d-1$, then we have*

$$D_l(x^a) \equiv D_{l+\ell \pmod{2d}}(x) \pmod{x^p - 1},$$

where $0 \leq l \leq 2d-1$.

Proof. By Lemma 1 and the definition of $D_l(x)$, we have

$$\begin{aligned} D_l(x^a) &= \textstyle\sum_{n\in D_l} x^{an} \\ &= \textstyle\sum_{m\in aD_l} x^m \\ &\equiv D_{l+\ell \pmod{2d}}(x) \pmod{x^p - 1}. \end{aligned}$$

□

Lemma 3. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$. For $U(x)$ in Equation (4), we have*

$$U(\beta^{ag^d}) = U(\beta^a) + 1,$$

where $\beta \in \overline{\mathbb{F}}_2$ is a primitive p-th root of unity.

Proof. Since $g^d \pmod p \in D_d$, using

$$D_0(\beta^a) + D_1(\beta^a) + \cdots + D_{2d-1}(\beta^a) = \sum_{i\in\mathbb{F}_p^*} \beta^{ai} = 1,$$

we have

$$\begin{aligned} & U(\beta^{ag^d}) \\ = \ & 1 + D_0(\beta^{ag^d}) + D_{d+1}(\beta^{ag^d}) + \cdots + D_{2d-1}(\beta^{ag^d}) \\ = \ & 1 + D_d(\beta^a) + D_1(\beta^a) + \cdots + D_{d-1}(\beta^a) \\ & \text{(by Lemma 2)} \\ = \ & 1 + 1 - D_0(\beta^a) - D_{d+1}(\beta^a) - \cdots - D_{2d-1}(\beta^a) \\ = \ & 1 + U(\beta^a). \end{aligned}$$

We note that the operations here (and hereafter) are performed in the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. □

Now we present main results of linear complexity of $\{e_u\}_{u\geq 0}$. According to Equation (3), we will consider below the number of $n : 0 \leq n < p$ such that $U(\beta^n) = 0$ for $\beta \in \overline{\mathbb{F}}_2$, which is a primitive p-th root of unity.

Proposition 1. *Let $p - 1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). Then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$\frac{p-1}{2} + \epsilon(\frac{p+1}{2}) \leq L(\{e_u\}_{u\geq 0}) \leq p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. As before, let $\beta \in \overline{\mathbb{F}}_2$ be a primitive p-th root of unity. If $U(\beta^n) = 0$ for some $n : 0 \le n < p$, we find that $U(\beta^{ng^d}) = 1$ by Lemma 3. We remark that the map $x \to xg^d$ on $\mathbb{F}_p^*$ is injective, so there are at most $(p-1)/2$ many $n \in \mathbb{F}_p^*$ such that $U(\beta^n) = 0$. Since there are exactly $(p+1)/2$ many 1's in one period of $\{e_u\}_{u\ge 0}$, we have $U(1) = (p+1)/2 \equiv 0 \pmod 2$ iff $\epsilon(\frac{p+1}{2}) = 0$. So in this case, we have the lower bound on linear complexity $L(\{e_u\}_{u\ge 0}) \ge (p-1)/2 + \epsilon(\frac{p+1}{2})$ and the upper bound $L(\{e_u\}_{u\ge 0}) \le p - 1 + \epsilon(\frac{p+1}{2})$ by Equation (3). □

For cryptographic applications, a sequence is required to have large linear complexity such that it can resist the Berlekamp-Massey algorithm. Below we discuss some special cases, under which the linear complexity of $\{e_u\}_{u\ge 0}$ is maximal.

Proposition 2. *Let $p - 1 = 2df$ and $\{e_u\}_{u\ge 0}$ be defined in Equation (2). If 2 is a primitive root modulo p, then the linear complexity of $\{e_u\}_{u\ge 0}$ satisfies*

$$L(\{e_u\}_{u\ge 0}) = p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. When 2 is a primitive root modulo p, we see that $x^{p-1} + \cdots + x + 1$ is irreducible and $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Since the minimal polynomial $M(x)$ of $\{e_u\}_{u\ge 0}$ satisfies $M(x)|(x^p - 1)$, there are only two choices for $M(x)$:

$$M(x) = x^p - 1 \quad \text{or} \quad M(x) = x^{p-1} + \cdots + x + 1.$$

On the other hand, we find that $\{e_u\}_{u\ge 0}$ satisfies the following recurrence relation

$$e_n + e_{n+1} + \cdots + e_{n+p-1} = (p+1)/2, \quad n \ge 0,$$

since again there are exactly $(p+1)/2$ many 1's in one period of $\{e_u\}_{u\ge 0}$. Hence $\epsilon(\frac{p+1}{2}) = 0$ implies $M(x) = x^{p-1} + \cdots + x + 1$ and $L(\{e_u\}_{u\ge 0}) = p - 1$, otherwise, $L(\{e_u\}_{u\ge 0}) = p$. □

When 2 is not a primitive root modulo p, it seems difficult to determine the linear complexity of $\{e_u\}_{u\ge 0}$, since now $x^{p-1} + \cdots + x + 1$ is reducible over $\mathbb{F}_2$. However, we have the following partial results.

Proposition 3. *Let $p - 1 = 2df$ and $\{e_u\}_{u\ge 0}$ be defined in Equation (2) and suppose that 2 is not a primitive root modulo p. If $2 \in D_0$ we have*

$$L(\{e_u\}_{u\ge 0}) = \frac{p-1}{2} + \epsilon(\frac{p+1}{2}).$$

And if $2 \in D_{\ell_0} \cup D_{2d-\ell_0}$ for some $1 \le \ell_0 \le d$ with $\ell_0|d$ or $\gcd(\ell_0, d) = 1$, we have

$$L(\{e_u\}_{u\ge 0}) = p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. Let $\beta \in \overline{\mathbb{F}}_2$ be a primitive p-th root of unity. If $2 \in D_0$, then $U(\beta^a) \in \mathbb{F}_2$ for all $a \in \mathbb{F}_p^*$ from the fact $(U(\beta^a))^2 = U(\beta^{2a}) = U(\beta^a)$. So by Lemma 3 for any $a \in \mathbb{F}_p^*$ either $U(\beta^a) = 0$ or $U(\beta^{ag^d}) = 0$, and hence there are exactly $(p-1)/2$ many $a \in \mathbb{F}_p^*$ such that $U(\beta^a) = 0$, which implies the value of the linear complexity.

For the second statement, we need to show $U(\beta^a) \notin \mathbb{F}_2$ for all $a \in \mathbb{F}_p^*$. Suppose that $U(\beta^{a_0}) \in \mathbb{F}_2$ for some $a_0 \in \mathbb{F}_p^*$. Firstly let $2 \in D_{\ell_0}$. Using the equation $(U(\beta^{a_0}))^{2^{i+1}} = (U(\beta^{a_0}))^{2^i}$ for all $i \ge 0$, we get

$$\sum_{k=1}^{\ell_0} D_{k+i\ell_0}(\beta^{a_0}) = \sum_{k=d+1}^{d+\ell_0} D_{k+i\ell_0}(\beta^{a_0}), \tag{5}$$

here and hereafter, the subscripts of D are all modulo $2d$.

If $\gcd(\ell_0, d) = 1$, after adjusting the equations above, we get

$$\sum_{k=1+j}^{\ell_0+j} D_k(\beta^{a_0}) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta^{a_0}) = 0$$

for $j = 0, 1, \ldots, d-1$. And hence we derive

$$\sum_{k=1+j}^{\ell_0+j} D_k(\beta) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta) = 0$$

for $j = 0, 1, \ldots, d-1$. If $d = 1$, it contradicts to

$$D_0(\beta) + D_1(\beta) = 1.$$

For $d > 1$, let

$$F_j(x) = \sum_{k=1+j}^{\ell_0+j} D_k(x) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(x).$$

For any $n \in D_i$, $0 \le i \le 2d-1$, we derive

$$\begin{aligned} F_j(\beta^n) &= \sum_{k=1+j}^{\ell_0+j} D_k(\beta^n) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta^n) \\ &= \sum_{k=1+j}^{\ell_0+j} D_{k+i}(\beta) + \sum_{k=d+1+j}^{d+\ell_0+j} D_{k+i}(\beta) \\ &= F_{j+i}(\beta) = 0 \end{aligned}$$

for $j = 0, 1, \ldots, d-1$. That is to say, each $F_j(x)$ has at least $p-1$ many roots. But we remark that $p - 1 = g^{(p-1)/2} = g^{df} \in D_0 \cup D_d$, which implies that there exists at least one $F_j(x)$ such that its degree is smaller than $p-1$, a contradiction.

If $\ell_0|d$, from Equation (5) we will get

$$\sum_{k=0}^{2d-1} D_k(\beta^{a_0}) = 0,$$

which contradicts to $\sum_{i\in\mathbb{F}_p^*} \beta^{ai} = 1$.

Secondly, let $2 \in D_{2d-\ell_0}$. Using

$$\sum_{i \in \mathbb{F}_p^*} \beta^{ai} = \sum_{k=0}^{2d-1} D_k(\beta^a) = 1$$

for all $a \in \mathbb{F}_p^*$, we derive a similar argument as above. □

In order to control the generation of $\{e_u\}_{u\geq 0}$ easily, we present the following corollary for special d.

Corollary 1. *Let $p-1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). If d is a prime, then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$L(\{e_u\}_{u\geq 0}) = \begin{cases} p-1+\epsilon(\frac{p+1}{2}), & \text{if } 2 \notin D_0, \\ \frac{p-1}{2}+\epsilon(\frac{p+1}{2}), & \text{if } 2 \in D_0, \end{cases}$$

where $\epsilon(z) \in \{0,1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Certain related binary sequences have been investigated in the references. As special cases of Corollary 1, the following cyclotomic sequence of order 4, which is a complement of $\{e_u\}_{u\geq 0}$ (in this case, $d=2$), see [8, Chapter 8] or [1], is defined as

$$f_u = \begin{cases} 0, & \text{if } u \pmod p \in \{0\} \cup D_0 \cup D_3, \\ 1, & \text{if } u \pmod p \in D_1 \cup D_2, \end{cases} \qquad u \geq 0,$$

and the cyclotomic sequence of order 6, see [14], is defined as

$$h_u = \begin{cases} 0, & \text{if } u \pmod p \in \{0\} \cup D_1 \cup D_2 \cup D_3, \\ 1, & \text{if } u \pmod p \in D_4 \cup D_5 \cup D_0, \end{cases} \quad u \geq 0$$

which is a slight modification of $\{e_u\}_{u\geq 0}$ (in this case, $d=3$). The idea of this article can help us to determine the linear complexity of $\{f_u\}_{u\geq 0}$ and $\{h_u\}_{u\geq 0}$.

Corollary 2. *Let $p-1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). If $d=4$, then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$L(\{e_u\}_{u\geq 0}) = \begin{cases} p-1+\epsilon(\frac{p+1}{2}), & \text{if } 2 \notin D_0, \\ \frac{p-1}{2}+\epsilon(\frac{p+1}{2}), & \text{if } 2 \in D_0, \end{cases}$$

where $\epsilon(z) \in \{0,1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Unfortunately, for other composite d, the argument is more complicated. With notations as in Proposition 3, when $1 < \gcd(\ell_0, d) < \ell_0$ experiments show that linear complexity might take other values except $p-1+\epsilon(\frac{p+1}{2})$ and $\frac{p-1}{2}+\epsilon(\frac{p+1}{2})$, see Table 1. In fact, let $\mathtt{ord}_p(2)$ be the order of 2 modulo p. When 2 is not a primitive root of p, from the fact that $x^{p-1}+\cdots+x+1$ can be written as the product of $\frac{p-1}{\mathtt{ord}_p(2)}$ many irreducible polynomials of degree $\mathtt{ord}_p(2)$ over $\mathbb{F}_2$, see e.g. [8], the linear complexity of $\{e_u\}_{u\geq 0}$ is of the form $\frac{p-1}{2}+k\cdot\mathtt{ord}_p(2)+\epsilon(\frac{p+1}{2})$ with some integer $0 \leq k \leq \frac{p-1}{2\cdot\mathtt{ord}_p(2)}$.

Table 1: Linear complexity of $\{e_u\}_{u\geq 0}$ for some p and d with $1 < \gcd(\ell_0, d) < \ell_0$

p	g	d	$L(\{e_u\}_{u\geq 0})$	ℓ_0	$\mathtt{ord}_p(2)$
31	3	15	25	6	5
73	5	12	55	8	9
127	3	63	119	54	7
151	6	15	120	10	15
241	7	15	193	6	10
337	10	12	253	8	12
337	10	24	293	16	21
601	7	60	551	48	25
631	3	21	540	14	45
881	3	40	826	16	55
911	17	65	819	20	91

Corollary 3. *Let E_p be the discrete logarithm threshold sequence (of period p) with the first period defined in Equation (1). Then the linear complexity of E_p satisfies*

$$L(E_p) \geq \frac{p-1}{2} + \epsilon(\frac{p+1}{2}).$$

In particular,

$$L(E_p) = p-1+\epsilon(\frac{p+1}{2})$$

if $(p-1)/2$ is prime or 2 is a primitive root modulo p.

There exist primes p such that $L(E_p) \neq p-1+\epsilon(\frac{p+1}{2})$ when $(p-1)/2$ is not a prime number. For example, in Table 1, $p=241$, we have $(p-1)/2 = 120$ and $L(E_p) = 193 \neq p-1+\epsilon(\frac{p+1}{2})$.

3 Concluding Remarks

In this work, we have shown that the linear complexity of a family of discrete logarithm threshold sequences of period p is at least the half of their period, which can resist the B-M attack. We also gave some special conditions under which the linear complexity can achieve maximal.

We remark that we only concentrate on the threshold sequences in terms of the discrete logarithm of integers modulo p. Recently a family of binary threshold sequences of period p^2 has been defined by using Fermat quotient and its generalizations, such sequences are related to discrete logarithm of integers modulo p^2 [5, 7, 22].

The idea of this work can also help us to deal with binary threshold sequences defined by the discrete logarithm of integers modulo p^r for $r \geq 3$. Actually Ref.[14] deals with the case of any $r \geq 2$ and $d=3$. Of course, it is interesting to study binary threshold sequences in terms of the discrete logarithm of integers modulo pq, thanks to the Jacobi sequence and its generalizations investigated in the literature [6, 10, 12, 20, 21].

Acknowledgements

The authors wish to thank Zhixiong Chen for helpful discussions. C.H.W. was partially supported by the National Natural Science Foundation of China under grant No.61373140, and the Natural Science Foundation of Fujian Province No.2015J01662. X.N.D. was partially supported by the National Natural Science Foundation of China under grant 61462077. Z.T.J. was partially supported by the National Natural Science Foundation of China(61103199), and the Engineering Program Project of CUC(3132015XNG1541).

References

[1] H. Aly, W. Meidl and A. Winterhof, "On the k-error linear complexity of cyclotomic sequences", *Journal of Mathematical Cryptology*, vol. 1, no. 3, pp. 283–296, 2007.

[2] H. Aly and A. Winterhof, "On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidel'nikov sequences", *Designs, Codes and Cryptography*, vol. 40, no. 3, pp. 369–374, 2006.

[3] N. Brandstätter and A. Winterhof, "Linear complexity profile of binary sequences with small correlation measure", *Periodica Mathematica Hungarica*, vol. 52, no. 2, pp. 1–8, 2006.

[4] A. Çeşmelioğlu and W. Meidl, "A General Approach to Construction and Determination of the Linear Complexity of Sequences Based on Cosets", in *Sequences and Their Applications (SETA'10)*, LNCS 6338, pp. 125–138, Springer, 2010.

[5] Z. Chen and X. Du, "On the linear complexity of binary threshold sequences derived from Fermat quotients", *Designs, Codes and Cryptography,* vol. 67, no. 3, pp. 317–323, 2013.

[6] Z. Chen, X. Du and G. Xiao, "Sequences Related to Legendre/Jacobi Sequences", *Information Sciences*, vol. 177, no. 21, pp. 4820–4831, 2007.

[7] Z. Chen, A. Ostafe and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients", *International Workshop on the Arithmetic of Finite Fields (WAIFI'10)*, LNCS 6087, pp. 73–85, Springer, 2010.

[8] T. W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998.

[9] C. Ding, "Pattern distribution of Legendre sequences", *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1693–1698, 1998.

[10] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2", *Finite Fields and Their Applications*, no. 3, pp. 159–174, 1997.

[11] C. Ding, T. Helleseth and W. Shan, "On the linear complexity of Legendre sequence", *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[12] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two", *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1699–1702, 1998.

[13] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Springer-Verlag, Berlin, 1991.

[14] X. Du and Z. Chen, "A Generalization of the Hall's Sextic Residue Sequences", *Information Sciences*, vol. 222, pp. 784–794, 2013.

[15] K. Gyarmati, "On a family of pseudorandom binary sequences", *Periodica Mathematica Hungarica*, vol. 49, no. 2, pp. 45–63, 2004.

[16] J. H. Kim and H. Y. Song, "Trace representation of Legendre sequences", *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 343–348, 2001.

[17] C. Mauduit and A. Sárközy, "On Finite Pseudorandom Binary Sequences I: Measures of Pseudorandomness, the Legendre Symbol", *Acta Arithmetica*, vol. 82, no. 12, pp. 365–377, 1997.

[18] H. Niederreiter, "Linear complexity and related complexity measures for sequences", *Progress in Cryptology (INDOCRYPT'03)*, LNCS 2904, pp. 1–17, Springer, 2010.

[19] A. Sárközy, "A finite pseudorandom binary sequence", *Studia Scientiarum Mathematicarum Hungarica*, vol. 38, no. 1–4, pp. 377–384, 2001.

[20] T. Yan, "New Binary Sequences of Period pq with Low Values of Correlation and Large Linear Complexity", *International Journal of Network Security*, vol. 10, no. 3, pp. 185–189, 2010.

[21] T. Yan, X. Du, S. Li and G. Xiao, "Trace representations and multi-rate constructions of two classes of generalized cyclotomic sequences", *International Journal of Network Security*, vol. 7, no. 2, pp. 269–272, 2008.

[22] C. Wu, Z. Chen and X. Du, "Binary Threshold Sequences Derived from Carmichael Quotients with Even Numbers Modulus", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E95-A, no. 7, pp. 1197–1199, 2012.

Chenhuang Wu was born in 1981. He received the M.S. degree in mathematics from Minnan Normal University in 2007. Now he is an associate professor of Putian University. His research interests include stream cipher, elliptic curve cryptography and digital signatures.

Xiaoni Du was born in 1972. She received the M.S degree in computer science from Lanzhou University in 2000 and Ph.D. degree in cryptography from Xidian University, China, in 2008, respectively. Now she is a professor of Northwest Normal University. Her research interests include cryptology and information security.

Zhengtao Jiang was born in 1976. He got doctor degree in 2005, and now he is an associate professor working for Department of Computer Science, Communication

University of China. His research interest include: Information security, Public opinion analysis, Computational advertising.

Stability Analysis of a Worm Propagation Model with Quarantine and Vaccination

Fangwei Wang[1,2], Fang Yang[3], Changguang Wang[1], Dongmei Zhao[1] and Yunkai Zhang[4]
(Corresponding author: Yunkai Zhang)

College of Information Technology, Hebei Normal University[1]
No. 20, South ErHuan Road, YuHua District, Shijiazhuang 050024, China
Shaanxi Key Laboratory of Network and System Security, Xidian University[2]
No. 1, TaiBai South Road, YanTa District, Xi'an 710071, China
Department of Science and Technology, Hebei Vocational College of Public Security Police[3]
No. 587, Gongnong Road, Qiaoxi District, Shijiazhuang 050011, China
Department of Information Engineering, Shijiazhuang Institute of Railway Technology[4]
No. 18, Sishuichang Road, Qiaodong District, Shijiazhuang 050071, China
(Email: zhyk@hebtu.edu.cn)
(Received Feb. 16, 2015; revised and accepted June 30 & July 29, 2015)

Abstract

Internet worms pose a serious threat to the Internet security. In order to effectively defend against Internet worms, this paper proposes a novel epidemic *e-SEIQV* model with quarantine and vaccination. Using this *e-SEIQV* model, we obtain the basic reproduction number for determining whether the worm dies out completely. The global stability of the worm-free equilibrium and the local stability of endemic equilibrium are proved, and determined by the basic reproduction number. Besides the impact of different parameters of this model is studied. Simulation results show that the number of susceptible and infected hosts are consistent with the theoretical analysis. The model provides a theoretical foundation for controlling and forecasting Internet worms.

Keywords: Endemic equilibrium, internet worm, network security, stability analysis, vaccination

1 Introduction

Internet worms are malicious codes which can replicate themselves and propagate via Internet. With the ever increasing number of Internet applications and the emergence of new technologies, Internet worms have become a great threat to our work and daily life, and caused tremendous economic losses. Especially, the advent of the Internet of things (IoT) would make the threat increasingly serious. How to combat Internet worms effectively is an urgent issue confronted with defenders. Therefore, it is necessary to comprehend the long-term behavior of worms and to propose effective strategies to defend against Internet worms. The similarity between the spread of biological viruses and that of Internet worms encourages researchers to adopt appropriately modified epidemic models to describe the propagation of worms across the Internet.

Based on the similarity between a malicious worm and a biological virus, some epidemic models representing worm propagation were presented to depict the propagation of worms, e.g., *SIR* model [17], *SIRS* model [10, 16], *SIQ* model [27], *SEIR* model [11], *SEIRS* model [15, 19], *SEIQV* model [20], *SEIQRS* model [28, 9], which assume that infected hosts in which the worm resides are in an exposed state and can not infect other hosts. Actually, an infected host which is in latency can infect other hosts by means of some methods, e.g., vulnerability seeking. All the previous models do not take this passive infectivity into consideration. Recently, Yang et al. [22, 23, 24, 25] proposed some models, by taking into account the fact that a host immediately possesses infectivity once it is infected. These models, however, all make an assumption that exposed hosts and infected hosts have the same infectivity. This is not consistent with the reality. Although an exposed host also sends scanning packets to find susceptive hosts with certain vulnerabilities, the number of scanning packets sent by an exposed host is less than that of an infected one. Usually, the infection rate of exposed hosts is less than that of infected ones. Therefore, they should have different infection rates.

Due to the frequent occurrence of worms over the Internet in the last decade, users usually install some antivirus softwares or firewalls to protect their hosts. Once a user feels that the performance of his host is degraded or there exists some useless data in disks (e.g., Witty can

do it), he will clean worms by antivirus softwares. In order to protect his important files, the user spontaneously clean worms even if he is not sure the existence of worms in his host. Additionally, an infected host often represents more obvious characteristics than an exposed host, the user could take some more effective measurements, e.g., patching. Therefore, the cured rate of exposed hosts would be lower than that of infected ones. The feature should be considered when modeling Internet worms. Recently, more attention has been paid to the combination of worm propagation model and countermeasures to study the prevalence of worms, e.g., quarantine [11, 20] and vaccination [4, 5, 14].

In this paper, we propose a new worm attack model, referred to as *e-SEIQV* (Susceptible - Exposed - Infectious - Quarantined - Vaccinated) model, which incorporates the features mentioned above. Using the basic reproduction number, we derive the global stabilities of a worm-free equilibrium and a unique endemic equilibrium by a Lyapunov function and a geometric approach. Based on these results and further analysis, some effective methods for controlling worms are recommended.

The rest of this paper is organized as follows. Section 2 formulates the new model and obtain its basic reproduction number. Section 3 proves the global stabilities of the worm-free equilibrium and the endemic equilibrium. Section 4 covers the numerical analysis and the simulations. Section 5 summarizes the paper with some future directions.

2 Model Formulation

The total host population N is partitioned into five groups and any host can potentially be in any of these groups at any time tick t: the susceptible, exposed (latent), infectious, quarantined, vaccinated, with sizes denoted by S, E, I, Q, V, respectively. The total number of population N at time t is given by $N(t) = S(t) + E(t) + I(t) + Q(t) + V(t)$. The dynamical transfer of hosts is depicted in the following figure.

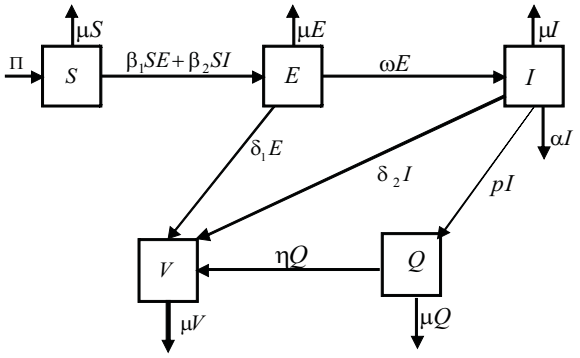


Figure 1: Schematic diagram for the flow of Internet worms

Figure 1 shows the five states and state transition in *e-SEIQV*. Based on the compartment model presented in Figure 1, the *e-SEIQV* model having infectious force in the exposed, infected period is described by the following system of differential equations:

$$\begin{cases} S'(t) = \Pi - \beta_1 SE - \beta_2 SI - \mu S, \\ E'(t) = \beta_1 SE + \beta_2 SI - (\mu + \delta_1 + \omega)E, \\ I'(t) = \omega E - (\mu + \alpha + \delta_2 + p)I, \\ Q'(t) = pI - (\eta + \mu)Q, \\ V'(t) = \delta_1 E + \delta_2 I + \eta Q - \mu V, \end{cases} \tag{1}$$

where Π is a constant recruitment of susceptible hosts. β_1, β_2 are the rates of the efficient contact in the latent, infected period, respectively. The positive parameter μ is the rate of natural death, α are non-negative constant and denote the rate of worm-caused death. δ_1, δ_1, ω are the transfer rates between the exposed and the vaccinated, between the infectious and the vaccinated, between the exposed and the infectious, respectively. The parameter p denotes the quarantined rate. The parameter η denotes the transfer rate between the quarantined and the vaccinated.

Summing the equations of the system (1), we obtain

$$N(t)' = \Pi - \mu N - \alpha I. \tag{2}$$

Therefore, the total population N may vary with time t. In the absence of disease, the total population size $N(t)$ converges to the the equilibrium Π/μ. It follows from Equation (2) that $\liminf_{t\to\infty} N(t) \le \Pi/\mu$. We thus study our system (1) in the following feasible region:

$$\Omega = \{(S, E, I, Q, V) \in \mathbb{R}^5_+ : S + E + I + Q + V \le \Pi/\mu\},$$

which is a positively invariant set of Model (1). We next consider the dynamic behavior of Model (1) on Ω.

Firstly, we obtain the basic reproduction number of Model (1) by the method of next generation matrix [1]. It is easy to see that Model (1) always has a worm-free equilibrium, $P_0 = (\Pi/\mu, 0, 0, 0, 0)$.

Let $x = (E, I, Q, V, S)^T$, then Model (1) can be written as

$$\frac{dx}{dt} = \mathcal{F}(x) - \mathcal{V}(x),$$

where

$$\mathcal{F}(x) = \begin{pmatrix} \beta_1 SE + \beta_2 SI \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$\mathcal{V}(x) = \begin{pmatrix} (\mu + \delta_1 + \omega)E \\ (\mu + \alpha + \delta_2 + p)I - \omega E \\ (\eta + \mu)Q - pI \\ \mu V - \delta_1 E - \delta_2 I - \eta Q \\ \beta_1 SE + \beta_2 SI + \mu S - \Pi \end{pmatrix}.$$

Differentiating $\mathcal{F}(x)$ and $\mathcal{V}(x)$ with respect to E, I, Q, V, S and evaluating at the worm-free equilibrium $P_0 = (\Pi/\mu, 0, 0, 0, 0)$, respectively, we have

$$D\mathcal{F}(P_0) = \begin{pmatrix} F_{2\times 2} & 0_{2\times 3} \\ 0_{3\times 2} & 0_{3\times 3} \end{pmatrix},$$

$$D\mathcal{V}(P_0) = \begin{pmatrix} Y_{2\times 2} & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ Y'_{3\times 2} & \eta+\mu & 0 & 0 \\ & -\eta & \mu & 0 \\ & 0 & 0 & \mu \end{pmatrix},$$

where

$$F_{2\times 2} = \begin{pmatrix} \frac{\beta_1\Pi}{\mu} & \frac{\beta_2\Pi}{\mu} \\ 0 & 0 \end{pmatrix}, Y'_{3\times 2} = \begin{pmatrix} 0 & -p \\ -\delta_1 & -\delta_2 \\ \frac{\beta_1\Pi}{\mu} & \frac{\beta_2\Pi}{\mu} \end{pmatrix},$$

and

$$Y_{2\times 2} = \begin{pmatrix} \mu+\delta_1+\omega & 0 \\ -\omega & \mu+\alpha+\delta_2+p \end{pmatrix}.$$

Thus, the spectral radius of the next generation matrix $\mathcal{F}\mathcal{V}^{-1}$ can be found as,

$$\rho(\mathcal{F}\mathcal{V}^{-1}) = \frac{\Pi(\beta_1(\mu+\alpha+\delta_2+p)+\beta_2\omega)}{\mu(\mu+\alpha+\delta_2+p)(\mu+\delta_1+\omega)}.$$

According to Theorem 2 in [1], the basic reproduction number of Model (1) is

$$R_0 = \frac{\Pi(\beta_1(\mu+\alpha+\delta_2+p)+\beta_2\omega)}{\mu(\mu+\alpha+\delta_2+p)(\mu+\delta_1+\omega)}. \quad (3)$$

For the concision of notation, let $m = \mu+\alpha+\delta_2+p$ and $n = \mu+\delta_1+\omega$. Thus $R_0 = \frac{\Pi(\beta_1 m+\beta_2\omega)}{\mu mn}$.

The endemic equilibrium $P^*(S^*, E^*, I^*, Q^*, V^*)$ of Model (1) is determined by equations

$$\begin{cases} \Pi - \beta_1 SE - \beta_2 SI - \mu S = 0, \\ \beta_1 SE + \beta_2 SI - nE = 0, \\ \omega E - mI = 0, \\ pI - (\eta+\mu)Q = 0, \\ \delta_1 E + \delta_2 I + \eta Q - \mu V = 0, \end{cases} \quad (4)$$

and

$$\Pi - \mu N - \alpha I = 0. \quad (5)$$

By some simple computation, we obtain

$$\begin{cases} S = \frac{\Pi\omega\alpha}{(\beta_1 m+\beta_2\omega)(\Pi-\mu N)+\alpha\omega\mu}, \\ E = \frac{m(\Pi-\mu N)}{\omega\alpha}, \\ I = \frac{\Pi-\mu N}{\alpha}, \\ Q = \frac{p(\Pi-\mu N)}{\alpha(\eta+\mu)}, \\ V = \frac{[\delta_1 m(\eta+\mu)+\omega\delta_2(\eta+\mu)+\omega\eta p](\Pi-\mu N)}{\omega(\eta+\mu)\mu\alpha}. \end{cases} \quad (6)$$

Substituting Equation (6) into the second equation of the system (1), N satisfies $F(N)(\Pi - \mu N) = 0$, where, $F(N) = [\mu mnN - \Pi(mn - \omega\alpha)](\beta_1 m + \beta_2\omega) - \mu mn\omega\alpha$.

For $R_0 > 1$, $F(0) = -\Pi(mn - \omega\alpha)(\beta_1 m + \beta_2\omega) - \mu mn\omega\alpha < 0$ and $F(\Pi/\mu) = \mu mn\omega\alpha(R_0 - 1)$, thus $F(N)$ is monotone increasing and $F(\Pi/\mu) > 0$. Within the interval $(0, \Pi/\mu)$, $F(N)$ has only a positive root. That is, Model (1) has an unique endemic equilibrium $P^*(S^*, E^*, I^*, Q^*, V^*)$, where S^*, E^*, I^*, Q^*, V^* are determined by Equation (6).

3 Analysis of Model

3.1 Global Stability of P_0

It is easily obtained that the model has a worm-free equilibrium given by $P_0 = (\Pi/\mu, 0, 0, 0, 0)$.

Lemma 1. *When $R_0 < 1$, the worm-free equilibrium P_0 is locally asymptotically stable in Ω. When $R_0 > 1$, the worm-free equilibrium P_0 is an unstable saddle point.*

Proof. The Jacobian matrices of Model (1) at P_0 is

$$J(P_0) = \begin{pmatrix} -\mu & -\frac{\beta_1\Pi}{\mu} & -\frac{\beta_2\Pi}{\mu} & 0 & 0 \\ 0 & \frac{\beta_1\Pi}{\mu} - n & \frac{\beta_2\Pi}{\mu} & 0 & 0 \\ 0 & \omega & -m & 0 & 0 \\ 0 & 0 & p & -(\eta+\mu) & 0 \\ 0 & \delta_1 & \delta_2 & \eta & -\mu \end{pmatrix}$$

It is easily obtained that $J(P_0)$ has three negative eigenvalues $\lambda_1 = \lambda_2 = -\mu$, and $\lambda_3 = -(\eta+\mu)$, the other eigenvalues of $J_{(0)}$ are determined by the following equation:

$$\lambda^2 + (m+n-\beta_1\Pi/\mu)\lambda + mn - (m\beta_1 + \omega\beta_2)\Pi/\mu = 0. \quad (7)$$

When $R_0 < 1$, $mn > (m\beta_1 + \omega\beta_2)\Pi/\mu$.

For $mn > (m\beta_1 + \omega\beta_2)\Pi/\mu$, we can obtain $m + n > m + \beta_1\Pi/\mu + \Pi\beta_2\omega/(\mu m)$, thus $m + n - \beta_1\Pi/\mu > m + \beta_2\Pi/\mu > 0$, which means the Equation (7) has two negative roots. Therefore, the worm-free equilibrium P_0 is locally asymptotically stable.

When $R_0 > 1$, $mn - (m\beta_1 + \omega\beta_2)\Pi/\mu < 0$, which means the Equation (7) has a positive root and a negative root. Therefore, the worm-free equilibrium P_0 is unstable saddle point. □

Lemma 2. *When $R_0 \leq 1$, the worm-free equilibrium P_0 is globally asymptotically stable in Ω. When $R_0 > 1$, all solutions starting in Ω and sufficiently close to P_0 move away from P_0.*

Proof. Consider the Lyapunov function

$$L = \frac{\beta_1 m + \beta_2\omega}{mn} E + \frac{\beta_2}{m} I.$$

Its derivative along the solutions to Model (1) is

$$\begin{aligned} L^{'} &= \tfrac{\beta_1 m+\beta_2\omega}{mn}(\beta_1 SE+\beta_2 SI-nE)+\tfrac{\beta_2}{m}(\omega E-mI) \\ &= \tfrac{\beta_1 m+\beta_2\omega}{mn}(\beta_1 SE+\beta_2 SI)-(\beta_1 E+\beta_2 I) \\ &= (\beta_1 E+\beta_2 I)(\tfrac{\beta_1 m+\beta_2\omega}{mn}S-1) \\ &\leq (\beta_1 E+\beta_2 I)(\tfrac{\Pi(\beta_1 m+\beta_2\omega)}{mn\mu}-1) \\ &= (\beta_1 E+\beta_2 I)(R_0-1) \\ &\leq 0. \end{aligned}$$

Furthermore, $L^{'}=0$ if and only if $E=I=0$ or $R_0=1$. Thus, the largest compact invariant set in $\{(S,E,I,Q,V)|L^{'}=0\}$ is the singleton $\{P_0\}$. When $R_0\leq 0$, the global stability of P_0 follows from LaSalle's invariance principle [6]. LaSalle's invariance principle [6] implies that P_0 is globally asymptotically stable in Ω. When $R_0>1$, it follows from the fact $L^{'}>0$ if $E>0$ and $I>0$. This completes the proof. □

3.2 Global Stability of P^*

Lemma 3. *When $R_0>1$, the endemic equilibrium P^* is locally asymptotically stable in Ω.*

Proof. Replacing S with $N-E-I-Q-V$ in Model (1), we obtain

$$\begin{cases} E^{'}(t)=(\beta_1 E+\beta_2 I)(N-E-I-Q-V)-nE, \\ I^{'}(t)=\omega E-mI, \\ Q^{'}(t)=pI-(\eta+\mu)Q, \\ V^{'}(t)=\delta_1 E+\delta_2 I+\eta Q-\mu V, \\ N^{'}(t)=\Pi-\mu N-\alpha I=0. \end{cases} \tag{8}$$

The Jacobian matrices of Model (8) at $P^*=(E^*,I^*,Q^*,V^*,N^*)$ is

$$J(P^*)=\begin{pmatrix} a\beta_1-b-n & a\beta_2-b & -b & -b & b \\ \omega & -m & 0 & 0 & 0 \\ 0 & p & -c & 0 & 0 \\ \delta_1 & \delta_2 & \eta & -\mu & 0 \\ 0 & -\alpha & 0 & 0 & -\mu \end{pmatrix}$$

where, $a=\frac{mn}{\beta_1 m+\beta_2\omega}$, $b=\beta_1 E+\beta_2 I$, and $c=\eta+\mu$. Its characteristic equation is $det(\lambda I-J(P^*))=0$, where I is the unit matrix. Therefore,

$$\begin{aligned} &det(\lambda I-J(P^*)) \\ &=(\lambda_1+\mu)(\lambda_2+(\eta+\mu))(\lambda^3+A\lambda^2+B\lambda+C)=0, \end{aligned}$$

where,

$$\begin{aligned} A &= b+m+\mu+n-\tfrac{\beta_1 mn}{\beta_1 m+\beta_2\omega} \\ &= b+\mu+m+\tfrac{\beta_2 n\omega}{\beta_1 m+\beta_2\omega}>0, \end{aligned}$$

$$\begin{aligned} B &= b(\delta_1+m+\mu+\omega)+m\mu+mn \\ &\quad +n\mu-(\tfrac{\beta_1 m^2 n+\beta_1 mn\mu+\beta_2 mn\omega}{\beta_1 m+\beta_2\omega}) \\ &= b(\delta_1+m+\mu+\omega)+m\mu+\tfrac{\beta_2\omega n\mu}{\beta_1 m+\beta_2\omega}>0, \end{aligned}$$

$$\begin{aligned} C &= b(m\delta_1+\alpha\omega+m\mu+\delta_2\omega+\omega\mu+p\omega) \\ &\quad +mn\mu-\tfrac{\beta_1 m^2 n\mu+\beta_2 mn\mu\omega}{\beta_1 m+\beta_2\omega} \\ &= b(m\delta_1+\alpha\omega+m\mu+\delta_2\omega+\omega\mu+p\omega)>0. \end{aligned}$$

By a direct calculation, we obtain that $AB-C>0$. According to the theorem of Routh-Hurwitz, the endemic equilibrium P^* is locally asymptotically stable. □

For Model (8), we consider global stability of the endemic equilibrium P^* when $\alpha=0$. Since $\liminf_{t\to\infty}N(t)\leq\Pi/\mu$, Model (9) is a four-dimensional asymptotically autonomous differential system with limit system

$$\begin{cases} E^{'}(t)=(\beta_1 E+\beta_2 I)(\frac{\Pi}{\mu}-E-I-Q-V)-nE, \\ I^{'}(t)=\omega E-mI, \\ Q^{'}(t)=pI-(\eta+\mu)Q, \\ V^{'}(t)=\delta_1 E+\delta_2 I+\eta Q-\mu V. \end{cases} \tag{9}$$

Next, we apply the geometrical approach [6] to investigate the global stability of the endemic equilibrium P^* in the region Ω.

Theorem 1. [6] *Consider the following systems:*
$x^{'}=f(x)$, $x\in\Omega$. If the following conditions are satisfied:

1) *The system $(*)$ exists a compact absorbing set $K\subset\Omega$ and has a unique equilibrium P^* in Ω;*
2) *P^* is locally asymptotically stable;*
3) *The system $(*)$ satisfies a Poincaré-Bendixson criterion;*
4) *A periodic orbit of the system $(*)$ is asymptotically orbitally stable, then the only equilibrium P^* is the globally asymptotically stable in Ω.*

Lemma 4. *If $R_0>1$, the unique positive equilibrium P^* of Model (9) is globally asymptotically stable in Ω.*

Proof. We only need to prove that all assumptions of Theorem 1 hold.

If $R_0>1$, then the worm-free equilibrium is unstable according to Lemma 1. Moreover, the behavior of the local dynamics near the region P_0 described in Lemma 1 implies that Model (9) is uniformly persistent in the region Ω. That is, there exists a constant $c>0$, such that any solution $(E(t),I(t),Q(t),V(t))$ of Model (9) with initial value $(E(0),I(0),Q(0),V(0))$ in Ω satisfies

$$min\{\liminf_{t\to\infty}E(t),\liminf_{t\to\infty}I(t),\liminf_{t\to\infty}Q(t),\liminf_{t\to\infty}V(t)\}\geq c.$$

This can be proved by applying a uniform persistent result in [3] and by the use of a similar argument as in the proof in [7]. The uniform persistence of system (9) in the bounded set Ω is equivalent to the existence of a compact $K\subset\Omega$ that is absorbing for system (9). In Section 3, during the process of obtaining the endemic equilibrium

P^*, we can know that P^* is the unique equilibrium in the interval $(0, \Pi/\mu)$. Assumption (1) holds.

According to Lemma 3, we know that the endemic equilibrium P^* is locally asymptotically stable in the region Ω. Assumption (2) holds.

The Jacobian matrix of Model (9) is denoted by

$$J(P^*) = \begin{pmatrix} \beta_1 S - b - n & \beta_2 S - b & -b & -b \\ \omega & -m & 0 & 0 \\ 0 & p & -c & 0 \\ \delta_1 & \delta_2 & \eta & -\mu \end{pmatrix}. \quad (10)$$

Choosing the matrix H as $H = diag(1, -1, 1, 1)$, it is easy to prove that HJH has non-positive off-diagonal elements, thus we can obtain that system (9) is competitive. This verifies the assumption (3).

The second compound matrix $J^{[2]}(P^*)$ of $J(P^*)$ can be calculated as follows:

$$J^{[2]}(P^*) = \begin{pmatrix} A1 & 0 & 0 & b & b & 0 \\ p & A2 & 0 & A & 0 & b \\ \delta_2 & \eta & A3 & 0 & A & -b \\ 0 & \omega & 0 & A4 & 0 & 0 \\ -\delta_1 & 0 & \omega & \eta & A5 & 0 \\ 0 & -\delta_1 & 0 & -\delta_2 & p & A6 \end{pmatrix} \quad (11)$$

where, $A = \beta_2 S - b$, $A1 = -(b + n + m - \beta_1 S)$,
$A2 = -(b + n + \eta + \mu - \beta_1 S)$, $A3 = -(b + n + \mu - \beta_1 S)$,
$A4 = -(m + \eta + \mu)$, $A5 = -(m + \mu)$, $A6 = -(\eta + 2\mu)$.

The second compound system of Model (9) in a periodic solution can be represented by the following differential equations:

$$\begin{cases} X^{'}(t) = A_1 X + bL + bM, \\ Y^{'}(t) = pX + A_2 Y - (b - \beta_2 S)L + bU, \\ Z^{'}(t) = \delta_2 X + \eta Y + A_3 Z - (b - \beta_2 S)M - bU, \\ L^{'}(t) = \omega Y - (m + \eta + \mu)L, \\ M^{'}(t) = -\delta_1 X + \omega Z + \eta L - (m + \mu)M, \\ U^{'}(t) = -\delta_1 Y - \delta_2 L + pM - (\eta + 2\mu)U. \end{cases} \quad (12)$$

In order to prove that the system (12) is asymptotically stable, we consider the following Lyapunov function:

$$V(X, Y, Z, L, M, U; E, I, Q, V)$$
$$= \sup\{|X| + |Y| + |Z|, \frac{E}{I}(|L| + |M| + |U|)\}.$$

According to the uniform persistence, we obtain that the orbit of $P(t) = (E(t), I(t), Q(t), V(t))$ remains a positive distance from the boundary of Ω, thus, we know that there exists a constant c satisfying

$$V(X, Y, Z, L, M, U; E, I, Q, V)$$
$$\geq c \sup\{|X|, |Y|, |Z|, |L|, |M|, |U|\},$$

for all $(X, Y, Z, L, M, U) \in \mathbb{R}^6$ and $(E, I, Q, V) \in P(t)$.

For the differential equations in Equation (12), we obtain the following differential inequalities by direct calculations:

$$D_+(|X| + |Y| + |Z|)$$
$$\leq -(2\mu + \delta_1 + \omega)(|X| + |Y| + |Z|)$$
$$+\frac{E}{I}(\beta_1 S + \beta_2 S \frac{I}{E})(|L| + |M| + |U|),$$

$$D_+(|X| + |Y| + |Z|)$$
$$\leq -(2\mu + \delta_1 + \omega)(|X| + |Y| + |Z|)$$
$$+\frac{E}{I}(\beta_1 S + \beta_2 S \frac{I}{E})(|L| + |M| + |U|),$$

Then,

$$D_+ \frac{E}{I}(|L| + |M| + |U|) \leq \omega \frac{E}{I}(|X| + |Y| + |Z|)$$
$$+(\frac{E^{'}}{E} - \frac{I^{'}}{I} - (2\mu + \alpha + \delta_2 + p))\frac{E}{I}(|L| + |M| + |U|).$$

From the pervious formula, we can obtain

$$D_+|V(t)| \leq \max\{g_1(t), g_2(t)\}V(t),$$

where,

$$g_1(t) = -(2\mu + \delta_1 + \omega) + (\beta_1 S + \beta_2 S \frac{I}{E}),$$

$$g_2(t) = \omega \frac{E}{I} + \frac{E^{'}}{E} - \frac{I^{'}}{I} - (2\mu + \alpha + \delta_2 + p).$$

From Model (1), we can obtain

$$\frac{E^{'}}{E} = \beta_1 S + \beta_2 S \frac{I}{E} - (\mu + \delta_1 + \omega),$$

$$\frac{I^{'}}{I} = \omega \frac{E}{I} - (\mu + \alpha + \delta_2 + p).$$

Therefore,

$$g_1(t) = \frac{E^{'}}{E} - \mu, g_2(t) = \frac{E^{'}}{E} - \mu.$$

Then,

$$\int_0^{\zeta} \sup\{g_1(t), g_2(t)\}dt \leq \ln E(t)|_0^{\zeta} - \mu\zeta = -\mu\zeta < 0,$$

which implies that $(X(t), Y(t), Z(t), L(t), M(t), U(t)) \to 0$, as $t \to \infty$. Thus, the second compound system (12) is asymptotically stable. This verifies the assumption (4).

We verify all the assumptions of Theorem 1. Therefore, P^* is globally asymptotically stable in Ω. □

4 Numerical Simulations

In this experiment, we choose the Code Red as basic behavior of a worm. The Code Red infected 360,000 hosts on July 19th 2001 [12], thus 360,000 hosts are selected as the population size. According to the real conditions of the Code Red worm, the worm's average scan rate is $s = 358$ per minute. Code Red worm's infection rate can then be computed as $\beta_2 = s/2^{32} = 8.34 \times 10^{-8}$, $\beta_1 = 8 \times 10^{-8}$. At the beginning, the number of susceptible, exposed, infected, quarantined and vaccinated hosts are $S(0) = 359,985$, $E(0) = 5$, $I(0) = 10$, $Q(0) = 0$ and $V(0) = 0$, respectively. The quarantined rate of infected hosts is $p = 0.2$ per minute, i.e., on average an infected host can propagate for about 5 minutes before it is alarmed and quarantined.

Other parameters in these simulations are given as follows: $\Pi = 2,160$, $\mu = 0.006$, $\gamma = 0.03$, $\theta = 0.03$, $\alpha = 0.005$, $\delta_1 = 0.02$, $\delta_2 = 0.04$, $\omega = 0.005$, $\eta = 0.005$, where $R_0 = 0.9873 < 1$. The worm will gradually disappear according to Theory 2. Figure 2 illustrates the number of susceptible and infected hosts when R_0 is 0.9873. From Figure 2, we can clearly see that the tendency of the worm propagation is depressive, which is consistent with Lemma 2. Finally, the whole population, in the long term, is in a vaccinated state. In order to effectively defend against such worms, we must adopt some feasible methods to decrease the infection rate [18, 21] or increase the following parameters (e.g., the transfer rates between the exposed and the recovered, between the exposed and the infectious) to guarantee the basic reproduction number $R_0 < 1$.

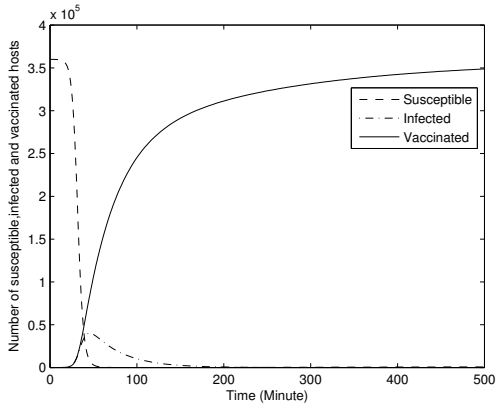


Figure 2: Globally asymptotically stable worm-free equilibrium

In the second experiment, the number of susceptible, exposed, infected, quarantined and vaccinated hosts are $S(0) = 359,985$, $E(0) = 5$, $I(0) = 10$, $Q(0) = 0$ and $V(0) = 0$, respectively. When $\delta_2 = 0.01$, $p = 0.02$, $\omega = 0.08$, we can obtain $R_0 = 6.9397 > 1$. For $\delta_2 = 0.01$, $p = 0.02$, $\omega = 0.04$, $R_0 = 10.5718 > 1$. For $\delta_2 = 0.01$, $p = 0.02$, $\omega = 0.02$, $R_0 = 11.2284 > 1$. Other parameters do not vary. We can see the results in Figure 3. As can be seen from Figure 3, the number of susceptible and infected hosts eventually become positive values between 0 and Π/μ. $S(t)$, $I(t)$ all approach their steady state, and the worm persists. This is fully consistent with the conclusions of Lemma 4.

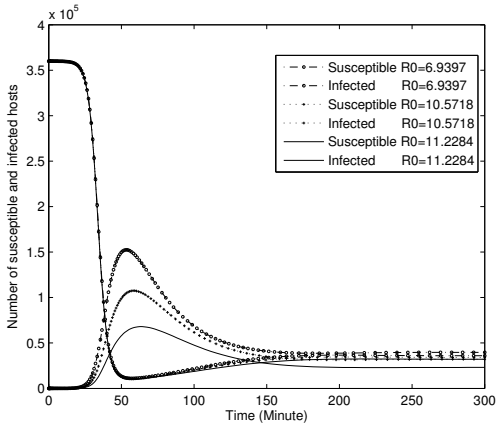


Figure 3: Globally asymptotically stable endemic equilibrium

With other parameters remaining the same, the quarantined rate p is set to different value at each time in order to state that the number of infected hosts is affected by every different value of the quarantined rate. Figure 4 shows the effects of changing the quarantined rate (which vary between 0.1 and 0.9) on worm propagations. As expected, a larger quarantined rate results in diminishing the worm propagation speed, and lowering the total number of infected hosts. Quarantined rate p relies mainly on the accuracy and detection speed of intrusion detection algorithms. Some methods have been proposed to reach the goal, e.g., a pulse quarantine strategy [26], an orchestration approach [2].

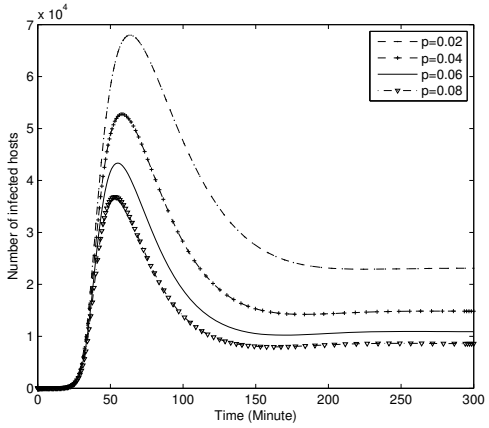


Figure 4: Effect of the quarantined rate p on the number of infected hosts

5 Conclusion

This paper presented a mathematical model to describe the dynamical behavior of an *e-SEIQV* epidemic model with quarantine and vaccination for Internet worms. Firstly, by the method of next generation matrix, we give the basic reproduction number to determine whether the worm extinguishes. Secondly, the global asymptotic stabilities of our model have been proved by using the Lyapunov function and a geometric approach. When the basic reproduction number is less than or equal to one, the proposed model has only a worm-free equilibrium being globally stable, which implies the worm dies out eventually; when the basic reproduction number is larger than one, our model has a unique endemic equilibrium being globally stable, which implies that the worm persists in the whole host population and tends to a steady state. Finally, some numerical examples are given to verify our conclusions. Our future work will expand this model to characterize more features of Internet worms, e.g., taking delay or impulse into consideration.

Acknowledgments

The authors gratefully acknowledge the erudite comments and suggestions of the anonymous reviewers, which have improved the presentation. This research was supported by the National Natural Science Foundation of China under No. 61272541 and No. 61572170, Natural Science Foundation of HeBei Province of China under No. F2015205157, Natural Science Foundation of Hebei Normal University of China under No. L2015Z08, Educational Commission of Hebei Province of China under No. QN2014165.

References

[1] V. D. Driessche, and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Mathematical Biosciences*, vol. 180, no. 1, pp. 29–48, 2002.

[2] E. Feitosa, E. Souto, and D.H. Sadok, "An orchestration approach for unwanted Internet traffic identification," *Computer Networks*, vol. 56, no. 12, pp. 2805–2831, 2012.

[3] H. I. Freedman, M. X. Tang, and S. G. Run, "Uniform persistence and flows near a closed positively invariant set," *Journal of Dynamics and Differential Equations*, vol. 6, no. 4, pp. 583–600, 1994.

[4] C. Gan, X. Yang, W. Liu, Q. Zhu, and X. Zhang, "An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate," *Applied Mathematics and Computation*, vol. 222, no. 3, pp. 265–274, 2013.

[5] C. Gan, X. Yang, W. Liu, and Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 92–100, 2014.

[6] J. P. LaSalle. *The Stability of Dynamical Systems, Regional Conference Series in Applied Mathematics*, SIAM, Philadelphia, PA, 1976.

[7] M. Y. Li, J. R. Graef, L. C. Wang, and J. Karsai, "Global dynamics of an SEIR model with varying total population size," *Mathematical Biosciences*, vol. 160, no. 2, pp. 191–213, 1999.

[8] M. Y. Li, and J. S. Muldowney, "A geometric approach to global-stability problems," *SIAM Journal on Mathematical Analysis*, vol. 27, no. 4, pp. 1070–1083, 1996.

[9] J. Liu, "Hopf bifurcation in a delayed SEIQRS model for the transmission of mali-cious objects in computer network," *Journal of Applied mathematics*, vol. 2014, Article ID 492198, 8 pages, 2014.

[10] B. K. Mishra, and S. K. Pandey, "Fuzzy epidemic model for the transmission of worms in computer network," *Nonlinear Analysis: Real World Applications*, vol. 11, no. 5, pp. 4335–4341, 2010.

[11] B. K. Mishra, and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[12] D. Moore, C. Shannon, and J. Brown, "Code Red: a case study on the spread and victims of an Internet worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, pp. 273–284, Marseille, France, 2002.

[13] J. S Muldowney, "Compound matrices and ordinary differential equations," *Rocky Mountain Journal of Mathematics*, vol. 20, no. 4, pp. 857–872, 1990.

[14] M. Ozair, and T. Hussain, "Analysis of vector-host model with latent stage having partial immunity," *Applied Mathematical Sciences*, vol. 8, no. 32, pp. 1569–1584, 2014.

[15] J. Ren, Y. Xu, Y. Zhang, Y. Dong, and G. Hao, "Dynamics of a delay-varying computer virus propagation model," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 371792, 12 pages, 2012.

[16] J. Ren, X. Yang, L. Yang, Y. Xu, and F. Yang, "A delayed computer virus propagation model and its dynamics," *Chaos Solitons Fractals*, vol. 45, no. 1, pp. 74–79, 2012.

[17] J. Ren, X. Yang, Q. Zhu, L. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[18] K. Simkhada, T. Taleb, Y. Waizumi, A. Jamalipour, and Y. Nemoto, "Combating against internet worms in large-scale network: an autonomic signature-based solution," *Security and Communication Networks*, vol. 2, no. 1, pp. 11–28, 2009.

[19] O. A. Toutonji, S. M. Yoo, and M. Park, "Stability analysis of VEISV propagation modeling for network worm attack," *Applied Mathematical Modelling*, vol. 36, no. 6, pp. 2751–2761, 2012.

[20] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. J. Moon, "Stability analysis of a SEIQV epidemic model for rapid spreading worms," *Computers and Security*, vol. 29, no. 4, pp. 410–418, 2010.

[21] Y. Wei, W. Xun, C. Adam, X. Dong, and L. David, "On detecting active worms with varying scan rate," *Computer Communications*, vol. 34, no. 11, pp. 1269–1282, 2011.

[22] L. Yang, X. Yang, L. Wen, and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307–2314, 2012.

[23] L. Yang, X. Yang, Q. Zhu, and L. Wen, "A computer virus model with graded cure rates," *Nonlinear Analysis: Real World Applications*, vol. 14, no. 1, pp. 414–422, 2013.

[24] M. Yang, Z. Zhang, Q. Li, and G. Zhang, "An SLBRS model with vertical transmission of Computer virus over the Internet," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 925648, 17 pages, 2012.

[25] X. Yang and L. Yang, "Towards the epidemiological modeling of computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012 Article ID 259671, 11 pages, 2013.

[26] Y. Yao, L. Guo, H. Guo, G. Yu, F. Gao, and X. Tong, "Pulse quarantine strategy of internet worm propagation: modeling and analysis," *Computers and Electrical Engineering*, vol. 38, no. 5, pp. 1047–1061, 2012.

[27] Y. Yao, L. Guo, G. Yu, F. Gao, and X. Tong, "Pulse quarantine strategy of internet worm propagation modeling and analysis," *Journal of Computers and Electrical Engineering*, vol. 38, vo. 5, pp. 1047–1061, 2012.

[28] Z. Zhang, and H. Yang, "Dynamics of a delayed model for the transmission of mali-cious objects in computer network," *The Scientific World Journal*, vol. 2014, Article ID 194104, 14 pages, 2014.

Fangwei Wang received his B.S. degree in 2000 from College of Mathematics & Information Sciences, Hebei Normal University, his M.S. degree in 2003 from College of Computer Science and Software, Hebei University of Technologyis, his Ph.D degree in 2009 from College of Computer at Xidian University. Currently he is an associate professor at Hebei Normal University, Shijiazhuang, China. His research interests include: network and information security, sensor networks.

Fang Yang received her B.S. degree in 2000 from College of Mathematics and Information Sciences, Hebei Normal University, his M.S. degree in 2005 from College of Computer Science and Technology, Huazhong University of Science and Technology. Currently she is a lecture at Hebei Vocational College of Public Security Police, Shijiazhuang, China. Her research interests include: network and information security.

Changguang Wang received his M.S. degree in 1996 from School of Physical Science and Technology, Sichuan University, and his Ph.D degree in 2009 from College of Computer at Xidian University. Currently he is a professor at Hebei Normal University, Shijiazhuang, China. His research interests include network and information security.

Dongmei Zhao received her M.S. and Ph.D degree in College of Computers from Xidian University, China in 1998 and 2006 respectively. Currently she is a professor at Hebei Normal University, Shijiazhuang, China. Her research interests include network and information security.

Yunkai Zhang received his B.S. degree in 1986 from Department of Electronic and Information Engineering, Hebei University, his M.S. degree in 1997 from Department of Telecommunication Engineering, Beijing University of Posts and Telecommunications, and his Ph.D degree in 2005 from College of Computer at Xidian University. Currently he is a professor at Hebei Normal University, Shijiazhuang, China. His research interests include network and information security.

Penetration Testing and Mitigation of Vulnerabilities Windows Server

Deris Stiawan[1], Mohd Yazid Idris[2], Abdul Hanan Abdullah[2], Mohammed AlQurashi[3], Rahmat Budiarto[3]

(Corresponding author: Deris Stiawan)

Department of Computer Science, Universitas Sriwijaya, Indonesia[1]
Department of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia[2]
College of Computer Science and Information Technology, Al Baha University, Kingdom of Saudi Arabia[3]
(Email: deris@unsri.ac.id)

(Received Jan. 15, 2015; revised and accepted Apr. 11 & Aug. 24, 2015)

Abstract

Cyber attack has become a major concern over the past few years. While the technical capability to attack has declined, hacking tools - both simple and comprehensive - are themselves evolving rapidly. Certain approaches are necessary to protect a system from cyber threats. This work engages with comprehensive penetration testing in order to find vulnerabilities in the Windows Server and exploit them. Some forms of method penetration testing have been used in this experiment, including reconnaissance probes, brute force attacks based on password guessing, implanting malware to create a backdoor for escalating privileges, and flooding the target. This experiment was focused on gaining access in order to ascertain the identities of hackers and thus better understand their methods and performed penetration testing to evaluate security flaws in the Windows Server, which is a famous OS for web applications. It is expected that this work will serve as a guideline for practitioners who want to prepare and protect their systems before putting them online.

Keywords: Mitigation, penetration testing, vulnerabilities, windows server

1 Introduction

A definition of hacking is presented by [9, 25]. These sources also identify security violation trends in internetworking and their effects. More illegal activities such as hacktivism, hacking and exploiting weaknesses have been described by [12, 16, 29] offer a different perspective by highlighting the potential economic threats and impacts of cyber attacks. A growing problem, hacking activities combine easy to learn pentest with a variety of tools such as those offered by C.E.H [11]. Moreover, they use both simple and comprehensive tools (defined as 'Metasploit'), as defined by [5, 21]. This reinforces the findings of previous work [14] which compares attack sophistication with attacker skill knowledge.

Meanwhile, analysis by [6, 12, 18] highlights an explosion of security threats in recent years such as Trojans, viruses, worms, adware, spyware and DoS which are continuing to grow, multiply and evolve. According to [14] indicate the technical capability to attack tended to decrease. On the other hand, hacking tools are getting more effective and also increasingly available and accessible to the public. Moreover, attackers are able to detect vulnerabilities faster than security experts or vendors and can cause time delays by patching in vulnerabilities.

Research conducted by [26, 27] found that Windows Server has more serious vulnerabilities, as several of its services and daemons are unsecured and open to access. This lays open the possibility of exploitation. Additionally [32] located vulnerabilities in the Apache and IIS HTTP server on the Windows Server operating system. [28] conducted an attack scenario on the Windows Server.

In order to understand how to protect against and prevent attacks, it is useful to understand from the attacker's perspective what methods they will use, what goals they have and how they launch their attacks. This experiment takes improvised actions to highlight several types of attacks carried out such as: probes to obtain detailed information, brute force for guessing passwords, gaining privileges access and flooding the target to reduce the availability of services.

The remainder of this paper is organized as follows. Section 2 presents the related works. Section 3 presents the taxonomy of the attack this experiment is concerned. Section 4 describes experimental experiments. This section deals with data collecting and an attack scenario including scanning and exploitation for mitigating vulnerability. Finally, Section 5 offers a conclusion and suggestions for future work.

2 Related Works

Penetration testing has been described in different ways since 1989 by [24]. New methods and approaches are continuously being expanded from year to year. In 2001, [7] described certain steps needed to prevent threats and convey the importance of understanding the mindset of an attacker, as well as their methods and goals. In line with that, [2] has suggested a methodology to ensure that the penetration testing exercise is reliable, repeatable and reportable.

Analyses and predictions by [12, 18] indicate that there has been an explosion of security threats in recent years. This has been corroborated and previously predicted by [17, 19], which describe a future war based on cyber attacks. More recently, [23] has predicted and analysed cyber attacks in the context of further security violation trends. Meanwhile, [10] has referred to Microsoft warning users about the strengths of character passwords such as: a combination of case sensitive letters and digits, maximum-minimum password age, and minimum password length.

Furthermore, it seems that every bug can cause vulnerabilities which are existent and undocumented, often never being revealed, discovered or exploited. From the attacker's perspective, vulnerability is an opportunity that can be exploited. A vulnerability database is a collection of records containing technical descriptions of vulnerabilities in computer systems. Common Vulnerabilities and Exposures (CVE) began in 1999 as a result of the adoption of a common naming practice for describing software vulnerabilities and including security tools and services as well as on the fixed sites of commercial and open source software package providers. We argue that dependencies exist between scanning phases and information holes from CVE vulnerability databases. This has consequences for access.

Additionally, work by [13, 15, 20] describes the benefits of CVE compatibility, integrating vulnerability services and tools allowing more complete security provision and more alert advisory services. Every month CVE MITRE receives between 150 and 300 new announcement alert and advisory submissions from ISS, Security Focus, Neohapsis, and the National Infrastructure Protection Centre. Currently CVE identifies compatible enablement data exchange between security products and provides a baseline for evaluating coverage of tools and services. There are thousands of information vulnerabilities within the CVE database. Unfortunately, time is required to make a patch release after exploitation has been found. Consequently, there is usually a a time delay between an exploitation identification and a patch and signature release. It can be argued that there are dependencies in the results between the scanning stages [15] and information vulnerabilities in the CVE database. This means that the vulnerability could be a security flaw exploitable by attackers.

In this experiment followed four dominant categories of attack: Probes, Remote to Local (R2L), User to Root (U2R) and DoS as widely used in the field of intrusion detection/prevention system, with reference to [3, 4, 8, 31].

3 Experiments

The dataset employed in this study was Intrusion Threat Detection Universiti Teknologi Malaysia (ITD UTM), as shown in Figure 1, available in [30]. All attacks were executed and infiltrated on ITD UTM. The network environment is set up for exploitation using Windows Server and two terminal clients running as attackers. They are connected to 3COM Superstack II 100 Mb/s, as shown in Figure 1.

3.1 Data Collecting and Procedures

Several steps must be taken to conduct these experiments. This work is an improvement on some of the advice offered by [22] and this research agrees with the argument expressed by [1], particularly on these problems: (i) recent trends and new methods of attack have been involved, (ii) control and guideline steps for penetration, and (iii) various methods of attack for penetration and mitigation become comprehensive. In this experiment, three weeks were spent collecting data and finding vulnerability within CVE and security communities. Moreover, five weeks was spent attempting penetration testing on the victim. There are some differences in the results obtained in the first and second data collection. The first data were collected directly from the server, regardless of the network broadcast. Conversely, the second data were collected using the hub terminal which also captured the broadcast network. Furthermore, this procedure was followed in this section:

1) To distinguish between normal traffic and attack, the attack was separated and divided into several stages based on time, machine target and method of attack.

2) Machine 10.10.10.1 is a NAT Firewall server that both allows and denies private traffic to and from the internet.

3) TCPdump is used to sniff real traffic. It uses the libcap library to capture packets and has the ability to consider the properties of an ideal as a packet sniffer. TCPdump produced raw data (pcap files) during experiments conducted via 10.10.10.30.

4) Machine 10.10.10.40 running on Snort IDS 2.8.5.2 (Build 121), PCRE ver 8.12. This is used to identify the threat as well as to compare attacks carried out which can be recognised by snort signature.

5) Two machine attackers, 10.10.10.15 (called Hacker XP) running on Windows XP SP3 and 10.10.10.20 based on Backtrack 4 (called Hacker BT) to penetrate Windows Server SP3 in 10.10.10.25.

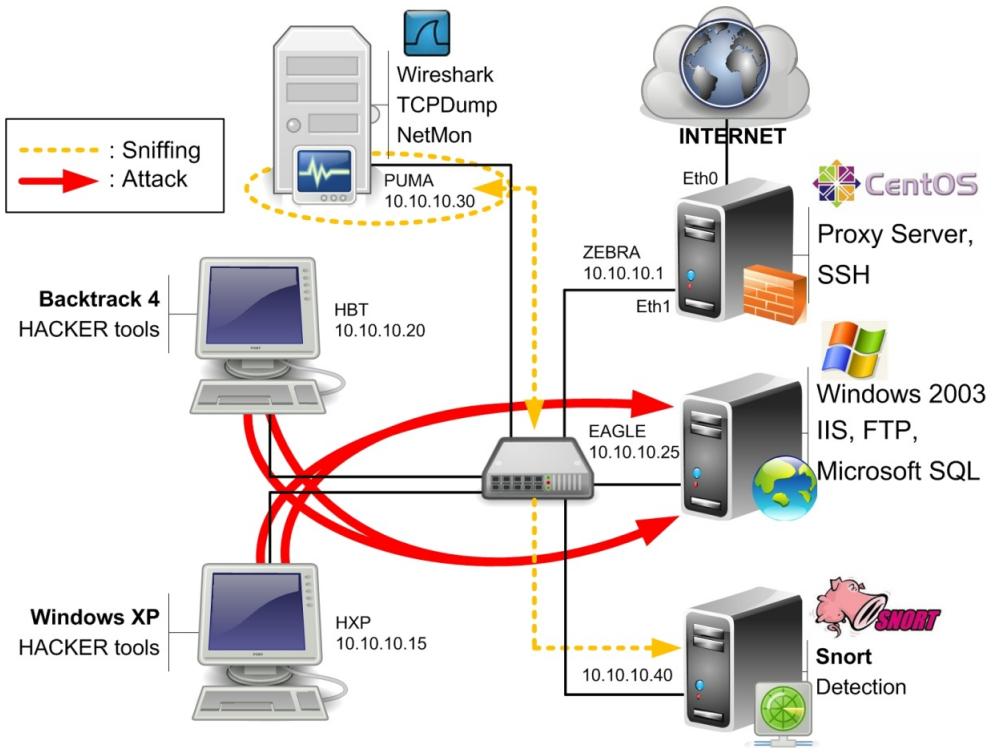


Figure 1: Topology of test bed environment

Meanwhile, in this experiment all attacks were executed on ITD UTM. The attack scenario for penetration is further illustrated below.

Step 1. Scanning

- Attackers probe the network 10.10.10.25 via GFI Scanning, Nessus, N-Stealth and Nmap;
- Attackers port reconnaissance of HTTP services via Nikto;
- Attackers find open port to potential penetration, 21 (FTP), 23 (Telnet), 80 (HTTP), 445 (SMB), 1433 (Microsoft SQL Server), 1026 (Remote Server).

Step 2. Brute Force

- Attackers attempt password of FTP & Telnet via brute-force tools;
- Attackers attempts to host 10.10.10.25 for guessing password remote access via TSgrinder;
- Attackers attempt SQL Ping and Brute force SQL Login;
- Attackers successfully find user authenticated of FTP;
- Nessus confirms user access "anonymous" enable and allowed in FTP;
- Attackers log in to the host via FTP Client.

Step 3. Gaining privileges

- Attackers try to escalate privilege to administrator level;
- Attackers attempt web attack via HTTP and launch "/.... access", "/ root access", "/etc/passwd", "/usr/bin/id", "/etc/shadow access" via HTTP port 80;
- Attackers attempts XSS attack - Attackers sniff the network via Cain Abel by utilising of ARP;
- Attackers launch man in the middle attack and SMB Unicode;
- Attackers add user "puma" password : 12345678 via console;
- Attackers add user "mike" password : 12345678 via console;
- Attackers add user "john" password : 12345678 via console;
- Attackers create directory /mkdir "tools" in 10.10.10.25 via console;
- Attackers crack root level hashing password via localhost;
- Attackers upload some files including Trojan to the victim via FTP;
- Attackers successfully implant the netbus to create backdoor via FTP;
- Attackers execute and enable netbus via remote desktop, then implant keylogger.

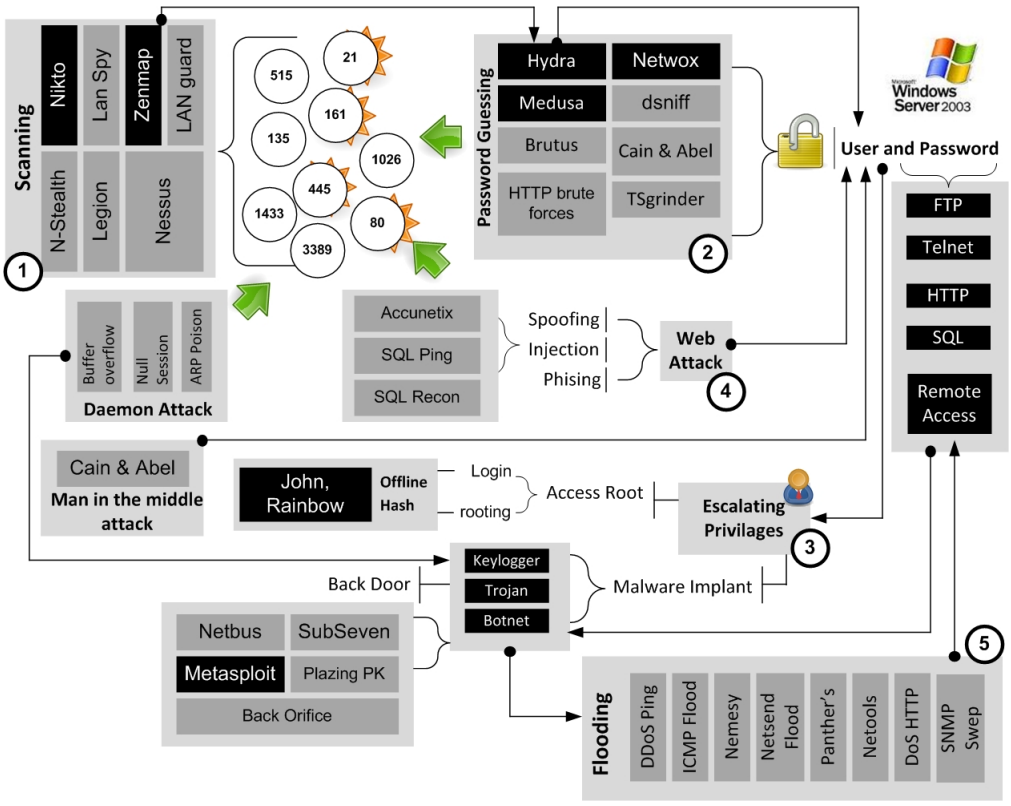


Figure 2: Attack scenario diagram

Step 4. DoS

- Hacker XP and Hacker BT send a large number of ICMP packets repeatedly to flood 10.10.10.25;
- Attackers launch attack LAND via sending TCP SYN;
- Attacker flood packets using forged source;
- Attackers flood traffic host victim via UDP to slow down the response of the target.

3.2 Scanning

An attacker's first steps need to obtain information about the victim and its environment. They map the network to determine the target, followed by scanning in order to interrogate and reconnoitre the victim. The attacker tries to map out the IP Address/subnet mask information and operating system that is in use, what services daemons are actively run and the kernel/services pack used. In other words, the attacker tries to map out the infrastructure and resources of the network.

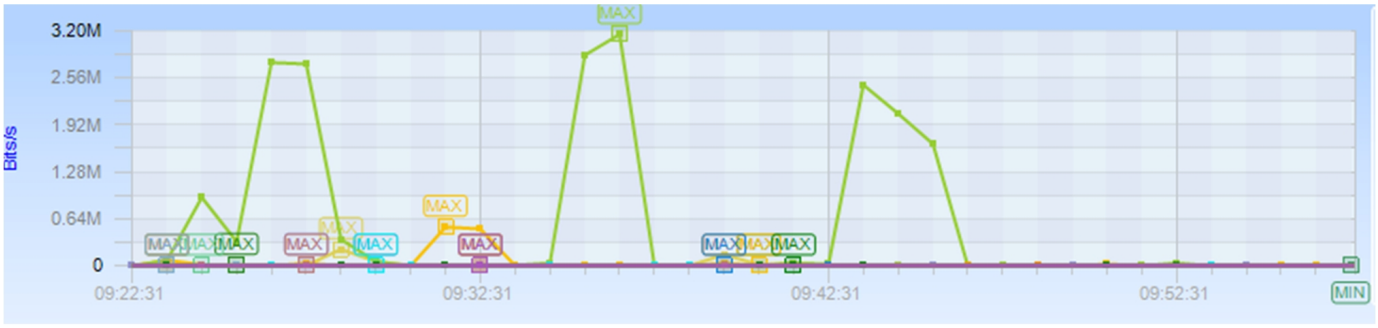
In this stage, several tools and scenarios are used to gather information, and findings known as vulnerabilities are mixed and combined to achieve the expected results. Some of the measures are adopted to enable these tools to complement each other. Moreover, none of these tools can provide all the detailed information. They have limitations particularly in translating the feedback packet from the target host. Some tools identify the open port and the rest are closed.

As mentioned in Section 3.1's attack scenario, some open ports were found and used to scan data coming from such ports. The success of this process depends on the operating system and the application that is run on the server. Some tools are used in Hacker BT running Zenmap, Xprobe2, Nikto, HTTPrint, and Hping2. Meanwhile, the Hacker XP machine runs these tools: GFiLAN, Legion, Nessus, N-Stealth, X-Scan, and LanSpy, which is a comprehensive target and a slow mode of scanning. This stage of attack depicted in Figure 2 produces visualisation, as shown in Figure 3(a) and (b) below.

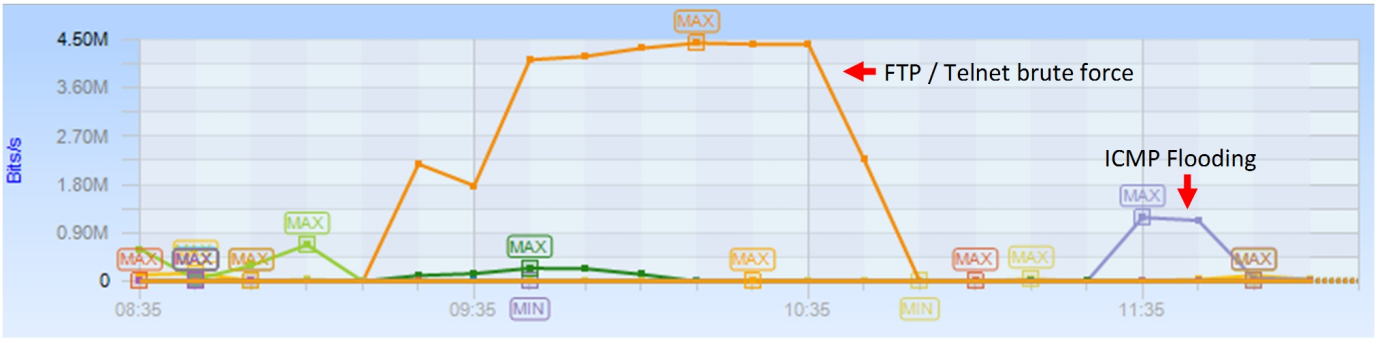
3.3 Vulnerability

This section presents vulnerabilities that arose during the scanning stages. From a hacker's perspective, searching for any kind information that can be exploited from the CVE database may identify vulnerabilities. It can be argued that there are dependencies between scanning and information holes within a CVE vulnerability database with respect to gaining access. The critical and medium risk vulnerabilities are as follows:

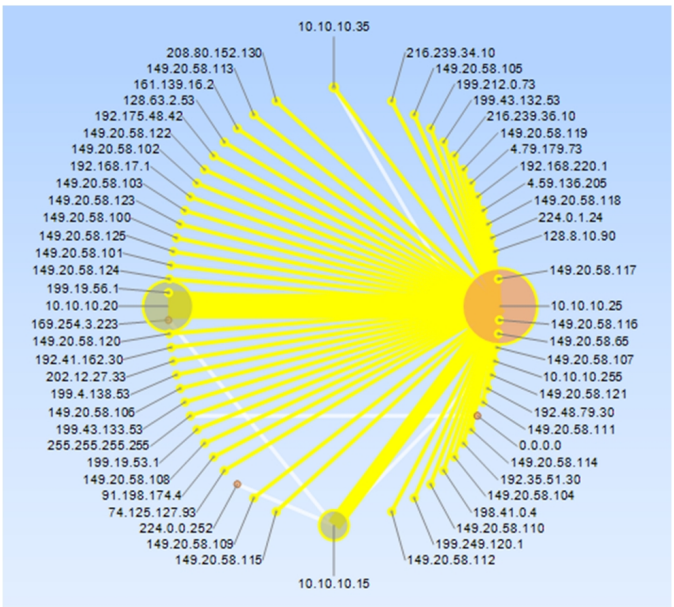
1) CVE-2011-1267, CVE-2011-1268, CVE-2011-0476 confirm SMB Server-Client to allow remote code ex-



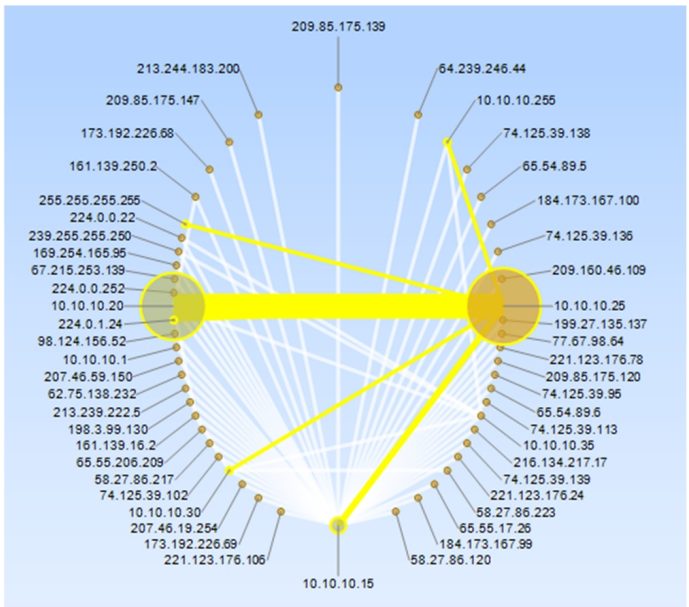
(a)



(b)



(c)



(d)

Figure 3: (a) Overall scanning traffic, (b) overall traffic of penetration stages. (c) refers to handshaking traffic attackers with victim in scanning stages and (d) shows penetration.

ecution if an attacker sends a specially crafted SMB response to a client-initiated SMB request.

2) CVE-2008-4250, RPC vulnerabilities allow remote code execution. An attacker could exploit this vulnerability without authentication to find arbitrary code & worm exploitations.

3) CVE-2006-5583 is vulnerable and can be exploited with regard to buffer overflow SNMP, allowing a remote attacker to execute arbitrary codes via a crafted SNMP packet via exec code overflow.

4) CVE-2006-3439 confirms vulnerability from buffer overflows. This attack allows remote attackers, including anonymous users to execute an arbitrary code via a crafted RPC message.

5) CVE-2006-0026 and CVE-2000-0071 is vulnerable to IIS. This attack can allow local and possibly remote attackers to execute arbitrary codes via crafted Active Server Pages (ASP) and allows a remote attacker to obtain the real pathname of a document.

6) CVE-2003-0352, CVE-2003-0003, Buffer overflow in a certain DCOM interface for RPC allows remote attackers to execute arbitrary codes via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms.

7) CVE-2011-1247, Path vulnerability from Microsoft active accessibility enables local users to gain privileges via a Trojan horse DLL in the current working directory.

8) CVE-2011-0654, Buffer overflow in Active Directory services. This attack allows remote attackers to execute arbitrary codes or cause a denial of service via a malformed BROWSER ELECTION message.

3.4 Penetration Testing

The stages identified certain holes to be exploited from previous stages and launched the attack, a so-called User-to-Root (U2R) attack. This extends the user's privilege to administrator/root to obtain full authorization access. The attacker can create the new user, implant the malware, create the backdoor and clean their track from the log server. Normally, the attacker starts with accessing a normal local user account then later exploits vulnerability to privileges. Moreover, the attackers also launched brute force for guessing the password, cracking the password, web injection and man in the middle attack.

This step is called the Remote-to-Local (R2L) attack. Request packets were sent to a machine over a network which then exploits machine's vulnerability to illegally gain local access as a user without privileges. In this stage, the attacker focused on brute force in order to gain access and escalate privileges. According to the scenario presented in Section 3.1 and Figure 2 above, attackers discovered multiple vulnerabilities. They successfully found the legitimate users then created a new user, and successfully used a brute force FTP log-in resulting in the malware to successfully create a backdoor. Figure 2 shows illustrated penetration of Windows, as follows:

1) Hacker BT and Hacker XP attempted to conduct surveillance whereby the attacker tries to map out of IP Address/subnet mask information, operating system being used, and which services are running in 10.10.10.25. In other words, these stages are called probes or scanning to map out and reconnoitre the victim's network infrastructure. Nessus, Nmap, Nstealth, Legion and GFILanGuard are used to communicate with the data base server several times to check available updates of existing vulnerabilities. There are some potential vulnerabilities to be exploited which are as follows:

PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
111/tcp	open	rpcbind
161/udp	open	snmp
445/tcp	open	microsoft-ds
1027/tcp	open	IIS
1433/tcp	open	ms-sql-s

2) Specific techniques are used to escalate privilege, attempt password one by one via guessing, theft, sniffing and cracking the password direct to target. From the attacker's perspective, the challenge is to find the legitimate user and implant the Trojan to create a backdoor. The attackers must prepare a dictionary/word list, accuracy in selecting the dictionary is a must and cracking the password in time depends on the length of the password's characters. Otherwise, a brute force password via user "administrator" can be successfully performed of FTP by Hydra and failed attempt Telnet.

```
root@bt:~# hydra -l administrator -P
passdict.txt 10.10.10.25 ftp
[DATA] 16 tasks, 1 servers, 26870 login tries
(l:1/p:26870), ~1679 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 10.10.10.25   login:
administrator   password: intrusion
```

Moreover, the attacker launched TSgrinder to guess the password of the remote desktop. This failed and the dsniff was launched to the sniff user and password in broadcast network. HTTP brute force was used to guess the web directory. Meanwhile, the traffic attempt of brute force is dominant, as shown in Figure 3(a).

3) The attacker launched powerful tools such as Metasploit, Cain and Abel and Netcat to find the command prompt. They attempted to obtain privileges and attack launches via the command prompt, which freely creates a new user account and removes the traces. In this step, after obtaining a valid user, the attackers attempted to implant a Trojan to create the backdoor. They successfully implanted the Netbus Trojan and executed the "Abel" in an ARP poison attack. New users "puma", "mike" and "john" were created before the attackers attempted to crack the administrator password via John the Ripper and Rainbow.The attacker attempted an IIS attack via buffer overflow and SQL injection to break into a system. During that time, they tried to find the weaknesses and structure of the website via SQL injection in order to ascertain certain information and the error page from HTTP server.

4) Finally, to reduce availability the attackers continuously launched DoS attacks by flooding the ICMP and UDP. They were successful; the system could not respond and crashed after a few minutes. Repeated requests meant that the target was unable to handle the service and reduce the availability. The results of this scenario are shown in Figure 3(b) below.

4 Experiment Results and Discussion

Snort is used to identify and recognize threats from data traffic. It produces lots of logs contained in machine 10.10.10.30 "var/log/snort" directory. The scanning stages produces 677,914 packets and snort identified 45,139 alerts among them as threats. Meanwhile, in the penetration stage there were 33,865,687 packets and 265,200 were identified by the existing signature as a threat.

4.1 Attack Pattern

This section presented some sample attack patterns (Probe, U2R, R2L and DoS) from the experiment. Every alert was compiled via snort and pcap files. In this case, the pcap file was extracted and revealed some features such as: time stamp, source IP Address, destination IP Address, Protocol, size of protocol, Flag of Protocol, Total Length of packet and content of packet.

From observations that were made, specific characteristics of line to line attacks from can be recognised from the header and payload of packets. They have a unique pattern which tends to iterate in a particular line. Some characteristics of pattern are as follows:

1) Web scanning, especially HTTP and HTTPS reconnaissance, has the following characteristics: (i) each packet has a source and destination IP address and port numbers are spoofed, (ii) connections are said to be state and number of ports accessed by a single source, (iii) TCP flags are used randomly during the attack, (iv) packet size and packet length are changed frequently.

2) Netbus have these characteristics: (i) computer victims or servers typically listen on specific ports waiting for instructions from attackers, (ii) they use TCP protocol and port address 12345 to communicate and each message has a fixed-length header, (iii) the variable-sized data section follows the header and its size is specified in the message-size field of the header, (iv) the flag is fixed to the computer victim during the communication process.

3) Brute force of FTP: (i) this attack generates repetition response, particularly content of flags and protocol length, (ii) anonymous user login attempts will occur, (iii) the port address and flags are fixed during attack, (iii) data connection uses the well-know port 20 at the server side and control connection is established on port 21.

4) Scenario of NetBIOS NULL session attack tries to attack enumeration user and getting administrator level, it have characteristic: (i) Packet size, total length and flags fixed with randomly generated on Port 139 (NetBIOS Session Service) and Port 445 (Common Internet File System), (ii) The flag value is fixed and dominate by NetBIOS protocol session, (iii) Vulnerability in Port 445 is possible to launched SMB or Common Internet File System (CIFS) attack, (iv) The TCP protocol are fixed during attack attempt, NetBios Session Services (NBSS) port 135, Remote Procedure Call (RPC) port 137, NetBIOS Name Service port 138 and NetBIOS Datagram Service port 139.

5) The characteristics of man in the middle attacks are: (i) the ARP packet lack flag and protocol length value, (ii) the ARP broadcasts from the attacker to all IP addresses in one subnetmask and without information of port source and destination, (iii) NetBIOS datagram fixed used port 138 and NetBIOS Name Service port 137.

Meanwhile, the number of rows that were generated by snort due to repetition of the same information were observed. This can be simplified by initialising the signature-id and priority. Each alert comprises of signature-id, priority, source of IP Address, source port, destination of IP Address, destination of port address, timestamp, Time To Live, Type of Service, IP Length and Datagram length.

4.2 Identify of Probe

In this phase, snort confirms that there are 4078 lines identified as "SCAN FIN" as shown in Figure 4 below and Table 1 shows the total attempts at probe attacks.

[**] [1:621:7] SCAN FIN [**]
[Classification: Attempted Information Leak]
[Priority: 2] 11/15-14:34:47.694055 10.10.10.20:3777 -> 10.10.10.25:0TCP
TTL:64 TOS:0x0 ID:55275 IpLen:20 DgmLen:40
*******F Seq: 0x26B3BDE5 Ack: 0x7895D1C4 Win: 0x200 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS27]

No	Timestamp	SRC_IP	DST_IP	SRC_port	DST_port	Protocol	Size	Flag	Total_Len	Content
535623	34:47.5	10.10.10.20	10.10.10.25	4022	0	TCP	60	R	40	P…P……
535735	34:47.7	10.10.10.20	10.10.10.25	3777	0	TCP	60	F	40	x…p…G……
535737	34:47.7	10.10.10.25	10.10.10.20	0	3777	TCP	60	A.R	40	&…P…5……

Figure 4: Probe stages

[**] [1:1497:6] WEB-MISC cross site scripting attempt [**]
[Classification: Web Application Attack] [Priority: 1]
08/07-02:32:58.279106 10.10.10.15:4579 -> 10.10.10.25:80
TCP TTL:128 TOS:0x0 ID:56110 IpLen:20 DgmLen:467 DF
AP Seq: 0xDAEC1AA2 Ack: 0x1102B98D Win: 0xFFFF TcpLen: 20

No.	Timestamp	Src_IP	Dst_IP	Src_Port	Dst_Port	Protocol	Size	Flags	Length	Summary
14723	32:58.3	10.10.10.15	10.10.10.25	4579	80	HTTP	481	AP	467	C: GET /citrix/nfuse/default/login.asp?NFuse_LogoutId= &NFuse_MessageType=Error&NFuse_Message= <SCRIPT>alert('Ritchie') </SCRIPT>&ClientDetection=ON HTTP/1.1
14724	32:58.3	10.10.10.15	10.10.10.25	4577	80	HTTP	54	A.R	40	Seq=0428859739,Ack=2717741707,F=.A.R..,Len= 0,Win= 0
14725	32:58.3	10.10.10.25	10.10.10.15	80	4579	HTTP	1,514	A	1500	S: HTTP/1.1 404 Not Found
14726	32:58.3	10.10.10.25	10.10.10.15	80	4579	HTTP	389	AP	375	S: Continuation of existing HTTP stream, 335 bytes text data
14732	32:58.3	10.10.10.15	10.10.10.25	4580	80	HTTP	400	AP	386	C: GET /devdescr.xml HTTP/1.1
14733	32:58.3	10.10.10.25	10.10.10.15	80	4580	HTTP	1,514	A	1500	S: HTTP/1.1 404 Not Found
14734	32:58.3	10.10.10.25	10.10.10.15	80	4580	HTTP	408	AP.F	394	S: Continuation of existing HTTP stream, 354 bytes text data
14735	32:58.3	10.10.10.15	10.10.10.25	4580	80	HTTP	54	A	40	Seq=3941520320,Ack=0432962896,F=.A....,Len= 0,Win=65535
14736	32:58.3	10.10.10.15	10.10.10.25	4579	80	HTTP	487	AP	473	C: GET /citrix/MetaframeXP/default/login.asp? NFuse_LogoutId= &NFuse_MessageType=Error&NFuse_Message= <SCRIPT>alert('Ritchie')</SCRIPT>& ClientDetection=ON HTTP/1.1
14737	32:58.3	10.10.10.15	10.10.10.25	4580	80	HTTP	54	A.R	40	Seq=3941520320,Ack=0432962896,F=.A.R..,Len= 0,Win= 0
14738	32:58.3	10.10.10.15	10.10.10.25	4581	80	HTTP	62	S	48	Seq=1832059795,Ack=0000000000,F=....S.,Len= 0,Win=65535
14739	32:58.3	10.10.10.25	10.10.10.15	80	4579	HTTP	1,514	A	1500	S: HTTP/1.1 404 Not Found

Figure 5: Root to Local (R2L)

Table 1: The Number of Alert from Scanning stages

No	Detected Alert	Priority	Total
1	SCAN FIN	2	4078
2	NETBIOS SMB repeated logon failure	1	453
3	WEBROOT DIRECTORY TRAVERSAL	3	433
4	WEB-MISC http directory traversal	2	142
5	NETBIOS SMB repeated logon failure	1	101
6	NETBIOS SMB-DS repeated logon failure	1	74
7	(portscan) TCP Portscan	2	49
8	ICMP Timestamp Reply	1	31
9	SQL ping attempt	3	17
10	ICMP Information Request	3	15
11	SCAN nmap XMAS	2	10
12	ICMP webtrends scanner	2	9
13	RPC portmap listing TCP 111	2	6
14	SCAN Amanda client version request	2	4
15	ICMP superscan echo	2	4
16	NETBIOS SMB-DS ADMIN$ unicode share access	3	4
17	NETBIOS SMB-DS D$ unicode share access	3	2
18	(portscan) TCP Portsweep	3	2
19	NETBIOS SMB-DS C$ share access	3	1
20	NETBIOS SMB-DS ADMIN$ share access	3	1

4.3 Identify R2L

Figure 5 shows one of the attacks as described in the 2nd scenario above. This attack focuses on obtaining privileges for the system. The attacker launched several methods to attempt to find the passwords for FTP and Telnet. Moreover, Figure 3(b) demonstrates that traffic of brute force becomes very dominant. Meanwhile, Table 2 shows the number of alerts from this attack. The attackers tried repeatedly to guess the password by using the default user.

4.4 Identify U2R

The attackers just focused on how to gain escalating privileges via level "administrator/root". They succeeded in creating some new users with administrator level, implanting the malware and finding the backdoor. Figure 6 shows a sample from this attack and how the attackers got into the system via an "anonymous" user, then attempts privileges infiltration via change working directory (CWD) of FTP. Table 3 shows the number of alerts from this attack.

4.5 Identify DoS

Flooding to Denial of Services (DoS) is the final scenario. Within hours the attackers attempted to disrupt the normal functioning to affect the availability of the target and succeeded. The system response delay value rose slightly as compared to before the attack. The result was system failures and crashes shows in Figure 7. Table 4 shows the number of alerts from this attack.

4.6 Network Traffic Visualisation

This section presented the overall network traffic from scanning and penetration stages shown in Figure 3 below. Item (a) depicts the overall traffic of HTTP from scanning stages and item (b) shows the dominant traffic from brute force attacks. Pecentage of SSH/Telnet is allocated 84.96% and ICMP allocated 6.41% from total overall traffic.

This attack focused on achieving access and escalating privileges, especially penetration via brute force to FTP and Telnet. Point (c) in Figure 3 shows some scanning tools from attackers to victim and some of the tools with open connections to the internet. We also see here whether there are any updates of existing vulnerabilities in their database. Meanwhile, item (d) is handshaking traffic attackers and victims in penetration stages; the mark indicates that the attacker launched a comprehensive attack. Items (c) and (d) highlight greater traffic flows from 10.10.10.20 and 10.10.10.15 to victim.

5 Conclusions and Future Works

We believe that penetration testing is vital in the search for all kinds of vulnerabilities and for evaluating overall systems. However, the small amount of vulnerability information obtained should be of particular concern. This paper presents the vulnerabilities of Windows Server.

Table 2: The Number of Alert from R2L stages

No	Detected Alert	Priority	Total
1	INFO FTP Bad login	2	67625
2	WEB-PHP remote include path	1	2709
3	WEB-MISC cross site scripting attempt	1	1380
4	COMMUNITY WEB-PHP XSS attempt	1	596
5	COMMUNITY WEB-PHP XSS attempt	1	510
6	NETBIOS SMB repeated logon failure	1	453
7	NETBIOS SMB-DS repeated logon failure	1	106
8	WEB-MISC Tomcat servlet mapping cross site scripting attempt	1	19
9	(ftp_telnet) Invalid FTP Command	3	18
10	WEB-CGI perl command attempt	2	13
11	FTP CWD ãttempt	2	2

Table 3: The Number of Alert from U2R stages

No	Detected Alert	Priority	Total
1	WEB-MISC /etc/passwd 2	1876	
2	NETBIOS SMB repeated logon failure	1	1161
3	ATTACK-RESPONSES Invalid URL	2	150
4	BACKDOOR netbus active	1	36
5	WEB-IIS CodeRed v2 root.exe access	1	19
6	BACKDOOR sensepost.exe command shell attempt	2	16
7	DOUBLE DECODING ATTACK	1	14
8	WEB-ATTACKS /etc/shadow access	2	12
9	BACKDOOR c99shell.php command request	1	4
10	WEB-MISC bad HTTP/1.1 request, Potentially worm attack	2	3
11	BACKDOOR netbus getinfo	1	1
12	FTP CWD ...	1	1
13	FTP CWD Root directory transversal attempt	3	1

Table 4: The Number of Alert from DoS stages

No	Detected Alert	Priority	Total
1	BAD-TRAFFIC tcp port 0 traffic	3	12548
2	ICMP PING Windows	3	8334
3	ICMP PING	3	6300
4	ICMP Echo Reply	3	2125
5	ICMP Destination Unreachable Port Unreachable	3	2082
6	(snort decoder) Bad Traffic Loopback IP	3	1332
7	(snort decoder) Bad Traffic Same Src/Dst IP	3	678
8	ATTACK-RESPONSES Invalid URL	2	150
9	SNMP trap udp	2	30
10	NETBIOS SMB Trans Max Param/Count DOS attempt	3	12
11	DDOS Stacheldraht client check gag	2	7
12	COMMUNITY WEB-MISC Hasbani-WindWeb GET DoS attempt	2	4
13	DDOS mstream client to handler	2	2
14	NETBIOS SMB-DS Trans unicode Max Param DOS attempt	3	1

[**] [1:1229:7] FTP CWD ... [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
08/07-02:33:30.183629 10.10.10.15:5241 -> 10.10.10.25:21
TCP TTL:128 TOS:0x0 ID:60987 IpLen:20 DgmLen:94 DF
AP Seq: 0xA0670E4B Ack: 0x38AD9A35 Win: 0xFF4E TcpLen: 20
[Xref => http://www.securityfocus.com/bid/9237]

No	Timestamp	SRC_IP	DST_IP	SRC_port	DST_port	Protocol	Size	Flag	Total_Len	Content
24186	33:30.0	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	70	AP	56	220 FTP SERVER
24187	33:30.0	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	70	AP	56	USER anonymous
24188	33:30.0	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	126	AP	112	331 Anonymous access allowed, send identity (e-mail name) as password.
24189	33:30.0	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	78	AP	64	PASS nessus@nessus.org
24190	33:30.0	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	85	AP	71	230-WELCOM TO FTP SERVER 2003
24191	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	54	A	40	
24192	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	85	AP	71	230 Anonymous user logged in.
24193	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	108	AP	94	CWD .../.../.../.../.../.../.../.../.../.../.../.../
24194	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	83	AP	69	250 CWD command successful.
24195	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	60	AP	46	PASV
24196	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	101	AP	87	227 Entering Passive Mode (10,10,10,25,18,4).
24197	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	62	S	48	
24198	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	62	A.S	48	
24199	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	54	A	40	
24200	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	69	AP	55	RETR boot.ini
24201	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	113	AP	99	550 boot.ini: The system cannot find the file specified.
24202	33:30.2	10.10.10.25	10.10.10.15	21	5241	FTP Ctrl	54	A.R	40	
24203	33:30.2	10.10.10.15	10.10.10.25	5241	21	FTP Ctrl	60	AP	46	QUIT

Figure 6: User to Root (U2R)

[**] [1:402:8] ICMP Destination Unreachable Port Unreachable [**]
[Classification: Misc activity] [Priority: 3]
11/16-12:04:44.947792 10.10.10.15 -> 10.10.10.25
ICMP TTL:128 TOS:0x0 ID:20401 IpLen:20 DgmLen:83
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP: 10.10.10.25:7 -> 10.10.10.15:59130
UDP TTL:128 TOS:0x0 ID:28414 IpLen:20 DgmLen:55 Len: 27 Csum: 17179 (27 more bytes of original packet)
** END OF DUMP
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-0068] [=> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0790]

No	Timestamp	SRC_IP	DST_IP	SRC_port	DST_port	Protocol	Size	Flag	Total_Len	Summary
33763346	12:04:44.944406	10.10.10.25	10.10.10.15	-	-	ICMP	190	-	176	Destination Port Unreachable
33763355	12:04:44.947278	10.10.10.25	10.10.10.15	-	-	ICMP	97	-	83	Destination Port Unreachable
33763356	12:04:44.947282	10.10.10.25	10.10.10.15	-	-	ICMP	97	-	83	Destination Port Unreachable
33763360	12:04:44.947792	10.10.10.15	10.10.10.25	-	-	ICMP	97	-	83	Destination Port Unreachable
33763361	12:04:44.947798	10.10.10.25	10.10.10.15	-	-	ICMP	97	-	83	Destination Port Unreachable
33763362	12:04:44.948045	10.10.10.25	10.10.10.15	-	-	ICMP	97	-	83	Destination Port Unreachable
33763363	12:04:44.948050	10.10.10.25	10.10.10.15	-	-	ICMP	97	-	83	Destination Port Unreachable
33763370	12:04:44.955090	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763371	12:04:44.955095	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763372	12:04:44.955099	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763373	12:04:44.955311	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763374	12:04:44.955316	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763375	12:04:44.955319	10.10.10.25	10.10.10.15	-	-	ICMP	83	-	69	Destination Port Unreachable
33763392	12:04:45.053473	10.10.10.25	10.10.10.15	-	-	ICMP	190	-	176	Destination Port Unreachable
33763414	12:04:45.104769	10.10.10.25	10.10.10.15	-	-	ICMP	82	-	68	Destination Port Unreachable

Figure 7: Denial of services (DoS)

This server presents many open invitations for attackers to exploit as can be gathered from all the experiments conducted: implanting malware, password guessing, rooting, web injection, creating a backdoor and DoS. It can be concluded that the OS is vulnerable and open to exploitation, and thus requires more effort to be secured. Our conclusions are as follows: (i) there are relationships resulting from the scanning and information from the CVE vulnerability database, (ii) update policy and management of authentication for user, (iii) it is important that security operators assume that they will be hacked and should better secure themselves for that reason.

Meanwhile, what this experiment indicates is that there a large number of new attacks that could remain hidden in the data and would not be identified using existing Snort signature. Snort cannot be used as a security platform to protect against threats; it cannot be expected to detect all threats and trigger the necessary response. However, Snort is adept at protocol analysis, content matching, and packet logging. Therefore, some future work must be conducted such as: (i) how to extract the data to analysed, (ii) how to classify the threat and normal access, and (iii) how to visualise alert to show details of taxonomy information from Snort.

References

[1] N. Athanasiades, R. Abler, J. Levine, H. Owen, and G. Riley, "Intrusion detection testing and benchmarking methodologies," in *First IEEE International Workshop on Information Assurance (IWIA'03)*, pp. 63–72, 2003.

[2] N. Barrett, "Penetration testing and social engineering: Hacking the weakest link," *Information Security Technical Report*, vol. 8, pp. 56–64, 2003.

[3] R. Beghdad, "Critical study of neural networks in detecting intrusions," *Computers & Security*, vol. 27, pp. 168–175, 2008.

[4] R. Beghdad, "Efficient deterministic method for detecting new U2R attacks," *Computer Communications*, vol. 32, pp. 1104–1110, 2009.

[5] D. Bradbury, "Hands-on with metasploit express," *Network Security*, vol. 2010, pp. 7–11, 2010.

[6] V. Broucek and P. Turner, "Technical, legal and ethical dilemmas: Distinguishing risks arising from malware and cyber-attack tools in the 'cloud'-a forensic computing perspective," *Journal of Computer Virology and Hacking Techniques*, vol. 9, pp. 27–33, 2013.

[7] R. Bruen, "Intrusion detection systems: Problems and opportunities," *Software Focus*, vol. 2, pp. 151–156, 2001.

[8] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *Computers & Security*, vol. 24, pp. 295–307, 2005.

[9] B. Clive, "Hacking: An abuse of privilege," *Computer Audit Update*, vol. 1990, no. 1, pp. 21–24, 1989.

[10] E. Conrad, S. Misenar, and J. Feldman, *Domain 2: Access Control (Chap. 3)*, CISSP Study Guide, pp. 37–89, 2010.

[11] J. Conrad, "Seeking help: The important role of ethical hackers," *Network Security*, vol. 2012, pp. 5–8, 2012.

[12] S. David, "The state of network security," *Network Security*, vol. 2012, pp. 14–20, 2012.

[13] H. Gascon, A. Orfila, and J. Blasco, "Analysis of update delays in signature-based network intrusion detection systems," *Computers & Security*, vol. 30, no. 8, pp. 613-624, 2011.

[14] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, pp. 31–43, 2005.

[15] H. Holm, "Performance of automated network vulnerability scanning at remediating security issues," *Computers & Security*, vol. 31, no. 2, pp. 164–175, 2012.

[16] J. Hua and S. Bapna, "The economic impact of cyber terrorism," *The Journal of Strategic Information Systems*, vol. 22, no. 3, pp. 175–186, 2013.

[17] G. Kenneth, "Cyber Weapons Convention," *Computer Law & Security Review*, vol. 26, pp. 547–551, 2010.

[18] S. Mansfield-Devine, "DDoS: Threats and mitigation," *Network Security*, vol. 2011, pp. 5–12, 2011.

[19] N. Martin and J. Rice, "Cybercrime: Understanding and addressing the concerns of stakeholders," *Computers & Security*, vol. 30, pp. 803–814, 2011.

[20] R. A. Martin, "Managing vulnerabilities in networked systems," *IEEE Computer*, vol. 34, no. 11, pp. 32–38, 2001.

[21] K. K. M. D. Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*, Elsevier Inc, pp. 1-64, 2007.

[22] P. Mell, V. Hu, R. Lippmann, J. Haines, and M. Zissman, *An Overview of Issues in Testing Intrusion Detection Systems*, Technical Report NISTIR 7007, July 11, 2003.

[23] D. E. Neghina and E. Scarlat, "Managing information technology security in the context of cyber crime trends," *International Journal of Computers Communications & Control*, vol. 8, pp. 97–104, 2013.

[24] C. P. Pfleeger, S. L. Pfleeger, and M. F. Theofanos, "A methodology for penetration testing," *Computers & Security*, vol. 8, pp. 613–620, 1989.

[25] R. J. Potts, "Hacking: The threats," *Computer Audit Update*, vol. 1990, no. 1, pp. 14–15, 1989.

[26] E. Schultz, "RPC in Windows systems: What you don't know could hurt you," *Network Security*, vol. 2004, pp. 5–8, 2004.

[27] E. Schultz, "Windows 2000 security A postmortem analysis," *Network Security*, vol. 2004, pp. 6–9, 2004.

[28] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security*, vol. 31, pp. 357–374, 2012.

[29] M. D. Steve, "Hacktivism: Assessing the damage," *Network Security*, vol. 2011, pp. 5–13, 2011.
[30] D. Stiawan, M. Y. Idris, and A. H. Abdullah, "Penetration testing and network auditing: Linux " *Journal of Information Processing Systems*, vol. 11, pp. 104–115, 2015.
[31] G. C. Tjhai, M. Papadaki, S. M. Furnell, and N. L. Clarke, "The problem of false alarms: Evaluation with snort and DARPA 1999 dataset," in *Trust, Privacy and Security in Digital Business*, LNCS 5185, pp. 139-150, Springer, 2008.
[32] S. W. Woo, H. Joh, O. H. Alhazmi, and Y. K. Malaiya, "Modeling vulnerability discovery process in Apache and IIS HTTP servers," *Computers & Security*, vol. 30, pp. 50–62, 2011.

Deris Stiawan (SCOPUS ID: 36449642900), received his Ph.D degree in Computer Science from Universiti Teknologi Malaysia in 2013. Currently he is an senior lecturer in Faculty of Computer Science, University of Sriwijaya, Indonesia. In 2011, He holds Certified Ethical Hacker (C—EH) & Certified Hacker Forensic Investigator (C—HFI) licensed from EC-Council. His research interests concern network & information security fields, focused on network attack and intrusion prevention/detection system.

Mohd Yazid Idris (SCOPUS ID: 36448800600), is a senior lecturer at of Computing, Universiti Teknologi Malaysia. He obtained his M.Sc and Ph.D in the area of Software Engineering, and Information Technology (IT) Security in 1998 and 2008 respectively. In software engineering, he focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of Intrusion Prevention and Detection (ITD). He is currently active in various academic activities and involves in university-industry link initiative in both areas.

Abdul Hanan Abdullah (SCOPUS ID: 11338934800), received his B.Sc. and M.Sc from University of San Francisco, California, and Ph.D from Aston University, Birmingham, United Kingdom. He is a Senior Professor at Faculty of Computing, Universiti Teknologi Malaysia (UTM). Currently, he is the Head of Pervasive Computing Research Group. His research areas of interest include Pervasive Computing, Network Security, Cloud and Grid Computing.

Mohammed AlQurashi received B.Sc. in Computer from King Abdul Aziz University, Saudi Arabia in 2009, and M.Sc. in Computer Science from University of Texas at San Antonio, USA, in 2013. Currently, he is a lecturer and researcher at Smart Network Research Group, at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include, Information Security, Cloud computing, and Network Security.

Rahmat Budiarto (SCOPUS ID: 6603477220) received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng, and Dr.Eng in Computer Science from Nagoya Institute of Technology in 1995 and 1998, respectively. He is currently a professor and the head of Smart Networked Research Group at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include IPv6, network security, Wireless sensor networks and MANETs.

A New Intrusion Detection System Based on Soft Computing Techniques Using Neuro-Fuzzy Classifier for Packet Dropping Attack in MANETs

Alka Chaudhary[1], V. N. Tiwari[2], and Anil Kumar[1]
(Corresponding author: Alka Chaudhary)

Department of Computer Science and Engineering, Manipal University[1]
Department of Electronics and Communication Engineering, Manipal University[2]
Jaipur 303007, India
(Email: alkachaudhary0207@gmail.com)
(Received Mar. 6, 2014; revised and accepted Sept. 16 & Dec. 22, 2014)

Abstract

Due to the advancement in communication technologies, mobile ad hoc networks are very attractive in terms of communication because mobile nodes can communicate without the relay on predefined infrastructure. Therefore, some complex properties of mobile ad hoc networks make it more vulnerable to internal and external attacks. From the security perspective, prevention based methods such as encryption and authentication are not considerably good solution for mobile ad hoc networks to eliminate the attacks so that intrusion detection systems are applied as a keystone in these types of networks. The main objective of intrusion detection system is to categories the normal and suspicious activities in the network. This paper proposed a novel intrusion detection system based on soft computing techniques for mobile ad hoc networks. The proposed system is based on neuro-fuzzy classifier in binary form to detect, one of vey possible attack, i.e. packet dropping attack in mobile ad hoc networks. Qualnet Simulator 6.1 and MatLab toolbox are used to visualize the proposed scenarios and evaluate the performance of proposed approach in mobile ad hoc networks. Simulation results show that the proposed soft computing based approach efficiently detect the packet dropping attack with high true positive rate and low false positive rate.

Keywords: Fuzzy inference system (FIS), IDS, MANET, neuro-fuzzy, packet dropping attack soft computing

1 Introduction

Mobile ad hoc networks (MANETs) are very prominent research area for researchers because MANETs have more vulnerabilities than the conventional networks. MANETs nodes can able to form the network without rely on predefined infrastructure or fixed infrastructure. Due to this nature of MANET, it is widely employed in many applications, E.g. military areas, disaster relief management virtual conferences, neighborhood area networks and likewise many others promising fields. MANETs are very prone to intrusions or attacks than the wired networks because of lack of clear line of defense, wireless links, no centralized points and dynamic topologies [9]. This paper focused on a very particular attack, i.e. packet dropping attack based on ad hoc on-demand distance vector (AODV) routing protocol [4]. In terms of security, prevention based techniques are not enough for MANETs security so that intrusion detection system (IDS) is used as a second line of defense for these networks.

When any set of actions make an effort to compromise with the security properties such as confidentiality, integrity, availability of resources and repudiation then these actions are called intrusions and detection of such intrusions are known as intrusion detection system. The primary objective of IDS is to categories the normal and suspicious activities in the network [26].

The basic functionality of IDS depends on three main components such as data collection, detection and response. The data collection component is responsible for collecting the data from various sources such as system audit data, network traffic data, etc. Detection module is responsible for analyzing the collected data to detect the intrusions, and if any suspicious activity detected than initiates the response by the response module.

There are three detection methods presented in the literature such as misuse based, anomaly based and specification based techniques [2, 3, 18]. The first method, misuse based detection systems detect the intrusions on the behalf of predefined attack signature. Second, anomaly-

based detection technique detects the intrusion on bases of normal behavior of the system. Defining the normal behavior of the system is a very challenging task because behavior of system can be changed time to time. This technique can detect the unknown or new attacks but with high false positive rates. The third technique is specification - based intrusion detection. This technique specified or defined the set of constraints on a specific protocol and then detects the intrusions at the run time violation of these specifications. Therefore, defining the specification is very time consuming job in this technique.

Normally there are three basic types of IDS architecture in literature: Stand-alone or local intrusion detection systems, Distributed and Cooperative intrusion detection systems, Hierarchical Intrusion Detection Systems [18]. This paper emphasized the local intrusion detection system (L-IDS) and distributed and cooperative intrusion detection system (DC-IDS) based on neuro-fuzzy classifier for detection of packet dropping attack in MANETs that are discussed in Section 5.

There are many IDSs have been developed for wired networks but these IDSs could not be employed on MANETs because of its complex characteristics. Accordingly, researchers have been designed new IDSs for MANETs domain [18]. However, this paper enforces the use of soft computing methods in MANETs.

Soft computing is viewed as an emerging method for computing which present the notable potentiality of human mind to understand and learn in the situation of imprecision and uncertainty [25]. Generally, soft computing admits three main components such as neural networks, fuzzy logic and genetic algorithms.

Many of the soft computing techniques have proved their applicability in the field of intrusion detection in wired networks. Recently, many of the researchers are emphasizing on soft computing techniques for intrusion detection in MANETs so that some of the IDSs based on soft computing techniques have been developed for MANETs [5, 11, 12, 13, 17, 20, 21, 22, 23].

Consequently, mostly fuzzy systems construct their fuzzy rules on the bases of human expert knowledge so that these systems have lake adaptation. Moreover, several methods have been proposed for automatically formation of fuzzy rules in fuzzy systems, i.e. fuzzy-genetic and neuro-fuzzy [1, 14]. This paper develops a new intrusion detection system based on neuro-fuzzy classifier. The main contribution of this work is to build the classifier in binary form for separating the normal and abnormal activities in MANETs. For this aim, ANFIS is employed as a neuro-fuzzy classifier in the binary form and subtractive clustering is utilized for defining the initial fuzzy rules and membership functions.

The rest of the sections of this paper are organized as follows: Section 2 defines AODV (Ad Hoc on Demand Distance Vector) routing protocol and presented the target attack related to this research. Section 3 elaborates the fuzzy inference systems, neuro-fuzzy concepts and particularly, ANFIS (Adaptive Neuro-Fuzzy Inference System). This section also describes the subtractive clustering technique. Section 4 presents the data extraction on specific features by Qualnet simulator 6.1 in MANET environment for the implementation of proposed method. In Sections 5 and 6, explain the proposed system and evaluate the performance of proposed system in local and cooperative environment. Finally, conclude the paper in Section 7.

2 Aodv and Packet Dropping Attack

One of the widely used routing protocol in MANETs is ad hoc on demand distance vector (AODV) [15]. We have used AODV routing protocol in this research. One of very particular attack on MANETs is packet dropping attack that is considered in this research. The full description of attacks on MANETs is elaborated in [19]. Packet Dropping Attack: In a packet dropping attack, an attacker or malicious node(s) drop the data packets not destined for disturbing the services or operations of the network [19]. For achieving their objective, malicious or attacker node(s) required to be on a routing path or take a part of routing operations so that attacker nodes have a very small reason to drop the RREQ, RREP and RERR packets. We assumed in this research that the attacker nodes do not drop the RREQ, RREP and RERR packets of AODV routing protocol. Due to dropping data packets, network performance can reduced in terms to retransmit the data packets or new efficient route discovery. This attack can prevent the communication between nodes in the network.

In this research during simulation, attacker nodes continuously drop the data packets in every 1 sec intervals. Generally in wired networks, the packet losses happen due to congestion. In MANETs, due to its complex characteristics there are some other reasons such as congestion, mobility and wireless links transmission error to drop the packets. As in MANETs, mobility is the major cause to lose the data packets on AODV [10]. That's why this research concentrates to differentiate the packet dropping due to the mobility from the packet dropping due to malicious nodes in MANETs.

3 Fuzzy and Neuro-fuzzy

Fuzzy logic is one of very important component of soft computing that can able to deal with uncertainty and impreciseness drived from human logical thinking or reasoning. Fuzzy logic is able to handle the multi valued logic of fuzzy set theory between the ranges of 0 to 1 and it gives the decisions in degrees form rather than yes or no terms [23]. IF-then- else based fuzzy rules can specify the every situation in the network for detecting the intrusions or attacks. Fuzzy inference system (FIS) is based on fuzzy rules for taking the decisions towards fuzzy reason-

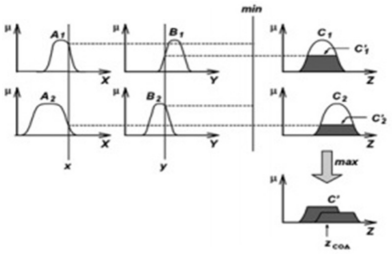


Figure 1: The Mamdani fuzzy interference system (MFIS) with min and max operators [8]

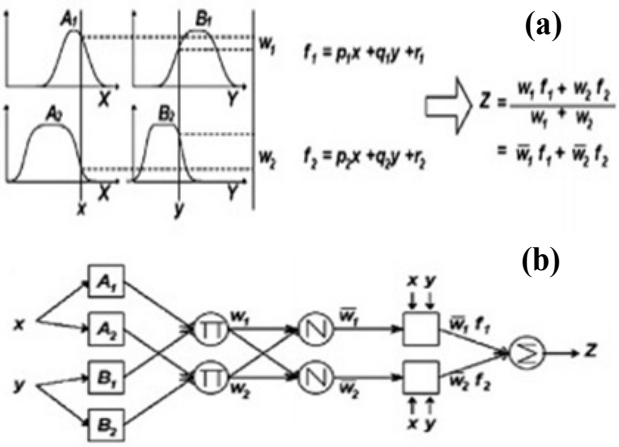


Figure 2: (a) Presents the Sugeno model fuzzy reasoning [8]. (b) Equivalent ANFIS structure [8]

ing. Some familiar fuzzy inference systems are proposed in the literature [8].

Mamdani FIS is shown in Figure 1. This is used defuzzification module that converts the fuzzy values to crisp values in terms of output. But, it is time consuming procedure. Takagi et al. suggested an approach to render the fuzzy rules from dataset [8] and is depicted in Figure 2(a). It is more efficient towards computation and also more suitable with adaptive techniques. Here, defuzzification is done by using weighted average.

There are several hybrids of soft computing approaches, where hybrid of neural and fuzzy has very popularity in many domains so that a very popular method has been proposed by Jang et al., which is known as ANFIS (Adaptive neuro-fuzzy inference system) [8].

In any modelling situation where nobody can't discover and recognize the membership functions and parameters linked with member functions for the large or vast data set. In this situation ANFIS is useful. It suggests a procedure for fuzzy modelling in respect of learning the information from a given dataset for computing the parameters of membership functions that permit the associated FIS to track or handle in best way of given input and output data. The membership functions related parameters will alter according to the procedure of learning. ANFIS can employ back propagation algorithm or aggregation of back propagation algorithm and least square estimation for the estimation of parameters related with membership functions. Figure 2(b) describes the ANFIS architecture [8]. This paper utilized the subtractive clustering method for determining the initial number of fuzzy rules and membership functions. However, ANFIS is applied for further fine tuning of these functions. Subtractive clustering [6] is quick, single pass algorithm for computing the clusters and cluster centres from a given dataset. Subtractive clustering is an extension of mountain clustering method that is indicated by Yager in [24].

According to the cluster information which is received by this algorithm is utilized to discover the initial rules and membership functions that are responsible to form the FIS. In this research work, FIS structure is received through subtractive clustering to cover the all features space. So this paper selected the subtractive clustering technique for evolving the numbers of initial fuzzy rules.

4 Features Selection and Dataset

"Features" are the spectacular attributes that are employed as inputs to our suggested system. For evolving of the better results, the selection of appropriate features is most important. Our proposed system has concentrated on features related to the packet dropping attack. Our proposed features are illustrated in Table 1, those are asserted on each node in the network through the AODV routing protocol. Basically this paper is emphasized to detect packet dropping attack through malicious nodes so that it permit to focuses a rich set of features for demonstrated the efficiency of proposed IDS.

The features are collected based on two categories, i.e. mobility related features and packet related features. Mobility related features devote the information regarding the reflection of mobility model for each node or network. Moreover, some features such as added neighbors; remove neighbors directly reflect the mobility of a node. Packet related features admit the information about the frequency of the routing protocol control packets for sent (RREQ), received (RREP) and forwarded at each time interval. However, some features are definitely presented the signature of particular attack e.g. detection of the packet dropping attack is possible through the "Dropped_datapkts" feature [17]. There is no requirement of communication amongst the mobile nodes during the collection of data, since totally selected features are local to each node [17]. This paper used the Qualnet simulator 6.1 [16] for extracting the data based on selected features to analyse the results of proposed system. Table 2 presented the list of parameters that have been set during the simulation by using Qualnet simulator and Table 3 is given the details of datasets in training, checking phases with simulation time 1,000s and testing with 800s

Table 1: The list of selected features

Abbreviations of Features	Explanations
Enum_dataPks_Initd	No. of data packets sent as source of the data by this node
num_dataPks_ fwrd	No. of data packets forwarded by this node
num_dataPks_ recvd	No. of data packets sent as destination of the data by this node
Num_ rep_ recvd_asSrce	No. of RREP packets received as source by this node
num_rep_initd_asDest	No. of RREP packets initiated from the destination by this node
num_rep_initd_asIntermde	No. of RREP packets initiated from the an intermediate node
num_rep_fwrd	No. of RREP packets forwarded by intermediate nodes
Num_ rep_ recvd	No. of RREP packets received by this node
num_req_recvd_asDest	No. of RREQ packets received as a destination for this node
num_err_ fwrd	No. of RERR packets forwarded by this node
num_err_ initd	No. of RERR packets initiated as this node detect the link break
num_routes	No. of routes added to the route cache
num_err_ recvd	No. of RERR packets received by this node
num_req_ initd	No. of RREQ packets initiates by this node
num_req_receivd	No. of RREQ packets received to this node
Num_brknLinks	Total no. of broken links
Dropped_datapkts	Calculates not forwarded data packets through this next node
num_addNbrs	No. of added neighbors of node during simulation time
num_rmveNbrs	No. of remove neighbors of node during simulation time
num_nbrs	No. of neighbors of node during simulation time

for neuro-fuzzy classifier based IDS in MANETs.

Table 2: Data samples in training, checking phase with simulation time 1,000s and for testing with 800s

Distributions of Data Samples	Class Normal	Class Attack
Training	12,000	12,000
Checking	3,000	3000
Testing	2,500	2500
Total	17,500	17500

Table 3: Simulation parameters list

Simulation Parameters	
Simulation time	1000s (Training) and 800s (Testing)
Mac Type	IEEE 802.11
Radio type	802.11b
Routing protocol	AODV
Antenna	Omni directional
No. Of Channels	One
Channel frequency	2.4 GHz
Packet size	512 bytes
Simulator	Qualnet 6.1
Energy Model	Generic
Path loss model	Two Ray
Pause time	30 second
Battery model	Linear model
Mobility speeds	0 to 25 mps
Batter Charge Monitoring	Interval 60 Sec.
Traffic type	CBR
Simulation area	1500m $\times 1500m$
Number of nodes	15 and 30 nodes
Mobility	Random Way Point
Malicious Nodes	4

5 Our Proposed Approach

The main motivation towards this proposed work to provide a framework for using hybrids of soft computing techniques, i.e. neuro-fuzzy to build the binary classifier that can act batter than the single soft computing technique.

In this section, we describe the proposed architectures of binary neuro-fuzzy classifier based intrusion detection system for MANETs which is depicted in Figure 3 and also includes data collection, detection and response modules. We utilized the feature list referred in Table 1, as the inputs for proposed IDS. Input patterns are labelled with 0 and 1 where 0 for normal and 1 for attack input data patterns for the point of view binary classifier

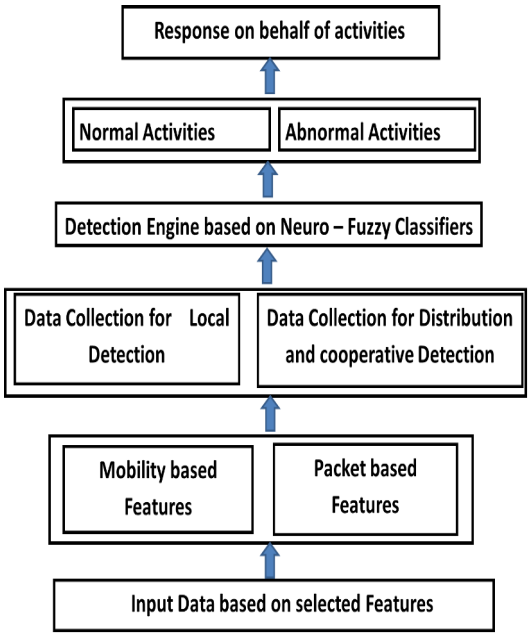


Figure 3: Architecture of proposed intrusion detection system

in MANETs. This paper described the two architectures of proposed binary neuro-fuzzy classifier based intrusion detection system, i.e. local, and distributed and cooperative.

In local intrusion detection system (L-IDS), each mobile node has an IDS agent in the network and detects the attacks on the bases of their own decision without the collaboration with other nodes. Moreover, in distributed and cooperative intrusion detection system (DC-IDS), each mobile node in the network has an IDS agent and detects the attacks on the bases of communication with other nodes to exchange the information, to share the decisions and finally to agree on responses with other nodes [18]. In this paper for DC-IDS, nodes communicate with their one hop away neighbors nodes to reach the decision that there is any malicious activity is available in MANETs or not.

For developing the L-IDS based on neuro-fuzzy classifier, 24,000 data patterns are used in training phase and 6,000 corrected label data patterns are used for checking phase to validate the model. As in Table 3 presented that 5,000 patterns are used for testing data that are not corrected label to test the model.

This paper used the subtractive clustering approach with neighborhood radius $r_a = 0.5$ to partition the training dataset and build the automatic initial fuzzy rules to make the fuzzy inference system (FIS) structure for training of ANFIS.

Hence, seven fuzzy rules and seven membership functions (Gaussian type) were received for each input. For further fine tuning and adaptation of membership functions, training dataset was applied for training of ANFIS and checking dataset was employed to check the validation of model since after some time in training phase, the model begins the over fitting with training dataset so that generated FIS acts bias with other independent datasets.

The employed ANFIS holds 272 nodes and total no. of fitting parameters are 364, in which premise parameters are 238 and consequent parameters are 126. The root mean square error (RMSE) of training and checking dataset are 0.34157 and 0.38461 after learning of 50 epochs.

As we discussed that the architecture of ANFIS gives simply one output so that here in this work the output of ANFIS architecture is mention by the class number, where class number 0 refers the normal activities and 1 presents the attacks.

For evolving the distributed and cooperative based intrusion detection system, the features for neighbor node is also available in Table 1 so that each mobile node can exchange the information about intrusions to their one hop away neighbor nodes through secure communication channels. The performance of training and testing of this architecture after 50 epochs is given in the Table 4. The performance of L-IDS and DC-IDS is demonstrated in Table 4.

The ANFIS output is not essential to provide the exact class number, i.e. 0 or 1 so that it may require the approximate value of class number. Due to this reason, a parameter is used to rounding off the given (output) number and provide the integer value (either 0 or either 1) to us. As per earlier mentioned in Section 4, ANFIS used the further fine tuning and adaptation of membership functions. Figure 4 shows the initial and final membership functions of some input features during ANFIS training phase.

There were developed some standard metrics, i.e. true positive rate and false positive rate for evaluating the performance of intrusion detection system [18]. Table 5 depicted the true positive rate and false positive rate after 50 epochs of training and checking dataset at $\mu = 0.5$.

6 Results

From the results point of view in this paper, two different ways of testing have been applied. This paper used all patterns of packet dropping attack without corrected labelled dataset to test our proposed neuro- fuzzy classifier based local intrusion detection system and cooperative detection system. Table 4 shows the detection rates, i.e. true positive rate and false positive rate of L-IDS and DC-IDS under 15 and 30 nodes with varied traffic rate and mobility speeds. Figures 5, 6 presented the true positive rate of L-IDS and DC- IDS and Figures 7, 8 presented the false positive rate in respect of L-IDS and DC- IDS. From the results it noticed that neuro-fuzzy classifier based DC-IDS increases the true positive rate and decreases the false positive rate in terms of L-IDS. But in DC-IDS, exchang-

Table 4: Shows the detection rates of L-IDS and DC-IDS

No of Nodes	Traffic	Mobility	Local Detection(%)		Distributed and Cooperative Detection(%)	
			TPR	FPR	TPR	FPR
15	high	low	98.0	1.31	98.52	1.12
15	low	low	99.84	0.47	99.85	0.31
15	low	high	99.90	0.82	99.95	0.79
15	medium	medium	99.53	1.50	99.73	1.37
30	high	low	98.48	1.76	98.53	1.53
30	low	low	99.87	0.89	99.85	0.83
30	low	high	0.99	99.97	5.5	0.95
30	medium	medium	99.61	99.75	5.5	2.00

ing the information between the neighbors nodes may be consumed more energy and bandwidth over L-IDS so an alternative solution for DC-IDS is that if any node having the symptoms about the suspicious activity present in the network, at that moment this node exchange the information their neighbor nodes.

In this paper, the receiver operating characteristics (ROC) analysis is used in regards of the parameter for presenting the effect on the true positive rate and false positive rate. Basically this ROC analysis is made for evaluating the performance of neuro-fuzzy classifier in respect of parameter. For discovering the variation between true positive rate and false positive rate, we varied the value of parameter between the 0 to 0.5 and plotted the coordinate points in respect of (FPR, TPR) μ [7].

Table 5: True positive rate (TPR) and false positive rate (FPR) of training and checking dataset at $\mu = 0.5$

Data Set	**TPR%**	**FPR%**
Training	99.82	0.61
Checking	98.1	1.7

7 Conclusion

In this paper, we have proposed a novel intrusion detection system based on neuro-fuzzy classifier in binary form for packet dropping attack in mobile ad hoc networks. In terms of IDS architecture, we have described two types of architectures based on neuro fuzzy classifier, i.e. local, and distributed and cooperative. From the results it's noticed that L-IDS and DC-IDS both the systems presented good performance to detect the packet dropping attack. The proposed architectures of IDS give the output in form of 0 or 1 where 0 shows the normal pattern and 1 presents the abnormal pattern so that in this paper, output 1 means malicious nodes are presented in the network. In future, we are concentrating to detect all type of attacks in MANETs environment.

Acknowledgments

This work is partially supported by government of India vide Dst/tsg/nts/2012/106, we acknowledge A.N.TOOSI (Department of Computing and Information System), University of Melbourne for their useful suggestions.

References

[1] M. S. Abadeh, J. Habibi, and C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm," *Journal of Network and Computer Applications*, vol. 30, pp. 414–428, 2005.

[2] A. Chaudhary, A. Kumar, and V. N. Tiwari, "A reliable solution against packet dropping attack due to malicious nodes using fuzzy logic in MANETs," in *International Conference on Optimization, Reliabilty, and Information Technology (ICROIT'14)*, pp. 178–181, 2014.

[3] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," *BVICAM's International Journal of Information Technology*, vol. 6, no. 1, pp. 690–696, 2014.

[4] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc network," in *IEEE International Advance Computing Conference (IACC'14)*, pp. 256–261, 2014.

[5] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A cooperative intrusion detection system for sleep deprivation attack using neuro-fuzzy classifier in mobile ad hoc networks," *Computational Intelligence in Data*, vol. 2, pp. 345–353, 2015.

[6] S. L. Chiu, "Fuzzy model identification based on cluster estimation," *Journal of Intelligent and Fuzzy Systems*, vol. 2, no. 3, pp. 267–278, 1994.

[7] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," in *Proceedings of the*

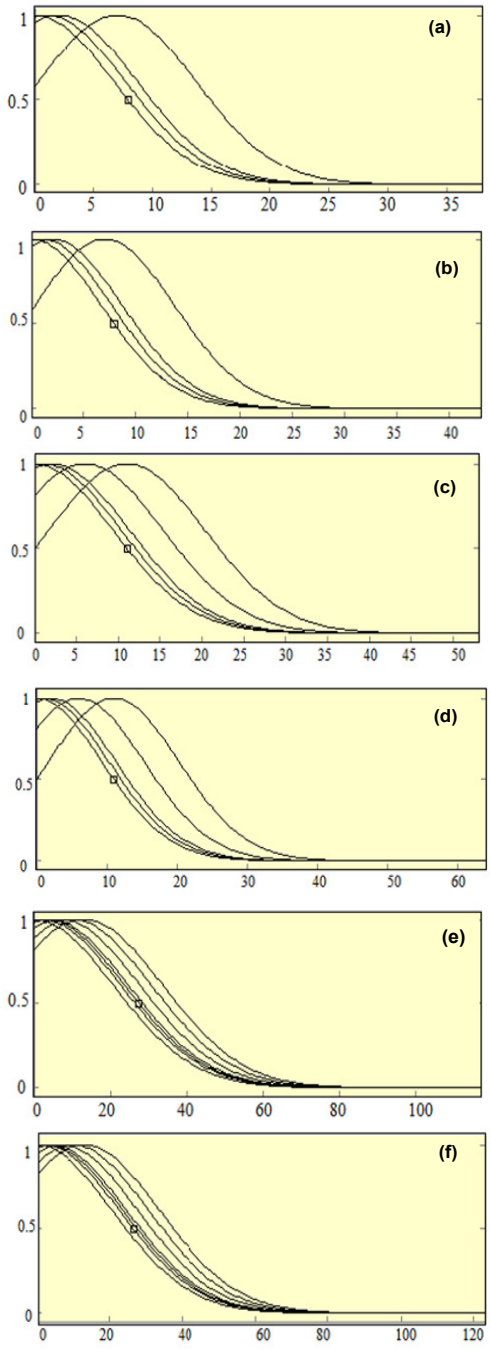


Figure 4: Initial and final membership functions of some input features during ANFIS training phase. (a) Before training, MFs of input feature 6 in L-IDS. (b)After training, MFs of input feature 6 in L-IDS. (c)Before training, MFs of input feature 11in L-IDS. (d) After training, MFs of input feature 11in L-IDS. (e) Before training, MFs of input feature 13in DC-IDS.(f)After training, MFs of input feature 13 in DC-IDS.(a), (c), (e) presents the initial membership functions before training phase and (b), (d), (f) final membership functions after training phase.

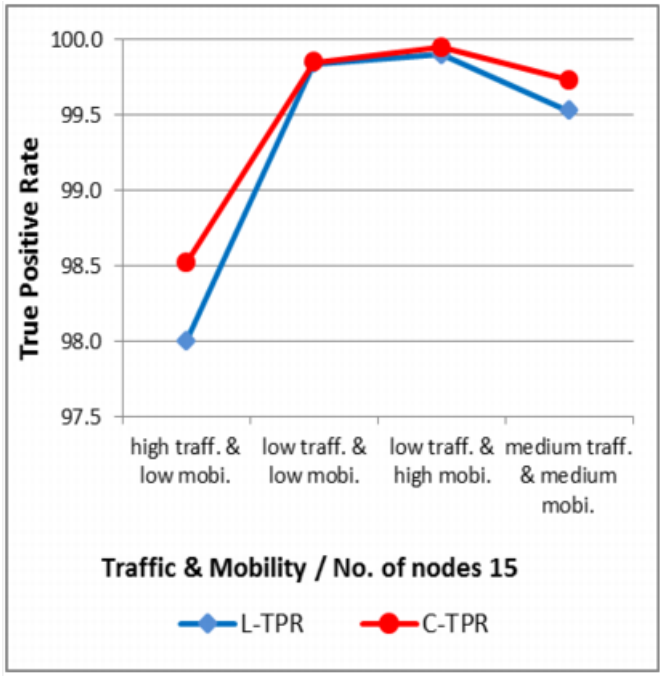


Figure 5: represents true positive rate under 15 nodes of L-IDS and DC-IDS

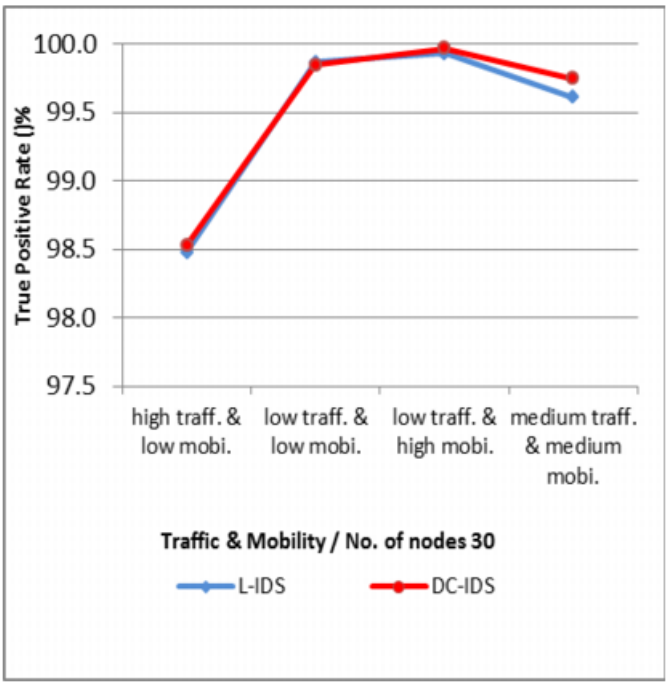


Figure 6: represents true positive rate under 30 nodes of L-IDS and DC-IDS

Figure 7: represents false positive rate under 15 nodes of L-IDS and DC-IDS

Figure 8: represents false positive rate under 30 nodes of L-IDS and DC-IDS

2002 IEEE Workshop on Information Assurance, vol. 6, pp. 1–8, 2002.

[8] J. S. R. Jang, C. T. Sun, and E. Mizutani, *Neuro-Fuzzy and Soft Computing - A Computational Approach to Learning and Machine Intelligence*, Prentice-Hall, 1996.

[9] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in manet," in *Proceedings of the Information Systems Education Conference*, pp. 1–17, 2004.

[10] Y. Lu, Y. Zhong, and B. Bhargava, *Packet Loss in Mobile Ada Hoc Networks*, Computer Science Technical Reports, Report Number: 03-009, Purdue University, 2003.

[11] A. Mitrokosta, N. Komninos, and C. Douligeris, "Intrusion detection with neural networks and watermarking techniques for MANETs," in *IEEE International Conference on Pervasive Services*, pp. 118–127, 2007.

[12] Z. Moradi and M. Teshnehlab, "Intrusion detection model in manets using ANNs and ANFIS," in *International Conference on Telecommunication Technology and Applications*, vol. 5, 2011.

[13] Z. moradi, M. Teshnehlab, and A. M. Rahmani, "Implementation of neural networks for intrusion detection in MANET," in *International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT'11)*, pp. 1102–1106, 2011.

[14] D. Nauck and R. Kruse, "Nefclassmdash: a neuro-fuzzy approach for the classification of data," in *Proceeding of ACM Symposium on Applied Computing*, pp. 461–465, 1995.

[15] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the Second IEEE workshop on Mobile Computer Systems and Applications*, pp. 90–100, 1999.

[16] SCALABLE Network Technologies, "Qualnet simulator," Sept. 1, 2015. (`http://www.scalable-networks.com`)

[17] S. Sen and J. A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks," in *ProceedingsIn of the Second ACM Conference on Wireless Network Security (WiSec'09)*, pp. 95–102, 2009.

[18] S. Sen and J. A. Clark, *Guide to Wireless Ad Hoc Networks: Chap. 17. Intrusion Detection in Mobile Ad Hoc Networks*, pp. 427–454, Springer, 2009.

[19] S. Sen, J. A. Clark, and J. E. Tapiador, "Ad-hoc on-demand distance vector routing," in *Security Threats in Mobile Ad Hoc Networks, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, pp. 127–147, 2010.

[20] M. H. Shao, J. B. Lin, and Y. P. Lee, "Cluster-based cooperative back propagation network approach for intrusion detection in MANET," in *IEEE 10th International Conference on Computer an Information Technology (CIT'10)*, pp. 1627–1632, 2010.

[21] S. Sujatha, P. Vivekanandan, and A. Kannan, "Fuzzy logic controller based intrusion handling system for mobile ad hoc networks," *Asian Journal of Information Technology*, vol. 7, pp. 175–182, 2008.

[22] M. Y. Tabari, H. Hassanpour, and A. Movaghar, "Proposing a distributed model for intrusion detection in mobile ad-hoc network using neural fuzzy interface," in *Journal of Advances in Computer Research*, vol. 1, pp. 85–96, 2011.

[23] M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic," in *3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS'12)*, pp. 189–192, 2012.

[24] R. Yager and D. Filev, "Generation of fuzzy rules by mountain clustering," *Journal of Intelligent and Fuzzy Systems*, vol. 2, no. 3, pp. 209–219, 1994.

[25] L. A. Zadeh, "Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems," in *Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications*, NATO ASI, vol. 162, pp. 1-9, Springer, 1998.

[26] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00)*, pp. 275–283, 2000.

Alka Chaudhary received her M.C.A. degree from Institute of Technology and Science (ITS), Mohan Nagar, Ghaziabad in 2010. Currently, she is pursuing Ph.D (Full Time) in Computer Science from Manipal University Jaipur (MUJ), Rajasthan. Her research interests include information security, Mobile Ad Hoc Networks, Neural network, Fuzzy Logic, intrusion detection/prevention, and Network Security.

V. N. Tiwari received his Ph.D degree from IIT, BHU, Varanasi in 1997. He is Currently Working as a HOD of Electronic and Communication Department in Manipal University Jaipur (MUJ), Rajasthan. He has published more than 35 research papers in National/International Journals and Conferences. He has 20 years of R and D and Teaching Experience. His research interests include Microwave Technology, Antennas and Radar.

Anil Kumar received his Ph.D. degree in Computer Science from Sikkim Manipal University, Sikkim (India). He is currently working as a Professor in Department of CSE, Manipal University Jaipur (MUJ). He is an IEEE Senior Member and he is currently guiding 3 - Full Time and 3 - Part Time Research Scholars. His research interests include Image processing algorithm, Cryptography, Artificial Intelligence, Signal and System, Neural System and Genetic Algorithm. He has published more than 70 research papers in international journal and conferences.

Improved Methods and Principles for Designing and Analyzing Security Protocols

Ali Kartit[1], Hamza Kamal Idrissi[2], and Mohamed Belkhouraf[1]
(Corresponding author: Ali Kartit)
Laboratory of Technology and Information, Department of TRI/ENSAJ, Chouaib Doukkali University[1]
No. 2, Avenue Mohamed ben Larbi Alaoui, El Jadida, Morocco
Laboratory of RIT, Department of Physics/FSR, Mohammed V University[2]
B.P. 554 3 Rue Michlifen, Rabat, Morocco
(Email: alikartit@gmail.com)
(Received Dec. 06, 2014; revised and accepted July 4 & August 12, 2015)

Abstract

Security protocols are a critical element of the infrastructures needed for secure communication and processing information. Before designing and analyzing protocols, it is important to reduce avoidable work. In this article, we presented the methods to prevent replay attacks [11] and attacks of the type flaw attacks on the protocols. We studied two types of attacks already mentioned. We presented some principles for secure protocols. To meet these principles, we have presented some methods for the design of security protocols. Some security vulnerabilities in security protocols published could be found by the principles presented and then we try to improve these protocols with the methods presented. A number of examples in the literature show that the work done in the document is very important.

Keywords: Analyzing security protocol, designing security protocol, flaw attack, replay attack

1 Introduction

Most security protocols are extremely simple if only their length is considered. However, the properties they are supposed to ensure are extremely subtle, and therefore it is hard to get protocols correct just by informal reasoning and "eyeballing".

Designing a secure protocol is a very difficult task. A set of principles and methods have been proposed from various aspects for different purposes [4]. Although these principles are described informally and are neither sufficient nor necessary for the reliability of the protocols, many flaws security protocol can be avoided from the start and the security protocols are designed more reliable if the designers or manuals developers automatic tools are familiar with them [1]. After our detailed analysis of these principles, we have found some existing problems, namely, some are too general to be practical; some are ambiguous so that designers are hard to grasp; some speak only of thought, not to study how to build protocols and avoid mistakes. We put forward a set of principles and methods against replay attacks and type flaw attacks by analyzing the attack characteristics and the reasons for the attack. A large number of examples show that the set of principles and methods are simple, efficient and practical.

2 Related Work

Above the previous two decades, the design of trustworthy and unfailing security protocols has been lectured by several publications. Introduced firstly in [5], the two-way authentication protocol based on symmetric key cryptography was enhanced in [6] in order to avoid weaknesses in the design of these types of protocols. This publication announced a methodology to automatically form a family of cryptographic two-way authentication protocols that are unaffected by the majority of attacks. In order to protect protocol messages from being vulnerable to replay attacks, [8] and [9] presented the notion of fail-stop protocols over a restricting group of protocol design considerations that prevent from replay attacks under some circumstances.

In 1996, [2] featured a group of elementary basics for reinforcing the security protocols design. They lectured two main issues messages authentication and trust. They incorporate also asymmetric key encryption. Nevertheless, these sets of principles do not guarantee protocol correctness. [3] and [15] suggested recommendations to avoid replay attacks, by using type-tagging messages with unique cryptographic functions and unique session keys without supposing common trust between the participants.

[13] recognized desynchronization attacks in 2013 on a group of protocols that employ dynamic shared secrets mechanisms for wireless messages. The authors a formal

system to model up-date mechanisms for shared secrets.

The effort on designing a novel trustworthy security protocols is still active today, as is the identification and solving design weaknesses in existing protocols [7, 10].

3 Principles and Methods

With the study of a large number of examples of replay attack [12, 17] and type flaw attack examples [18], and to investigate the cause of the attacks leads us to say that to avoid both types of attacks, applicable to principals session key must satisfy the following conditions:

- It can correctly judge that the principals of the session key produced belongs to;
- It can correctly judge which protocol run received messages belongs to;
- It can correctly judge whether a received message is reassembled and is a whole message sent by other party;
- It can correctly distinguish between messages structured by other party and by myself.

To make the application of guiding the session key to achieve the objectives mentioned above, the server must meet the following conditions:

- It knows which principals are applying for a session key;
- It knows identities of protocol runs initiated by principals applying for session keys;
- A message must be structured as a whole, in addition to principals who know the decryption key, no entity can separate it.

In addition, the type flaw attack result from the cause that different principal might use same key to encrypt similar or anti-symmetric similar massages. Many solutions have studied how to build differentiable messages, but often their methods, as long as adding a viable hypothesis; they may not enter law attack. From another point of view, we find that principals send clear on the application server for a session key, which play the same role with the encrypted message. Thus, in the protocols, only the use of shared server key to encrypt a message, which makes the distinction, encrypted messages. With the method, attack type law would be avoided.

3.1 Principles

With above analysis, design principles of security protocols against replay attack or type flaw attack are as follows.

Principle 1. *Principals and server can distinguish between protocol runs, which is critical to make protocol avoid a wide variety of attacks.*

Principle 2. *The distributing session key message must be a whole, in addition to principals applying the session key, no one can separate them [16].*

Principle 3. *Principal must know which principals the obtained session key is distributed to and which protocols run it belongs to.*

Principle 4. *Principal can identify that received encrypted message is not structured by himself.*

Principle 5. *If a protocol run is interrupted or intercepted after some steps, it must be satisfied that the risk is as less as possible.*

3.2 Methods

In order to make generated messages in the protocol meet the above principles, we design security protocol with the following methods:

Method 1. *Generate SID (Session Identifier) of protocol run copy. SID often consists of identifiers of principals applying for session key, nonce produced by principals and so on. SID contains nonce or a time stamp. Different principal has different nonce, and different runs copy has different nonce. Every nonce is unique. Using the time stamp requests that all participants have a global time system, namely, their time must be consistent, but, because time stamp has a valid period, near runs are difficult to be distinguished.*

Method 2. *Message distributing session key should contain SID.*

Method 3. *Message distributing session key is encrypted with shared key between receiver and server as a whole, and, generally, is structured as follows.*

$$\{SID, SeK, \{SID, SeK\}_{ShK_1}\}_{ShK_2}$$

where SeK denotes session key, and ShK denotes a shared-key.

Method 4. *In protocol, message applying for session key is plaintext as possible as. Considerable evidences show that sending encrypted message applying for session key plays the same role as sending plaintext message.*

Method 5. *The order sending of messages is presented in the Figure 1.*

The order of sending messages is adopted mainly because protocols run is initiated firstly by principal who has secret information to send other party. If the principal believes that applying session key have been successful, he will encrypt secret message with the gained session key and then will send it. After, he thinks that the task has been completed. If other party thinks that applying session key have been successful, but the initiator doesn't know it, the initiator re-initiates protocol run after a period of time, which wouldn't bring out much damage.

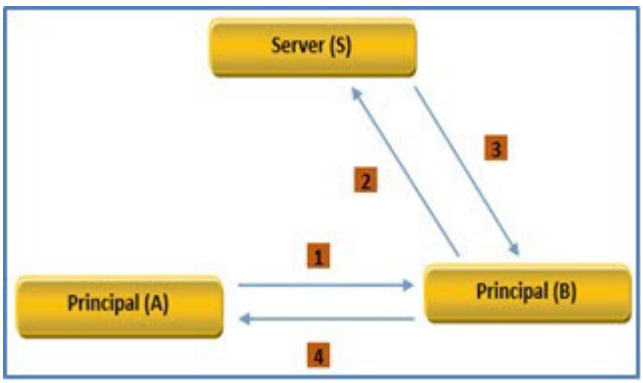


Figure 1: Order of sending messages

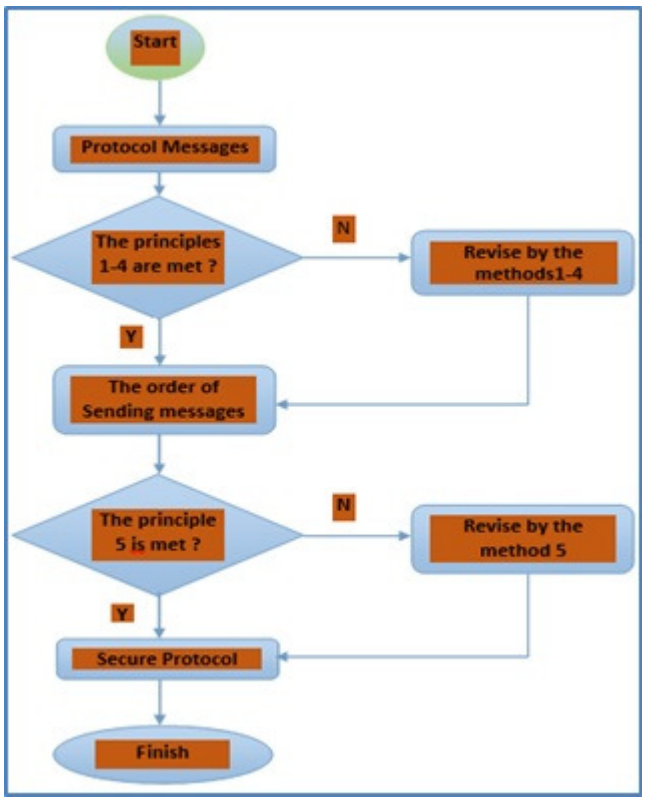


Figure 2: Process of analyzing and improving

4 Analysis and Improvement of the BAN-Yahalom Protocol

The process of using the above principles and methods to analyze and improve some security protocols is presented in the Figure 2.

By BAN logic analysis of Yahalom protocol, it is found that if A selects an old key to replay to B, B could not find it [14]. Therefore, BAN logic author improved Yahalom protocol. The improved Yahalom protocol (called BAN-Yahalom protocol) is as follows:

1) $A \longrightarrow B : A, N_a$;

2) $B \longrightarrow S : B, N_b, \{A, N_a\}_{Kbs}$;

3) $S \rightarrow A : N_b, \{B, K_{ab}, N_a\}_{Kas}, \{A, K_{ab}, N_b\}_{Kbs}$;

4) $A \rightarrow B : \{A, K_{ab}, N_b\}_{Kbs}, \{Nb\}_{Kab}$.

In this protocol, obviously, Principle 2, Principle 4 and Principle 5 are not met.

4.1 Principle 2 Destruction

To Principle 2 destruction, the protocol can be attacked as follows:

1) $A \longrightarrow P(B) : A, N_a$;

1') $P(B) \rightarrow A : B, N_a$;

2') $A \rightarrow P(S) : A, N'_a, \{B, N_a\}_{Kas}$;

2") $P(A) \rightarrow S : A, N_a, \{B, N_a\}_{Kas}$;

3') $S \rightarrow P(B) : N_a, \{A, K_{ab}, N_a\}_{Kbs}, \{B, K_{ab}, N_a\}_{Kas}$;

3) $P(S) \rightarrow A : N_p, \{A, K_{ab}, N_a\}_{Kbs}, \{B, K_{ab}, N_a\}_{Kas}$;

4) $A \rightarrow P(B) : \{A, K_{ab}, N_b\}_{Kbs}, \{N_p\}_{Kab}$.

In the above description, P(A), P(B) and P(S) represent that attacker P personate identity of A, B and S respectively. During the attack, the attacker P personate B to intercept the message (1) $A \longrightarrow P(B) : A, N_a$ and change the label of entity's name from A to B (1') $P(B) \rightarrow A : B, N_a$, by it A initiates a new run of distributing session key. The entity A thinks that B want to apply a session key with him, selects the nonce N'_a and encrypts received message in (1') to send them to S. However, the attacker P intercept the message (2') $A \rightarrow P(S) : A, N'_a, \{B, N_a\}_{Kas}$ In (2"), N'_a will be replaced with Na by the attacker P, by which P personate A to send message to S. When S receive the applying session key message, he think that B initiate a protocol's run round of applying session key to A and then generates a session key and encrypt it with the shared key K_{bs} to send B. The attacker personate B to intercept it, changes the inside plaintext N_a as N_p and personate S to send the obtained message to A in (3). When A receives the message (3), he can prove that protocol run applying session key initiated by oneself has successfully completed and gets the session key K_{ab}. Finally, A encrypt the nonce N_p with K_{ab} and send encrypted message and the message that S send to B to B, but the messages are intercept by the attacker P. As the result, A believe that protocol run of applying session key with B is successful and obtained session key is K_{ab}. Nevertheless, in the whole process, B does not participate in at all. To avoid the attack, we modify the above message (3) by Method 3 as follows:

3) $S \rightarrow A : \{B, K_{ab}, N_a, \{A, K_{ab}, N_b\}_{Kbs}\}_{Kas}$.

4.2 Principle 4 Destruction

Because Principle 4 is not satisfied, we can carry out the following attacks in the above protocol:

1) $P(A) \rightarrow B : A, N_a$;

2) $B \rightarrow P(S) : B, N_b, \{A, N_a\}_{Kbs}$;

1') $P(A) \rightarrow B : A, N'_a$;

2') $B \rightarrow P(S) : B, N'_b, \{A, N'_a\}_{Kbs}$;

4) $P(A) \rightarrow B : \{A, N'_b\}_{Kbs}, \{N_b\}_{Kab}$.

In above expression, P(A) and P(S) stand for that attacker P personate identity of A and S respectively. Assume that message $N'_a = K_{ab} + N_b$ and message K_{ab} are any strings that attacker know. In the process, entity A and entity S don't participate in the run of protocol, but the result is that attack P personate identity of A to share the key K_{ab} with B and that attack P know the key K_{ab}, which is very dangerous. To this defect, we use Method 4 to modify message 2 as follows:

2) $B \rightarrow S : A, B, N_a, N_b$.

4.3 Principle 5 Destruction

In this protocol, exchanging message sequence is not perfect and violates Principle 5. The attacker only need to intercept the message in the fourth step to make A believe that the application is successful and make B believe that the application is failed. In order to reduce harm that this kind of simple attacks brought about, the exchanging message order should be adjusted according to the design Method 5. Therefore, to avoid attack of BAN-Yahalom protocol, we modify the protocol by our principles and methods as follows:

1) $A \rightarrow B : A, N_a$;

2) $B \rightarrow S : A, B, N_a, N_b$;

3) $S \rightarrow B : \{A, K_{ab}, N_b\{B, K_{ab}, N_a\}_{Kas}\}_{Kbs}$;

4) $B \rightarrow A : \{B, K_{ab}, N_a\}K_{as}$.

5 Analysis and Modification of Abadi and Needhan Improved Otway-Rees Protocol

The Otway-Rees protocol is a simple security protocol put forward by 1987. On the help of server, both parties of communication securely get the session key. The author of BAN logic formally analyzed the Otway-Rees protocol and the result is that the protocol is secure, but there are redundant messages in it. Therefore, he modified the Otway-Rees protocol. Later, Boyd and Mao found the improved protocol to have security flaws. Since then, Adadi and Needham noted this defect and improved it. The improved protocol is as follows:

1) $A \rightarrow B : A, B, N_a$;

2) $B \rightarrow S : A, B, N_a, N_b$;

3) $S \rightarrow B : \{N_a, A, B, K_{ab}\}_{Kas}, \{N_b, A, B, K_{ab}\}_{Kbs}$;

4) $B \rightarrow A : \{N_a, A, B, K_{ab}\}_{Kas}$.

The above protocol is correct and efficient by BNA logic verification. but we can easily see that it doesn't meet Principle 2. There are a replay attack defect in the protocol because the message that server sends to entity B doesn't meet the atomicity principle. The attack process is as follows:

1) $A \rightarrow B : A, B, N_a$;

2) $B \rightarrow S : A, B, N_a, N_b$;

3') $S \rightarrow P(B) : \{N_a, A, B, K_{ab}\}_{Kas}, \{N_b, A, B, K_{ab}\}_{Kbs}$;

2") $P(B) \rightarrow S : A, B, N_a, N_b$;

3") $S \rightarrow P(B) : \{N_a, A, B, K'_{ab}\}_{Kas}, \{N_b, A, B, K'_{ab}\}_{Kbs}$;

3) $P(S) \rightarrow B : \{N_a, A, B, K'_{ab}\}_{Kas}, \{N_b, A, B, K_{ab}\}_{Kbs}$.

P(B) stands for that attacker P personate identity of B. The attacker intercepts the message in Step 3) and personate B to initiate a new run of protocol. S think that A and B apply for a new session key and distribute a session key K'_{ab} to B. The attacker intercepts it. At the time, the attacker has two distributed session keys K_{ab} and K'_{ab} to A and B and in Step 3) combine them to personate S to send it to B. When B receive the combined messages, he doesn't know that the message has been reassembled, and he believes that applying the session key is successful and forwards message to A. When A receives the message, he verify it to be his application session key. As the result, both believe that this application is successful, but their obtained the session keys are inconsistent. The attacker reach his deliberate destruction goal. To such attack, the protocol could be modified by above Method 3. The revised protocol is as follows:

1) $A \rightarrow B : A, B, N_a$;

2) $B \rightarrow S : A, B, N_a, N_b$;

3) $S \rightarrow B : \{N_a, A, B, K_{ab}, \{N_a, A, B, K_{ab}\}_{Kas}\}_{Kbs}$;

4) $B \rightarrow A : \{N_a, A, B, K_{ab}\}_{Kas}$.

The revised protocol meet the above principles, which can avoid various kinds of attacks. Here the exchanging message sequence is of vital importance. We exchange Steps 3) and 4) as follows.

3) $S \rightarrow A : \{N_a, A, B, K_{ab}, \{N_b, A, B, K_{ab}\}_{Kas}\}_{Kbs}$;

4) $A \rightarrow B : \{N_b, A, B, K_{ab}\}_{Kbs}$.

There is no much effect on the attack, but their security goal is not the same. When A receives message from server, he verify that the session key is correct and then forwards the corresponding message to B. However, he was not sure whether B receives the message. Therefore, he cannot decide that whether send his secret message encrypt by the session key to B or initiate a new run of protocol for applying session key. It can be easily seen that exchanging messages sequence is very important and that designing security protocol is difficult, in which subtle difference will bring about different effect.

6 Conclusion

In this article, the theory of examples of the replay attack and the type flaw attack are analyzed and a set of principles and methods are put forward.

In addition, we illustrated their simplicity and efficiency through analyzing and improving some classic protocols. The result shows that understanding the set of principles and methods make us avoid errors of replay or type-flaw attack in designing and analyzing security protocols. We hope that the work has a good guiding role in protocol analysis and design.

Before using formal tool to analyzing security protocols, defects of replay and type flaw attack can be found and avoided as much as possible by informal ways.

In future work, we intend to put into practice the principles and methods mentioned above to secure such a protocol.

References

[1] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols," *IEEE Transactions on Software Engineering*, no. 1, pp. 6–15, 1996.

[2] R. Anderson and R. Needham, "Robustness principles for public key protocols," in *Advances in Cryptology (CRYPTO'95)*, pp. 236–247, Springer, 1995.

[3] T. Aura, "Strategies against replay attacks," in *Proceedings of 10th IEEE Workshop on Computer Security Foundations*, pp. 59–68, 1997.

[4] G. Bella, "The principle of guarantee availability for security protocol analysis," *International Journal of Information Security*, vol. 9, no. 2, pp. 83–97, 2010.

[5] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "Systematic design of two-party authentication protocols," in *Advances in Cryptology (CRYPTO'91)*, pp. 44–61, Springer, 1992.

[6] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, et al., "Systematic design of a family of attack-resistant authentication protocols," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 679–693, 1993.

[7] B. Blanchet, "Automatic verification of security protocols in the symbolic model: The verifier proverif," in *Foundations of Security Analysis and Design*, pp. 54–87, Springer, 2014.

[8] U. Carlsen, "Cryptographic protocol flaws: know your enemy," in *Proceedings of IEEE Computer Security Foundations Workshop (CSFW'94)*, pp. 192–200, 1994.

[9] Li Gong and P. Syverson, "Fail-stop protocols: An approach to designing secure protocols (preprint)," in *Dependable Computing for Critical Applications*, pp. 44–55, IEEE, 1994.

[10] A Jurcut, T. Coffey, and R. Dojen, "Establishing and fixing security protocols weaknesses using a logic-based verification tool," *Journal of Communication*, vol. 8, no. 11, pp. 795–806, 2013.

[11] A. D. Jurcut, T. Coffey, and R. Dojen, "Design guidelines for security protocols to prevent replay & parallel session attacks," *computers & Security*, vol. 45, pp. 255–273, 2014.

[12] R. Khera and R. Sethi, "Enhancement in alarm protocol to prevent replay attack in MANET," in *International Journal of Engineering Research and Technology*, vol. 2. no. 5, pp. 2115–2119, 2013.

[13] I. Lasc, R. Dojen, and T. Coffey, "On the detection of desynchronisation attacks against security protocols that use dynamic shared secrets," *Computers & Security*, vol. 32, pp. 115–129, 2013.

[14] G. M. Li, "Secure analysis and improvement of yahalom protocol," *Microcomputer Development*, vol. 4, pp. 34, 2005.

[15] S. Malladi, J. Alves-foss, and R. B. Heckendorn, "On preventing replay attacks on security protocols," in *Proceedings of the International Conference on Security and Management*, pp. 77–83, CSREA Press, 2002.

[16] T. S. Sobh, A. Elgohary, and M. Zaki, "Performance improvements on the network security protocols," *International Journal of Network Security*, vol. 6, no. 1, pp. 103–115, 2008.

[17] L. Sun, Z. Luo, Y. Wu, and Y. Wang, "A technique for preventing replay attack in road networks," in *7th IEEE International Conference on Computer Science & Education (ICCSE'12)*, pp. 807–810, 2012.

[18] J. Wang, J. Zhang, and H. Zhang, "Type flaw attacks and prevention in security protocols," in *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'08)*, pp. 340–343, 2008.

Ali Kartit received the PhD degree in Computer Science (November 2011) Specialty Security of Computer Networks. He graduated from the University Mohamed V Faculty of Rabat. The author has developed a rich and diverse experience of over 12 years in the computer world, including 8 years in technical and vocational education as a computer network trainer and manager module "computer network security notions" and 4 years

in the corporate world as Administrator of computer networks and Head of the park. The author is a certified Cisco and Microsoft Exchange Server 2003. His research area covers security policies of firewalls, the Intrusion detection systems and cloud security.

Hamza Kamal Idrissi graduated in 2010 at ENSIAS, Mohammed V University Rabat, as an IT Engineer. After a three years experience as a formative teaching Computer Networks and IT development for post baccalaureate students, he is currently working on a PhD, his area of research covers security aspects in the Cloud Computing, IDS and security policies.

Mohamed Belkhouraf graduated in 2010 at ENSIAS, Mohammed V University Rabat, as an IT Engineer. After a three years experience as an Information System Project Engineer in the private sector, he is currently working on a PhD, his area of research covers security aspects in the Cloud Computing.

An Improved Privacy Solution for the Smart Grid

Mohamad Badra[1] and Sherali Zeadally[2]
(Corresponding author: Mohamad Badra)
College of Technological Innovation, Zayed University[1]
P.O. Box 144534, Abu Dhabi, U.A.E.
College of Communication and Information, University of Kentucky[2]
Lexington, KY 40506-0224, USA
(Email: mohamad.badra@zu.ac.ae)
(Received Dec. 20, 2013; revised and accepted Feb. 12 & Mar. 9, 2014)

Abstract

Recent advances in hardware, software, computing, and communication technologies have enabled the design and deployment of a smarter, interactive, dynamic 21st century electrical grid, also known as the smart grid. The bi-directional flow of information between the customer premise and the utility provider opens up several privacy challenges that must be addressed. We describe possible man-in-the-middle attacks against one (proposed by Marmol et al.) of the recently proposed privacy solutions for the smart grid environment. To address this vulnerability, we propose an improved privacy solution. We demonstrate the robustness and efficiency of our solution through a detailed security analysis.

Keywords: Advanced metering infrastructure, communication, man-in-the-Middle attack, privacy, protocol, security, smart grid

1 Introduction

In the last few years, we have witnessed a growing interest and increasing investments in smart grid technologies around the world. A smart grid is a complex infrastructure based on a set of seven domains [18]: bulk generation, energy distribution, power transmission, operation and control, market, service providers, and customers. Each domain comprises heterogeneous elements that include organizations, buildings, individuals, systems, system resources and other entities. The backhaul communication and the Internet are crucial for connecting the different entities involved such as customers and utility systems through an Advanced Metering Infrastructure (AMI) [6]. An AMI is an interface with the capability for managing and interacting with smart meters and utility business systems through a bi-directional communication. This communication replaces the traditional one-way Advanced Meter Reading (AMR) approach by enabling business utilities or providers to notify their customers of electricity pricing at any time, providing them with customizable services to manage their power consumption themselves in addition to controlling the demand in real time.

There are several technologies and applications that have been integrated into an AMI system [5] including (as shown in Figure 1): smart meters, wide-area communications infrastructure, Home (local) Area Networks (HANs) and operational gateways working as main collectors. The smart meter is an advanced meter that measures energy consumption in much more detail than a conventional meter does. Future smart meters are envisaged to communicate information back to the local utility company for monitoring voltage loads and for billing purposes. Among some of the tasks that a smart meter can do are [18]: time-based pricing, collecting consumption data for consumer and utility, net metering, or communications with other intelligent devices or appliance devices in the home. As a result, the smart meters make it possible to add some kind of "intelligence" to the network and individual features of each residential consumer.

One of the key characteristics of the smart grid is its support for bi-directional information flow between the customer's premise and the utility provider using Internet Protocol-based technologies [19]. The bi-directional nature of information flow has however opened up various security and privacy challenges which are being addressed by many recently proposed security solutions. Currently, there are several types of concerns related to the privacy and security of data associated with the smart grid. The most serious threats related to the privacy deterioration of smart grid consumers include:

1) Cyber-attack and intrusion: the use of communication capabilities and technologies for critical functions such as control and monitoring of smart meters makes smart grid more prone to cyber-attacks.

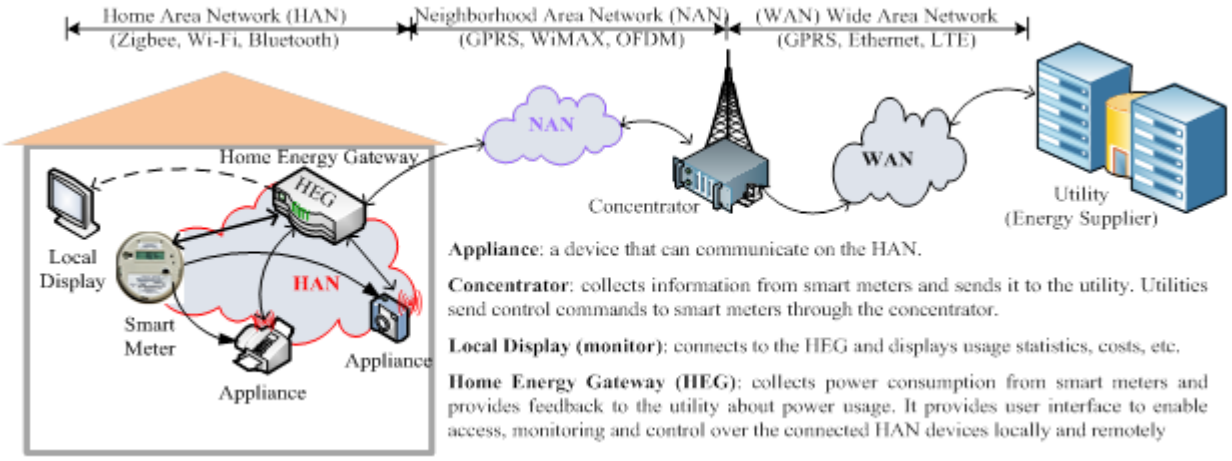


Figure 1: The AMI architecture

Some examples of cyber-attacks include denial-of-service attacks and the cyber vulnerabilities that are exploitable by malicious entities to disrupt smart grid operations on a large scale [1].

2) Identity theft: an attacker could manipulate, clone or steal the smart meter's identifier by tracking and observing the behavioral patterns of the consumers and the appliances being used, and could conduct real time spying and surveillance [5].

The two-way information flow between the consumer and the utility in the smart grid environment opens up several privacy issues. In this paper, we focus on the issue of privacy primarily related to the information on the consumer's energy usage. Some of the privacy concerns associated with smart grid consumers include [19]: the type of data collected from the consumer; the frequency of such collection; the future usage and disclosure of such data to other parties; what permissions will be needed to allow the collected data to be shared among other third parties; and any legal consequences related to any unauthorized disclosure or analysis of consumer information.

The rest of this paper is organized as follows. In Section 2, we review the privacy scheme of Marmol et al. [13] and we show its vulnerability to man-in-the-middle attacks. In Section 3, we propose an improved security solution that can mitigate these attacks. Section 4 presents a security analysis of our solution and Section 5 presents a second solution to mitigate man-in-the-middle attacks. Finally, our concluding remarks are presented in Section 6.

Privacy issues in the smart grid environment are being studied extensively at the moment [2, 3, 4, 8, 9, 12, 13, 16, 17]. In [19], we presented an analysis of most of the recently proposed smart grid privacy solutions and identify their strengths and weaknesses in terms of their implementation complexity, efficiency, robustness, and simplicity.

Recently, Marmol et al. proposed a Homomorphic encryption based solution to protect the privacy of smart grid customers. Homomorphic encryption [11] allows specific types of computations to be carried out on cipher text and obtains an encrypted result. It allows one to compute arbitrary functions over encrypted data without the decryption key. In [13], smart meters individually encrypt their requests with an encryption function that allows the energy supplier to decrypt their aggregation result with an aggregated key, but no one can decrypt them individually. An encryption mechanism with this property is known as additively Homomorphic encryption [13]. In this paper, we demonstrate that the solution proposed by Marmol et al. is not resilient against man-in-the-middle attacks and we extend Marmol's solution to counter these attacks.

The attacks described later cannot be avoided without establishing an authenticated and secure channel between the ES and each smart meter belonging to the group. In a recent publication [14], the authors propose establishing a Transport Layer Security (TLS) secure connection to authenticate the ES using digital certificates. After the ES has been authenticated and in order to avoid smart meters' profile creation, the authors opted to use anonymous credentials as a solution to ensure the privacy of smart meters. By using an anonymous credential scheme, the smart meters prove that they are entitled to send their requests. However, using TLS based certificate can affect the performance of memory-constrained systems. A key impediment to the adoption of TLS is the computational and memory constraints of smart meters. The authors do not take into consideration the memory overhead for the smart meters to execute TLS as well as the communication overhead related to the TLS negotiation. In contrast to the approach described in [14], our proposed solutions in this work can effectively prevent the attacks described later without introducing additional overheads when compared to [14].

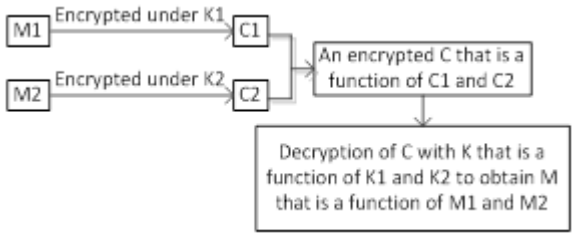


Figure 2: An example of two messages encrypted using Homomorphic encryption

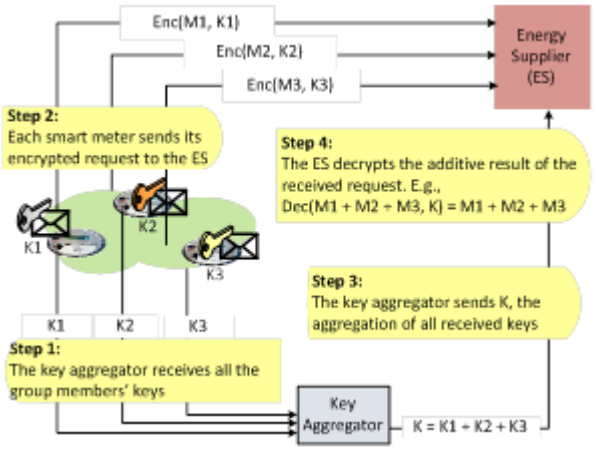


Figure 3: Basic privacy solution of Marmol et al.

2 Man-in-the-middle Attacks on the Privacy Scheme

In this section, we review Marmol et al. [13] privacy scheme for the smart grid and we show that the scheme they claimed to be secure against the man-in-the-middle attack is vulnerable to this attack. In their scheme, they use an additive Homomorphic encryption which allows specific types of computations to be carried out on cipher texts to obtain an encrypted result.

2.1 Homomorphic Encryption

It is usually impossible for someone without the decryption key to manipulate the underlying data in any useful way [7]. However, some encryption schemes are Homomorphic; they are based on specific types of computations on encrypted data and allow the manipulation of the encrypted data, even without knowing the secret key [7] used to encrypt the data. By applying this scheme for securing data from a group's nodes, each node encrypts its request (e.g., M1 and M2 in Figure 2) with a different key (e.g., K1 and K2) and sends the encrypted request (e.g., C1 and C2) to an aggregator node. The aggregator node does not need to individually decrypt the date received from the nodes. It performs a transformation (e.g., addition or multiplication) on the received requests and decrypts the obtained result (e.g., C) with the aggregation key (e.g., K). The aggregation key is computed from the secret keys used by the group's nodes to encrypt their data.

Homomorphic encryption is being used by many practical applications where privacy is required. It was initially proposed in the context of Electronic Voting [15] in order to prevent the identification of users based on application-layer information.

2.2 Review of Marmol et al. Scheme

Marmol et al. proposed forming multiple groups of smart meters; each group consists of several smart meters belonging to the same building/street and is limited to one Energy Supplier (ES). One smart meter is randomly designated as a key aggregator to receive the group members' keys (as shown in Figure 3). Each member of the group encrypts its request using its current key and sends the encrypted request to the *ES* which performs an addition on the received requests and decrypts the obtained result with the aggregation key received from the key aggregator. However, if a smart meter sends its key to the key aggregator but does not send the corresponding encrypted content to the *ES* (or vice and versa), the *ES* cannot decrypt the aggregate value and causing the whole process to fail.

To address this problem, the authors propose an additional mechanism called "tokens solution" that works as follows (as shown in Figure 4). Before aggregating the individual keys received from smart meters, the key aggregator generates a token for each key and sends them back to the corresponding smart meters. Each smart meter reports its encrypted request together with the received token to the ES. The *ES* sends an acknowledgement message for each request received with a valid token to the key aggregator and the key aggregator will aggregate only the keys which are acknowledged by the *ES* [13]. Next, the ES performs a transformation (e.g., addition) on the received requests and decrypts the obtained result with the aggregation key received from the key aggregator. Since the key aggregator is elected periodically, the possibility to match the smart meter and its request is limited. However, it is always possible to establish this match if the key aggregator and the *ES* collaborate with each other.

2.3 Man-in-the-middle Attacks on Marmol et al. Scheme

As we mentioned previously, the solution described in [13] is not effective in thwarting man-in-the-middle attacks. We describe two scenarios where man-in-the-middle attacks are possible. We also describe an impersonation attack scenario.

Scenario A. In this scenario, the attacker replaces the encrypted re-quest being transmitted from a particular smart meter (victim) to the *ES* with another

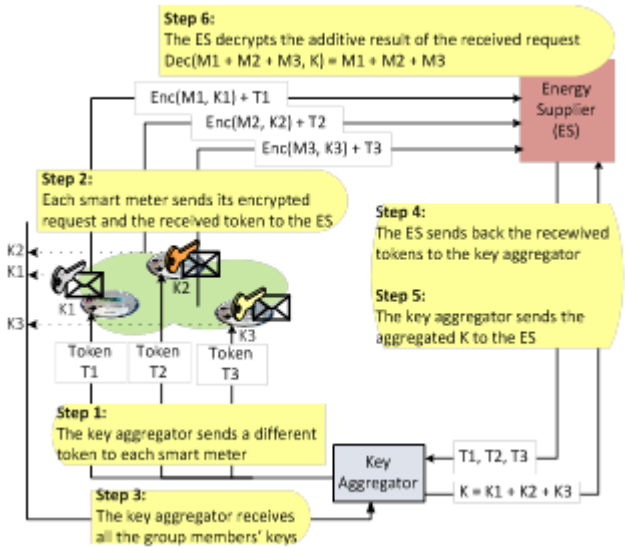


Figure 4: Enhanced privacy architecture of Marmol et al.

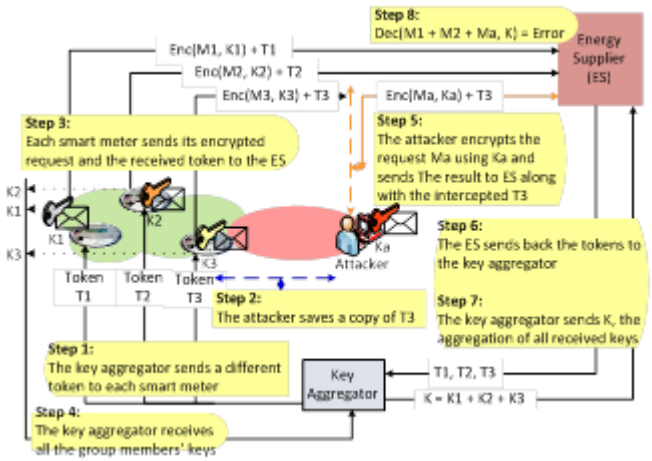


Figure 5: The man-in-the-middle attack on the privacy architecture proposed by Marmol et al.

request encrypted with a key that is never sent to the key aggregator (as shown in Figure 5). The attacker sends its encrypted request to the ES together with the token extracted from the request generated by the victim.

Next, the *ES* sends an acknowledgement message for the request received from the key aggregator. The key aggregator will consider the victim's key when aggregating the keys acknowledged by the ES. Hence, the *ES* will not be able to decrypt the additive result of the received requests and consequently, the entire process is compromised.

Scenario B. In this scenario, the man-in-the-middle attack intercepts the communication between the smart meter and the key aggregator and the communication between the same smart meter and the

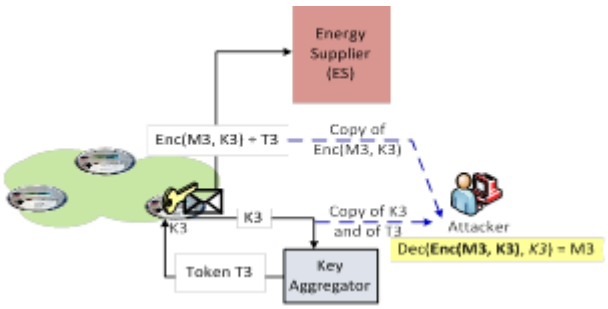


Figure 6: Another man-in-the-middle attack on Marmol et al.

ES (as shown in Figure 6). Since the smart the smart meter sends its key in clear text to the key aggregator, the attacker will be able to decrypt the encrypted request sent from the smart meter to the ES. Hence, the solution of [13] does not always guarantee the privacy of customers.

Impersonation Attack. An attacker spoofs the key aggregator and sends tickets to the group's members. By doing so, the attacker can let the group's members send their current keys to it. Since the current keys of the group's member are sent in clear text to the key aggregator, the attacker is able to compute the aggregation key and intercepts any future encrypted data being transmitted by the group's members to the *ES* or to the key aggregator.

3 Our Improved Privacy Solution

In this section, we describe our proposed solution to mitigate the possible attacks described above. Our solution uses a modified architecture of the solution proposed by Marmol et al. In our proposed privacy solution, the smart meters of the same group share the same key (key group) with the ES. The key group is generated by the *ES* and is installed on every smart meter of the same group (the installation could be done during the personalization phase of the smart meters).

3.1 Notations

The notations in Table 1 are used throughout this paper.

3.2 Overview of Our Proposed Solution

Before aggregating the individual keys received from smart meters, the key aggregator generates a token for each key and sends the tokens back to the corresponding smart meters. The token used by Marmol et al. is opaque or a string of data. In our architecture, we propose a semantic meaning for the token being used here. By semantic meaning we mean that the key aggregator

Table 1: Notations and definitions

Notation	Definition
$Dec(C, K)$	Decrypting the encrypted value C using the key K
$Enc(M, K)$	Encrypting the message M suing the key K
Entity	Smart meter, Energy Supplier, etc.
ES	Energy Supplier
$HMAC(SK, M)$	Calculating a message authentiction code (MAC) of the message M by using a hash function and a secret key SK
K	Aggregated key
KA	Key Aggragator
K_G	The group's key shared between all group's members
K_{sm}	A key generated by the smart meter sm
T_E	A token generated by the entity E
M_{sm}	A request generated by the smart meter
sm	sm smart meter
$\|\|$	Concatenation

will be authenticated which results in reducing the identity usurpation attacks. The token is generated as follows. The key aggregator generates a digest by applying the Keyed-Hashing for Message Authentication Code (HMAC) [10] on the token using the group key. Next, the key aggregator sends the digest along with the token to the smart meter. Upon receipt, the smart meter computes the HMAC and compares it with the received HMAC for equality (as shown in Figure 7).

Upon receipt of the token, each smart meter sm generates its key ksm, encrypts it along with the received token Tsm and sends the result back to the key aggregator (i.e., Enc(ksm —— Tsm, kG)). Next, the sm encrypts the Tsm and its request M_{sm} using the generated key ksm (i.e. Enc(M_{sm}, ksm)). Finally, the sm sends the encrypted value along with the digest value obtained by applying HMAC on the concatenation of the encrypted value and the token Tsm using the key group kG, as follows.

$$Enc(M_{sm}, k_{sm})||T_{sm}||HMAC(k_G, Enc(M_{sm}, k_{sm})||T_{sm}).$$

The HMAC value in the message being transmitted from the smart meter sm to the key aggregator authenticates the smart meter as a member of the group of authorized smart meters. Moreover, it detects falsified messages injected by man-in-the-middle attacks as we discuss later.

The ES computes the HMAC and then compares it with the received HMAC for equality (an attacker of scenario A and B described earlier cannot compute a valid HMAC without the key). Next, the ES collects the received tokens and sends them back to the key aggregator which then aggregates only the keys which are acknowledged by the ES to obtain the key K. During the key aggregation, the key aggregator decrypts only the encrypted values received from the smart meters and acknowledged by the ES. Finally, the key aggregator sends the aggregated key to the ES using a secure channel that could be established using the Transport Layer Security (TLS) or any other available security protocol.

3.3 Upgrading the Keys of Smart Meters

Marmol et al. define the bi-Homomorphic encryption as an encryption that is additive Homomorphic on both the plaintext and key spaces. For the key spaces, they define a mechanism based on the use of a ring to update their keys without changing the aggregated key (the aggregation of all the keys remains constant). To this end, each smart meter in the ring selects a random value and then subtracts this random value from its own key and at the same time sends that random value to its successor through a secure channel. The random value received from the predecessor is added to each smart meter's own key. Each random value added to one smart meter's key is therefore subtracted from another smart meter key's to keep the key K constant (the key K is updated every time one smart meter leaves/fails or enters/joins the group). However, the authors did not define the way to build the ring and did not specify the way a smart meter securely sends its random value to its successor. Moreover, it is not clear how the smart meters can be sure that the key update is successfully achieved.

Since each smart meter sends its updated key to the key aggregator, there is no need to use a ring and increase both the management and the computation overheads. We propose that every smart meter selects a random value and then subtracts this random value from its own key and at the same time sends update key and the selected random value to the key aggregator through a secure channel. Next, the key aggregator has the option of sending the sum of all received random values to the ES to update the aggregated key by subtracting the sum of the received random values from the current aggregated key K. If the objective of Marmol et al.'s proposal is to

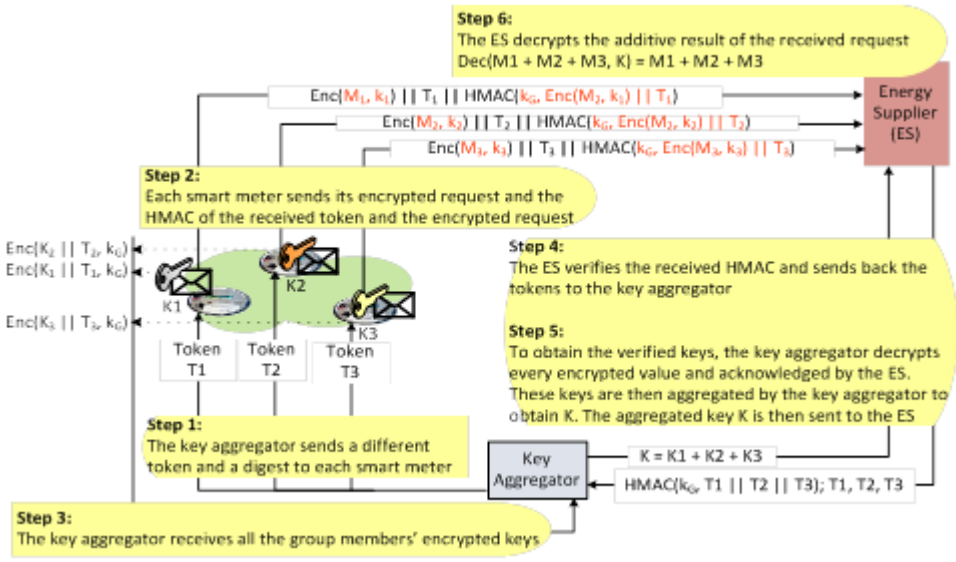


Figure 7: Our improved privacy solution

keep the unmodified key K constant, then the key aggregator selects one of the smart meters in the group and sends to it the sum of the received random values. The selected smart meter adds the received sum to its current key.

4 Security Analysis of Our Proposed Solution

In this section, we evaluate our proposed approach to demonstrate its effectiveness in maintaining data privacy and confidentiality. We also show that it is resilient against man-in-the-middle attacks and replay attacks.

4.1 Replay Attack

It may be possible for an attacker to read the data being transmitted from the group's members to the ES or to the key aggregator and save them for later use. However, it is useless for the attacker in both the scenarios A and B described earlier to use the token being transmitted from the key aggregator to a specific smart meter because the attacker needs to compute a correct HMAC operation that is applied on the fresh token and the secret key, an operation that is not possible if the attacker does not have the secret key.

4.2 Spoofing Attack

It is meaningless for the attacker to impersonate the key aggregator because it could learn nothing about the current keys of the group's members which are encrypted before being transmitted to the key aggregator. The attacker is unable to decrypt the current key of a smart meter without the group's key kG. Moreover, the group's members can verify the token's authenticity to avoid the impersonation attack described here.

4.3 Man-in-the-middle Attack

Our proposed solution mitigates both the man-in-the-middle scenarios A and B described earlier via the mutual authentication between smart meters and the ES and the key aggregator as well. Moreover, all the messages being exchanged between the entities are encrypted and HMACed using secret keys. Hence, it is not be possible for man-in-the-middle attacks to falsify the exchanged messages without being detected. If a man-in-the-middle-attack falsified the authenticated message being transmitted by a specific smart meter, only that specific smart meter would not be served, the ES would be able to serve the other group's members as long as the HMAC value in each of their requests is successfully verified. During the key aggregation phase, the key aggregator would omit the key of the victim and only those keys acknowledged by the ES would be considered. The proposal of Marmol et al. is not only ineffective in thwarting man-in-the-middle attacks but also fails when a single encrypted request is falsified by such attacks.

4.4 Analysis of Computational Costs and Comparison with Marmol et al. Scheme

We evaluate the performance of our improved privacy solution and compare it with the proposed approach of Marmol et al. Our solution introduces the use of HMAC to protect the encrypted requests and the tokens against man-in-the-middle attacks. Every smart meter performs one HMAC operation compared to Marmol et al. Moreover, every smart meter encrypts its key before being

transmitted to the key aggregator. On the ES side, one HMAC operation is needed to protect the list of verified tokens from any modification. Table 2 summarizes the additional crypto-graphic operations needed by our solution when compared to Marmol et al. In Table!2, t_e denotes a time to encrypt or decrypt a message by using a symmetric cryptosystem; t_{HNAC} denotes a time to execute one HMAC operation.

Table 2: Additional computational costs needed by our solution when compared to Marmol et al.

	Marmol et al.	Our improved solution
Each sm	$1t_e$	$2t_e + 1t_{HMAC}$
ES	$2t_e$	$(n+1)t_{HMAC}$
KA	$1t_e$	$nt_e + 1t_{HMAC}$
Total	$(n+3)t_e$	$3nt_e + 2(n+1)t_{HMAC}$

As shown in Table 2, our solution introduces more crypto-graphic operations when compared to Marmol et al. Each smart meter authenticates the key aggregator by verifying the HMAC value (i.e., the token) received from the key aggregator. Moreover, each smart meter performs a HMAC operation to link its encrypted request and the token received from the key aggregator in order to mitigate the man-in-the-middle attacks described above and to authenticate itself as a member of the group of authorized smart meters.

By deploying our solution, it is easy for the ES to identify the sender of a falsified or badly formatted request and asks that sender to resend its request again. This operation costs four HMAC operations; two of them are executed by the victim and the other two are executed by the ES. In the case of Marmol et al., if a single request is falsified, the ES will not be able to detect it or to identify the sender of that falsified request. Hence, the entire process will fail and none of the group's member will be served by the ES. As a result, all of the cryptographic operations should be repeated by the involved entities (i.e., $O(n+3)$ encryption operations).

5 A Second Solution to Mitigate Man-in-the-middle Attacks

We assume that smart meters within the same group form a ring in which every smart meter in the ring has only two neighbors - a clockwise one (upstream neighbor) and an anticlockwise one (downstream neighbor). Each smart meter sm shares its initial key IK_{sm} with the ES so the ES is able to compute the aggregated key K.

Every smart meter sm will compute a second key K_{sm} as follows. Every time a smart meter is designated as a key aggregator or when a smart meter leaves/fails or enters/joins the ring, a key update process is initiated by the key aggregator. To this end, each smart meter

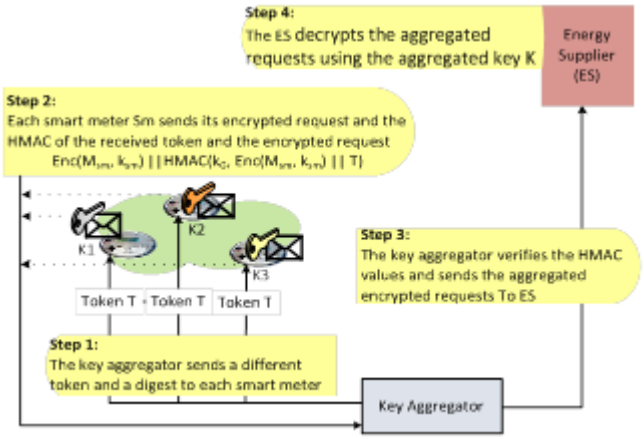


Figure 8: A second proposed solution

sm in the ring will generate a random value RV_{sm} and then subtracts it from the random value received from its downstream neighbor. The result obtained is added to its initial key IK_{sm} to obtain its current key K_{sm}. At the end of the process, the keys of the ring's members are updated but the aggregated key K is always constant. The key K_{sm} is used by sm to encrypt its requests.

Figure 8 summarizes the required steps to send the requests of the ring's members as follows:

Step 1. The key aggregator multicasts to the group's members a token T that could be generated and authenticated as shown in Figure 7.

Step 2. Each smart meter encrypts its request using its current key K_{sm} and performs a HMAC on its encrypted request and on T using the group's key kG.

Step 3. The key aggregator receives the encrypted requests and the HMAC values from the group's members. It individually verifies the HMAC values and in case a specific HMAC value is not true, the key aggregator will inform the concerned smart meter to resend its request and to compute a valid HMAC value. Next, the key aggregator aggregates the received encrypted requests and sends the obtained value to the ES through a secure channel.

Step 4. The ES decrypts the aggregated requests using the aggregated key K.

By using the above scheme, the key aggregator can individually verify the HMAC value of each smart meter in the ring. As a result, it is not possible to have an unexpected decryption error caused by man-in-the-middle attacks. Since the keys of the ring's members are updated every time a smart meter is designated as a key aggregator, matching the smart meter and its request is not possible in case the key aggregator and the ES are collaborating with each other.

We evaluate the performance of our second solution and we compare it with our first solution described ear-

Table 3: Additional computational cost needed by our 1^{st} and 2^{nd} solutions when compared to Marmol et al.

	Our 1^{st} solution	Our 2^{nd} solution
Each *sm*	$2t_e + 1t_{HMAC}$	$1t_e + 1t_{HMAC}$
ES	$(n+1)t_{HMAC}$	-
KA	$nt_e + 1t_{HMAC}$	nt_{HMAC}
Total	$3nt_e + 2(n+1)t_{HMAC}$	$nt_e + 2nt_{HMAC}$

lier. Table 3 summarizes the additional cryptographic operations needed by our second solution when compared to the first solution. In our second solution, the smart meters do not send their keys to the key aggregator and hence we save 2n encryption/decryption operations.

However, the key aggregator verifies n HMAC values received from the smart meters. Table 4 summarizes the performance comparison in terms of the communication overhead for the two proposed solutions. The analysis shows that our second solution reduces the number of exchanged messages by (n+1) messages.

6 Conclusion

In this paper, we first analyze Marmol et al.'s privacy scheme for the smart grid and we show that it is easily broken by man-in-the-middle attacks. To address the weaknesses resulting from such attacks, we propose an improved privacy solution which extends the scheme of Marmol et al. We show that our proposed extension is secure against replay attacks, man-in-the-middle attacks and provides mutual authentication. It also provides the Energy Supplier the ability to identify falsified smart meters' requests without revealing those smart meters' identities and without dropping the requests of other smart meters. Compared to Marmol et al.'s scheme, our smart grid privacy solution requires more symmetric encryption and HMAC operations. However, these operations have no considerable performance impact given the security robustness our extension provides.

Acknowledgments

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. AlMajali, A. Viswanathan, and C. Neuman, "Analyzing resiliency of the smart grid communication architectures under cyber attack," in *Proceedings of the Fifth Workshop on Cyber Security Experimentation and Test*, pp. 4, 2012.

[2] M. Badra and S. Zeadally, "Design and Performance analysis of a virtual ring architecture for smart grid privacy," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 321–329, 2014.

[3] M. Chen, C. Yang, and M. Hwang, "Privacy protection data access control," *International Journal of Network Security*, vol. 15, no. 6, pp. 411–419, 2013.

[4] S. Das, K. Kant, and N, Zhang, *Security and Privacy in the Smart Grid, Handbook on Security Cyber-Physical Critical Infrastructure*, Morgan Kaufmann, Chapter 25, Feb. 2012.

[5] C. Efthymiou, G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of the First IEEE International Conference on Smart Grid Communications*, pp. 238–243, 2010.

[6] Federal Energy Regulatory Commission, Assessment of Demand Response & Advanced Metering, Staff Report, 2008. (`http://www.ferc.gov/legal/staff-eports/demand-response.pdf`)

[7] C. Gentry, *Computing Arbitrary Functions of Encrypted Data*, 2008. (`http://crypto.stanford.edu/craig/easy-fhe.pdf`)

[8] Q. Jiang, J. Ma, G. Li, and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy," *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[9] W. Juang and J. Wu, "Efficient user authentication and key agreement with user privacy protection," *International Journal of Network Security*, vol. 7, no. 1, pp. 120–129, 2008.

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

[11] J. Liu, Y. Lu, and C. Koh, *Performance Analysis of Arithmetic Operations in Homomorphic Encryption*, 2010. (`http://docs.lib.purdue.edu`)

[12] 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 and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[13] F. Marmol, C. Sorge, O. Ugus, and G. Perez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Communications*, pp. 166–172, 2012.

[14] F. Marmol, C. Sorge, R. Petrlic, O. Ugus, D. Westhoff, and G. Perez, "Privacy-enhanced architecture for smart metering," *International Journal of Information Security*, vol. 12, no. 2, pp. 67–82, 2013.

[15] R. Rivest, *Lecture Notes 15: Voting, Homomorphic Encryption, Computer and Network Security*, 2002. (`http://web.mit.edu`)

[16] F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, "Smart grid privacy: Issues and solutions," in *Proceedings of Second International Workshop on Privacy, Security, and Trust in Mobile and Wireless Systems (MobiPST 2012)*, (held in conjunction with IEEE ICCCN 2012), Munich, Germany, July 2012.

Table 4: Communication overhead of our 1^{st} and 2^{nd} solutions and of Marmol et al. (Messages exchanged between X and Y ($X \leftrightarrow Y$))

	$KA \leftrightarrow sm$	$KA \leftrightarrow ES$	$sm \leftrightarrow ES$	Total
Marmol et al. Scheme	$2n$	2	n	$3n+2$
our 1^{st} solutions	$2n$	1	-	$2n+1$
our 2^{nd} solutions	$2n$	2	n	$3n+2$

[17] Y. Simmhan, A. Kumbhare, B. Cao, V. Prasanna, "An analysis of security and privacy issues in smart grid software architectures on clouds," in *Proceedings of IEEE International Conference on Cloud Computing*, pp. 582–589, 2011.

[18] U. S. Department of Energy, Advanced Metering Infrastructure, White paper by the NETL for U.S. DOE Office of Electricity Delivery and Energy Reliability, 2008.

[19] S. Zeadally, A. Pathan, C. Alcaraz, M. Badra, "Towards privacy protection in smart grid," *Wireless Personal Communications*, vol. 73, no. 1, pp. 23–50, 2013.

Mohamad Badra is an Assistant Professor at Zayed University, Abu Dhabi, UAE. He received a PhD degree in Networks and Computer Science from TLECOM ParisTECH. His research interests include key exchange, wireless/wired network security and privacy, public key infrastructures, smart cards, and wireless sensors networks. He is the author of several international standards on the security of exchanges and the co-author of many international conference and journal papers.

Sherali Zeadally is an Associate Professor at the College of Communication and Information, University of Kentucky, Lexington, KY, 40506, USA. He received his Bachelor's degree and Doctoral degree, both in Computer Science, from the University of Cambridge, England and the University of Buckingham, England respectively. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, England.

An Improved Lindell-Waisbard Private Web Search Scheme

Zhengjun Cao[1], Lihua Liu[2], Zhenzhen Yan[1]
(Corresponding author: Zhengjun Cao)
Department of Mathematics, Shanghai University[1]
No. 99, Shangda Road, Shanghai, China.
Department of Mathematics, Shanghai Maritime University[2]
No. 1550, Haigang Ave, Pudong New District, Shanghai, China.
(Email: caozhj@shu.edu.cn)
(Received May 27, 2015; revised and accepted Aug. 10 & Sept. 6, 2015)

Abstract

In 2010, Lindell and Waisbard proposed a private web search scheme for malicious adversaries. At the end of the scheme, each party obtains one search word and queries the search engine with the word. We remark that a malicious party could query the search engine with a fake word instead of the word obtained. The malicious party can link the true word to its provider if the victim publicly complain for the false searching result. To fix this drawback, each party has to broadcast all shares so as to enable every party to recover all search words and query the search engine with all these words. We also remark that, from a user's perspective, there is a very simple method to achieve the same purpose of private shuffle. When a user wants to privately query the search engine with a word, he can pick another $n-1$ padding words to form a group of n words and permute these words randomly. Finally, he queries the search engine with all these words.

Keywords: ElGamal encryption, private shuffle, private web search

1 Introduction

As we see private web search (PWS) has become a serious problem. There are several tricks to deal with it. The anonymous routing system [6] can be used though it is somewhat inefficient. So do the private information retrieval [4, 21] and mix-net [3, 5, 11]. In 2009, Castellà-Roca et al. [2] suggested a new approach for the problem.

Their proposal is for a group of users to shuffle their search words amongst themselves. After the shuffle, each user has someone's search word (but doesn't know whose), and each party then query the search engine with the word obtained. Finally, the parties all broadcast the result. Their private shuffle protocol is secure only in the presence of semi-honest adversaries.

At PETS'2010, Lindell and Waisbard [17] pointed out that the scheme suggested by [2] is unrealistic because it is vulnerable to many attacks. They proposed a private shuffle protocol for malicious adversaries and proved its security according to their security definition. They also addressed some practical considerations. But we would like to stress that at the end of the Lindell-Waisbard scheme, like the previous work [2], each party obtains only one search word and query the search engine with the word.

In this paper, we remark that in the Lindell-Waisbard private web search scheme a malicious party could query the search engine with a fake word instead of the word obtained. Thus the party corresponding to the true word cannot obtain the proper searching result.

More worse, the malicious party can link the true word to its provider if the victim publicly complain for the false searching result. However, the victim himself can not find who is the malicious party. To fix this drawback, each party has to broadcast all shares so as to enable every party to recover all search words and query the search engine with all these words. We also remark that from a user's perspective there is a very simple method to achieve the same purpose of private shuffle. Besides, we shall correct some misunderstandings about "denial of service" and "malicious attacks in cryptography".

The primitive of mix network is introduced by Chaum [3], which can be used for e-voting, e-auction and private web search. Loosely speaking, a mix network shuffles a number of inputting ciphertexts (each from one user) to the same number of outputting plaintexts such that: 1) the outputs are a permutation of the plaintexts of the inputs; 2) the permutation between the inputs and the outputs is unknown so that the users cannot be linked to their outputs.

Since then, researchers have put forth many proposals on mix network [1, 3, 5, 9, 10, 11, 20] and its applica-

tions [8, 15, 22, 24, 25, 26]. In recent, Juarez and Torra [12, 23] have studied the technique of dissociating privacy agent, which is a browser extension that acts as a proxy between the user and the search engine and semantically dissociates queries on real time. Romero-Tris et al. [23] have pointed out the differences between single-party PWS model and multi-party PWS model.

The anonymous routing system [6, 16, 18, 19] can be also used for private web search but it is somewhat inefficient for multi-party PWS. Recently, Li and Hwang [13, 14] have designed a lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks.

2 Review of the Lindell-Waisbard Private Web Search Scheme

A shuffle functionality is a probabilistic function $f(x_1, \cdots, x_n) = (y_1, \cdots, y_n)$, such that for every $i, y_i = x_{\pi(i)}$ where π is a random permutation over $\{1, 2, \cdots, n\}$. A shuffle is private if an adversary cannot link between the inputs and the outputs of the protocol.

Assume that all parties hold a unique session identifier *sid* (e.g., this could be a timestamp). There is a group $\mathbb{G}$ of order q with generator g, to be used for the ElGamal encryption [7]. Let (E, D) denote a CCA2-secure public-key encryption scheme. At the beginning of the scheme, each party P_j has a search word w_j, $j = 1, \cdots, n$. At the end of the scheme, each P_j obtains an arbitrary search word $w'_j \in \{w_1, \cdots, w_n\}$. The Lindell-Waisbard private web search scheme [17] can be described as follows.

Initialization stage.

1) Each party P_j chooses a random $\alpha_j \in \mathbb{Z}_q^*$, computes $h_j = g^{\alpha_j}$, and chooses a pair of keys (sk_j, pk_j) for the CCA2-secure encryption. P_j sends (h_j, pk_j) to all the other parties and proves knowledge of α_j. P_j signs the message and sends together with the identifier *sid* using its certified private signing key.
2) Each party verifies the signatures on the messages and the proofs that it received and aborts unless all are correct.
3) Each party P_j encrypts its input w_j using ElGamal with the public key $h = \prod_{i=1}^{n} h_i$. That is, it chooses a random $\rho_j \in \mathbb{Z}_q^*$ and computes an encryption
$$m_j = (g^{\rho_j}, h^{\rho_j} w_j).$$
4) Each party P_j computes
$$c_j = E_{pk_1}(E_{pk_2}(\cdots(E_{pk_n}(m_j))\cdots))$$
and sends c_j to P_1.

The output of this phase is the list of the encrypted c_j's, denoted by $\mu_0 = \langle c_1^0, \cdots, c_n^0 \rangle$.

Shuffle stage.

For $j = 1, \cdots, n$, P_j receives μ_{j-1} and computes μ_j as follows:

1) P_j checks that there are no duplications in μ_{j-1}. If there are, it aborts.
2) P_j decrypts every c_i^{j-1} in μ_{j-1} by computing
$$c_i^j = D_{sk_j}(c_i^{j-1}).$$
3) P_j randomly permutes the list of values c_i^j computed above. The result is denoted by μ_j.
4) P_j sends μ_j to P_{j+1}. The last party P_n sends μ_n to all parties.

Verification stage.

1) Every party P_j checks its ElGamal ciphertext m_j appears in the vector μ_n. If yes it sends $(sid, P_j, \textbf{true})$, signed with its private signing key, to all the other users. Otherwise it sends $(P_j, \textbf{false})$.
2) If P_j sent false in the previous step, or did not receive a validly signed message $(sid, P_i, \textbf{true})$ from all other parties P_i, then it aborts. Otherwise, it proceeds to the next step.

Reveal stage.

1) For every (u_i, v_i) in μ_n, P_j computes $s_i^j = u_i^{\alpha_j}$ and sends s_i^j to P_i.
2) Every party P_j computes
$$w'_j = \frac{v_j}{\prod_{k=1}^{n} s_j^k},$$
thereby decrypting the ElGamal ciphertext and recovering the search word w'_j (here j denotes the current index in μ_n and not the index of the party who had input w_j at the beginning of the protocol).

Query stage.

After the above shuffle, each party has someone's search word, and the parties then query the search engine with the word obtained. Finally, the parties all broadcast the result to all others.

We refer to Figure 1 for the basic idea behind the Lindell-Waisbard private web search scheme.

3 An Attack Launched by any Malicious Party in Query Stage

The Lindell-Waisbard private web search scheme is builded on the previous work [2]. They claim that the protocol is secure in the presence of malicious adversaries. We now remark that the scheme is vulnerable to an attack launched by any malicious party.

Table 1: Difference between the Lindell-Waisbard scheme and the modification

	The Lindell-Waisbard scheme	The modification
Reveal	For every (u_i, v_i) in μ_n, P_j computes $s_i^j = u_i^{\alpha_j}$ and sends s_i^j to P_i. Every party P_j computes w'_j.	For every (u_i, v_i) in μ_n, P_j computes $s_i^j = u_i^{\alpha_j}$ and broadcasts s_i^j and *the proof of* α_j to all others. Every party P_j checks the proofs and computes $w'_1, \cdots, w'_n$.
Query	Each party P_j queries the search engine with w'_j, and broadcasts the searching result.	Each party P_j queries the search engine with $w'_1, \cdots, w'_n$.

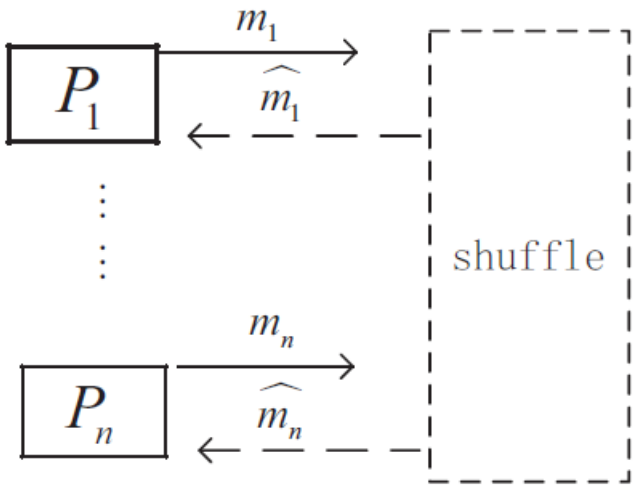


Figure 1: The Lindell-Waisbard shuffle

Suppose that P_k is a malicious party and the others are semi-honest. At the end of Reveal stage, P_k obtains a word w'_k which is in the set $\{w_1, \cdots, w_n\}$. In Query stage, P_k can query the search engine with an arbitrary word $\widehat{w_k}$ such that $\widehat{w_k} \neq w'_k$.

He broadcasts the searching result corresponding to the word $\widehat{w_k}$. Since the probability that $\widehat{w_k} \in \{w_1, \cdots, w_n\}$ is negligible, the party corresponding to the word w'_k shall not obtain the proper searching result. More worse, if the victim publicly complains for the false searching result, then P_k can link the true word w'_k to the victim. Note that the victim himself can not find who is the malicious party.

4 A Modification of the Lindell-Waisbard Scheme

The Lindell-Waisbard PWS scheme requires many broadcast channels. For example, each party P_j has to broadcast (h_j, pk_j) in Initialization stage, $(sid, P_j, \textbf{true})$ or $(P_j, \textbf{false})$ in Verification stage, and the searching result in Query stage. In view of that each party can access to these broadcast channels, in Reveal stage for every (u_i, v_i) in μ_n each party P_j can broadcast s_i^j to all others, instead of sending it to P_i in the mode of point-to-point. Hence, every party can recover all search words $w'_1, \cdots, w'_n$. Finally, every party can query the search engine with all these search words. See the following Table 1 for the differences between the original Lindell-Waisbard scheme and its modification.

The modification requires that P_j broadcasts the zero-knowledge proof of α_j with respect to u_i. The requirement cannot be removed. Otherwise, there exists a similar attack launched by any malicious party. Suppose that P_j is the malicious party and the others are semi-honest. In Reveal stage, P_j broadcasts $\widehat{s_i^j}$ such that $\widehat{s_i^j} \neq u_i^{\alpha_j}$ for some index i. Hence, the others shall obtain $w'_1, \cdots, \widehat{w'_i}, \cdots, w'_n$. If the party corresponding to w'_i complains for the false word $\widehat{w'_i}$, P_j can link the true word w'_i to the victim. However, the victim himself can not find who is the malicious party.

We refer to Figure 1 and Figure 2 for the essential differences between the original Lindell-Waisbard scheme and the modification.

5 A Simple Method for Single-party Private Web Search

The essence of a private shuffle protocol is to mix a user's search word with another $n-1$ words such that an adversary cannot know which is the user's true search word. In fact, from a user's perspective there is a very simple method to achieve the same purpose. Concretely, when a user wants to privately query the search engine with a word, he first chooses $n-1$ padding words to form a group of n words and then permutes these words. Finally, he queries the search engine with these words. Figure 3 is a simple private web search method.

It is easy to see that the simple scheme is secure be-

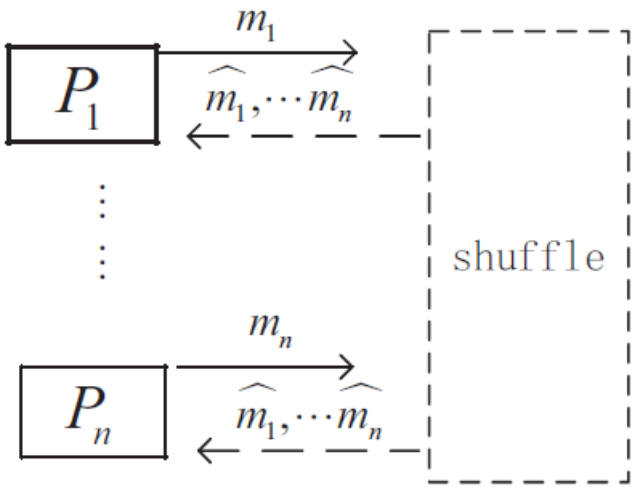


Figure 2: The modified Lindell-Waisbard shuffle

cause the adversary can know the true word with the probability of $1/n$. In comparison with the modified Lindell-Waisbard scheme, the simple method requires relatively little cost.

6 Further Discussions

We have received some comments on the manuscript. Somebody argues that

> *The attack proposed could be viewed as a type of denial of service where a malicious party always complains in the protocol, causing the whole session to abort. The last simple fix does not work because one will know all the words are from the same user, and as long as one of the words is sensitive, it is linked to that user. The correctness guarantee is not required for the Lindell-Waisbard scheme, and as such malicious parties are allowed to perform denial of service type attacks (the attack mentioned above is one such attack).*

We now want to point out that:

- Their security model has actually considered replacement attacks but they did not pay attentions to the proposed malicious attack in the paper. It points out in the introduction that [17]: "we still have to deal with 'replacement attacks' where the first party carrying out the mix replaces all of the encrypted search words with terms of its own, except for the one ciphertext belonging to the user under attack."

- In the Lindell-Waisbard scheme, it is very likely to happen that a malicious adversary changes the search word from others when submitting it to a search engine. This is because: 1) his malicious behavior cannot be detected by others so that he does not undertake any obligations; 2) the false searching result broadcasted could tempt the victim to complain.

- The last simple fix is helpful to explain the essence of Lindell-Waisbard Scheme. From each user's point of view, the Lindell-Waisbard shuffle scheme is just mixing his searching word with other $n-1$ words submitted by other $n-1$ users. We do not consider whether an adversary can find a "sensitive" word among these n words. Actually, it is difficult to define the term of "sensitive" in the scenario.

- The replacement attack cannot be falsely regarded as a type of "denial of service", because it takes place just at the end of the whole session. In such case, users can obtain proper searching results, except for the victim.

7 Conclusion

We show that there is a drawback in the Lindell-Waisbard private web search scheme. We also remark that from a user's perspective there is a very simple method to achieve the same purpose of the Lindell-Waisbard scheme. This paper, we think, is helpful to explain the gist of Lindell-Waisbard private shuffle and correct some misunderstandings about "denial of service" and "malicious attacks in cryptography".

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

References

[1] M. Abe, "Mix-networks on permutation net-works," in *Proceedings of Advances in Cryptology (ASIACRYPT'98)*, pp. 258–273, Beijing, China, Oct. 1998.

[2] J. Castellà-Roca, A. Viejo, and J. Herrera-Joancomarti, "Preserving user's privacy in web search engines," *Computer Communications*, vol. 32, no. 13-14, pp. 1541–1551, 2009.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of the ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[5] Y. Desmedt and K. Kurosawa, "How to break a practical mix and design a new one," in *Proceedings of Advances in Cryptology (EUROCRYPT'00)*, pp. 557–572, Bruges, Belgium, May 2000.

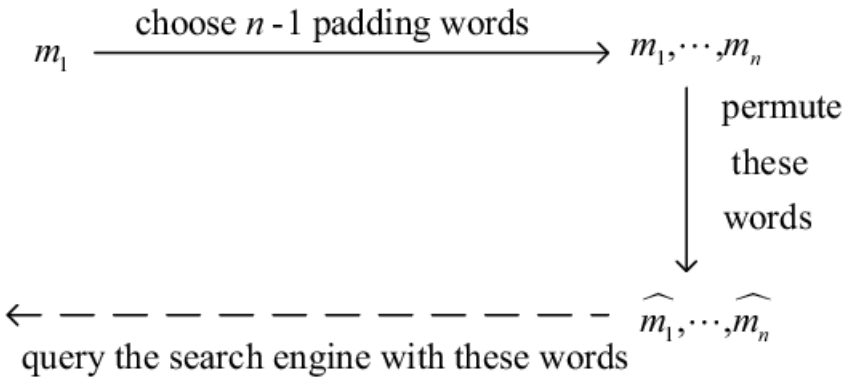


Figure 3: A simple private web search method

[6] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, pp. 303–320, San Diego, CA, USA, Aug. 2004.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of Advances in Cryptology (CRYPTO'84)*, pp. 10–18, Santa Barbara, California, USA, Aug. 1984.

[8] T. H. Feng, W. T. Li, and M. S. Hwang, "A false data report filtering scheme in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 17, no. 3, pp. 229–236, 2015.

[9] J. Furukawa and K. Sako, "An efficient scheme for proving a shuffle," in *Proceedings of Advances in Cryptology (CRYPTO'01)*, pp. 368–387, Santa Barbara, California, USA, Aug. 2001.

[10] J. Groth, "A verifiable secret shuffle of homomorphic encryptions," *Journal of Cryptology*, vol. 23, no. 4, pp. 546–579, 2010.

[11] M. Jakobsson, "A practical mix," in *Proceedings of Advances in Cryptology (EUROCRYPT'98)*, pp. 448–461, Espoo, Finland, June 1998.

[12] M. Juarez and V. Torra, "Dispa: An intelligent agent for private web search," *Studies in Computational Intelligence*, vol. 567, pp. 389–405, 2015.

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

[14] C. T. Li, C. C. Yang, and M. S. Hwang, "A secure routing protocol with node selfishness resistance in manets," *International Journal of Mobile Communications*, no. 10, pp. 103–118, 2012.

[15] W. T. Li, T. H. Feng, and M. S. Hwang, "Distributed detecting node replication attacks in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.

[16] X. D. Lin and et al., "Asrpake: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," in *Proceedings of IEEE International Conference on Communications (ICC'07)*, pp. 5333–5347, Glasgow, Scotland, June 2007.

[17] Y. Lindell and E. Waisbard, "Private web search with malicious adversaries," in *Proceedings of Privacy Enhancing Technologies, 10th International Symposium (PETS'10)*, pp. 220–235, Berlin, Germany, July 2010.

[18] R. X. Lu, Z. F. Cao, L. C. Wang, and C. K. Sun, "A secure anonymous routing protocol with authenticated key exchange for ad hoc networks," *Computer Standards and Interfaces*, vol. 29, no. 5, pp. 521–527, 2007.

[19] R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," *International Journal of Network Security*, vol. 16, no. 3, pp. 182–192, 2014.

[20] C. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of ACM Conference on Computer and Communications Security 2001*, pp. 116–125, Philadelphia, USA, Nov. 2001.

[21] R. Ostrovsky and W. Skeith, "A survey of single-database pir: Techniques and applications," in *Proceedings of 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC'07)*, pp. 393–411, Beijing, China, Apr. 2007.

[22] S. Patel, D. Punjani, and D. Jinwala, "An efficient approach for privacy preserving distributed clustering in semi-honest model using elliptic curve cryptography," *International Journal of Network Security*, vol. 17, no. 3, pp. 328–339, 2015.

[23] C. Romero-Tris, A. Viejo, and J. Castella-Roca, "Multi-party methods for privacy-preserving web search: Survey and contributions," *Studies in Computational Intelligence*, vol. 567, pp. 367–387, 2015.

[24] S. Sarpong, C. X. Xu, and X. J. Zhang, "An authenticated privacy-preseving attribute matchmakng protocol for mobile social networks," *International Journal of Network Security*, vol. 17, no. 3, pp. 357–364, 2015.

[25] F. Wang, C. C. Chang, and Y. C. Chou, "Group authentication and group key distribution for ad hoc

networks," *International Journal of Network Security*, vol. 17, no. 2, pp. 199–207, 2015.

[26] T. J. Wei, "Communication efficient shuffle for mental poker protocols," *Information Sciences*, vol. 181, pp. 5053–5066, 2011.

Zhengjun Cao is an associate professor of department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Department of Computer Science, University Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Lihua Liu is an associate professor of department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhenzhen Yan is currently pursuing her M.S. degree from Department of Mathematics, Shanghai University. Her research interests include information security and cryptography.

A New Digital Signature Scheme from Layered Cellular Automata

Xing Zhang[1], Rongxing Lu[2], Hong Zhang[1], Chungen Xu[3]
(Corresponding author: Rongxing Lu)

School of Computer Sciences and Engineering, Nanjing University of Science and Technology[1]
No. 200, Xiaolingwei Street, Nanjing, Jiangsu 210094, P.R. China
School of Electrical and Electronic Engineering, Nanyang Technological University[2]
50 Nanyang Avenue, 639798 Singapore
School of Science, Nanjing University of Science and Technology[3]
(Email: rxlu@ntu.edu.sg)
(Received Apr. 25, 2014; revised and accepted Aug. 25 & Nov. 27, 2014)

Abstract

Cellular Automata (CA) is one of the important tools to design cryptographic algorithms, and in the past years many researchers have explored several cryptographic algorithms based on CA. However, most of reported CA-based cryptographic algorithms focus on the symmetric key encryption schemes and few CA-based asymmetric encryption scheme has been proposed, let alone the CA-based digital signature scheme. In this paper, to fill this gap, we present a new digital signature scheme based on the layered CA technique. Specifically, in the proposed layered CA-based digital signature scheme, we combine the transition rules of some one-dimensional (1D) reversible CAs to generate the rules of a two-dimensional (2D) CA, where the reverse of the 1D transition rules are kept as the private key and the 2D transition rules are set as the corresponding public key. Based on the hardness assumption of the layered CA reversibility (LCAR) problem, we formally prove the proposed scheme is semantically secure against chosen-message attack in the random oracle model.

Keywords: Digital signature, layered cellular automata, reversible cellular automata, T-shaped neighborhood

1 Introduction

Digital signature is an indispensable technique in modern information security system [20]. In particular, a digital signature is a mathematical tool for demonstrating the authenticity of a digital message. A valid signature can give a recipient reason to believe that the message was created by a known signer, such that the signer cannot deny having signed the message (i.e., authentication) and the message not changed in transit (i.e., integrity) [18, 21]. Therefore, digital signatures have been widely used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering today.

Applying cellular automata (CA) tool to design cryptographic algorithms is a promising technique in modern cryptography. CA can be regarded as a discrete model that consists of a number of individual cells, each cell exists several states and will change its state based on the states of its neighboring cells by following a prescribed rule. In general, the overall structure can be viewed as a parallel processing device. However, the simple structure will produce complex patterns when iterated several times. Since most CA can be implanted on very fast hardware and software, as well as its inherent features like parallelism, locality and homogeneity, CA has become an important tool to design cryptographic algorithms.

While most of the investigations of CA-based cryptographic algorithms have been focused on traditional symmetric cryptosystems, few CA-based public key cryptosystem has been found in the literature [5, 11, 15, 24], and let alone the CA-based digital signature scheme. Therefore, there is a high desire to design a CA-based digital signature in the complement of existing RSA and ElGamal signatures [8, 19, 25].

In this paper, to fill this gap, we would like to present a new digital signature scheme based on the layered CA technique [2, 12, 23, 28]. Specifically, in the proposed CA-based digital signature scheme, we will combine the transition rules of some one-dimensional (1D) reversible CAs to generate the rules of a two-dimensional (2D) CA, where the reverse of the 1D transition rules are kept as the private key and the 2D transition rules are set as the corresponding public key. Based on the hardness assumption of the layered CA reversibility (LCAR) problem, we formally prove the proposed scheme is semantically secure against chosen-message attack in the random oracle

model [3].

The remainder of this paper is organized as follows. In Section 2, some preliminaries are introduced, including some notations, the foundations of digital signature, and the concept of the cellular automata and its corresponding security assumption. In Section 3, we present our layered cellular automata based signature scheme, followed by security analysis in Section 4, and a simple example in Section 5. In Section 6, we analyze the strengths of the proposed signature scheme. Finally, we draw our conclusions in Section 7.

2 Preliminaries

2.1 Notations

Let $\mathbb{N} = \{1, 2, 3 \ldots\}$ be the set of positive integers. If x is a string , then $|x|$ denotes its length, while if $\mathbb{S}$ is a set then $|\mathbb{S}|$ denotes its cardinality. If $k \in \mathbb{N}$ then 1^k denotes the string k ones. If $\mathbb{S}$ is a set then $s \xleftarrow{R} \mathbb{S}$ denotes the operation of picking a random element s of $\mathbb{S}$ uniformly.

2.2 Foundations of Digital Signature

A digital signature (DS) scheme consists of three algorithms: Key Generation, Signature Generation, and Signature Verification.

- Key Generation (KG): On input of an unary string 1^k with security parameter k, KG outputs a public and private key pair (pk, sk). Here, KG is a randomized algorithm in digital signature.
- Signature Generation (SG): On input of a message m, the public and private key pair (pk, sk), SG outputs a signature σ of m with respective to the public key pk. Note that, SG here is referred as a deterministic algorithm [25]; when SG is randomized one, some random input should also be included [8].
- Signature Verification (SV): On input of a purported signature σ of m with respective to the public key pk, SV outputs "1" if (m, σ) is valid, and "0" otherwise. Note that, SV must be a deterministic algorithm in digital signature.

The above algorithms must satisfy the standard consistency constraint of the digital signature. That is, if a signature $\sigma \leftarrow SG(m, pk, sk)$ is generated, then we must have "1" $\leftarrow SV(\sigma, m, pk)$.

Security Model of Digital Signature. For digital signatures, the well-known strong security notion is existential forgery against adaptive chosen message attacks (EF-CMA) presented by Goldwasser [9] et al.

In the random oracle model [6], we consider the most powerful adversary $\mathcal{A}$ as follows: i) $\mathcal{A}$ is allowed to access to the signing oracle $\mathcal{O}_S$ and the random oracle $\mathcal{O}_H$; ii) $\mathcal{A}$ returns a new valid signature $\sigma^\star$ on message $m^\star$, with a natural restriction that the signature $\sigma^\star$ has not been obtained from the signing oracle $\mathcal{O}_S$ before.

Definition 1 (Unforgeability). *Let DS be a digital signature, and $\mathcal{A}$ be an EF-CMA adversary against DS. We consider the following random experiments, where k is the security parameter:*

$$\begin{aligned} &\text{Experiment } \mathbf{Exp}^{\mathsf{EF\text{-}CMA}}_{\mathsf{DS},\mathcal{A}}(k) \\ &\quad (pk, sk) \leftarrow KG(k), \\ &\quad (\sigma^\star, m^\star) \leftarrow \mathcal{A}^{\mathcal{O}_H, \mathcal{O}_S}(pk) \\ &\quad \text{return } SV(pk, \sigma^\star, m^\star) \end{aligned}$$

We define the success probability of $\mathcal{A}$ via

$$\mathbf{Succ}^{\mathsf{EF\text{-}CMA}}_{\mathsf{DS},\mathcal{A}}(k) = \Pr[\mathbf{Exp}^{\mathsf{EF\text{-}CMA}}_{\mathsf{DS},\mathcal{A}}(k) = 1]$$

Let $\tau \in \mathbb{N}, \epsilon \in [0, 1]$, we say that DS is (τ, ϵ)-secure if no EF-CMA adversary $\mathcal{A}$ running in time τ has a success $\mathbf{Succ}^{\mathsf{EF\text{-}CMA}}_{\mathsf{DS},\mathcal{A}}(k) \geq \epsilon$.

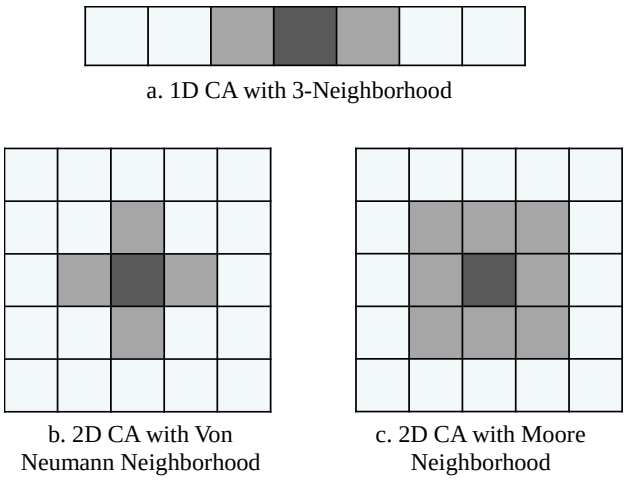
2.3 Concepts of Cellular Automata

2.3.1 Basis of Cellular Automata

A Cellular Automata (CA) is a discrete model in which space and time are discrete, and consists of grids of cells in which each cell can exist in a finite number of states. All cells change their states synchronously, according to a predefined transition rule that specifies the new state of each cell based on the old states of the cell and its neighboring cells. As CA exhibits some inherent features like parallelism, locality, simplicity, unpredictability and homogeneity, it is naturally efficient in its hardware and software implementations [28].

Formally, a CA is often defined by a quadruple $\{D, S, N, f\}$ with the dimension D , the state set S , the neighboring states set N, and the transition rule f.

- Dimension D: define the dimension of CA, which can be one-dimensional (1D) or two-dimensional (2D), and a d-dimensional ($d \in \mathbb{N}$) CA consists of a d-dimensional array of identical cells [15]. Most of existing studies of CA are focused on 1D and 2D CA [1, 4, 13, 14, 26, 27] as shown in Figure 1.
- State Set S: define a set of possible states of all cells in a CA, which is often defined as the sets, such as $S_1 = \{0, 1\}$, $S_2 = \{0, 1, 2, \ldots\}$, and $S_3 = \{white, black\}$.
- Neighboring States N: define a set of neighboring states based on the existing neighborhood structures. Currently, the most popular structures are 3-neighborhood, Von Neumann and Moore neighborhood [28], as shown in Figure 1.
- Transition Rule f: define a transition map $f : S \rightarrow S$ as the transition rule from one state to another.



a. 1D CA with 3-Neighborhood

b. 2D CA with Von Neumann Neighborhood

c. 2D CA with Moore Neighborhood

Figure 1: Typical neighborhood structure of CA with radius $r = 1$

Let $s_i^t \in S$ denote as the state of the i-th cell at t time step and $s_i^{t+1} \in S$ be the state of the i cell at $t+1$ time step. Then, the states of all cells in a CA at t time step can be denoted as $S^t = (s_0^t, s_1^t, \cdots, s_i^t, \cdots)$, also called a configuration. As the state of each cell at the next time step s_i^{t+1} is determined by the transition rule along with its current state s_i^t and states of its neighboring cells, we can represent s_i^{t+1} by the following formula:

$$s_i^{t+1} = f(s_{i-r}^t, \cdots, s_{i-1}^t, s_i^t, s_{i+1}^t, \cdots, s_{i+r}^t)$$

where r denotes its neighborhood radius.

Boundary Conditions. Though a CA is an infinite system, it should be finite-dimensional in practical applications. As a result, it is crucial to define the boundary conditions of a CA. Currently, the boundary conditions, including periodic boundary condition, mapped boundary condition, and fixed boundary [30], are mostly considered in CA systems, as shown in Figure 2. Since the periodic boundary comes closest to simulate an infinite lattice, it has been widely suggested in many CA systems.

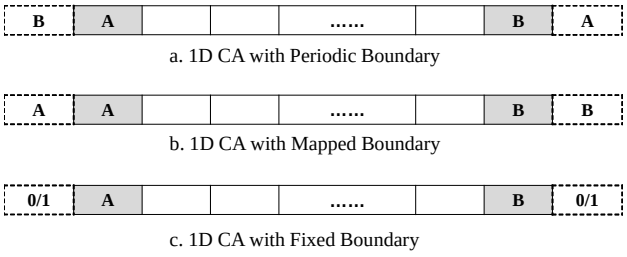
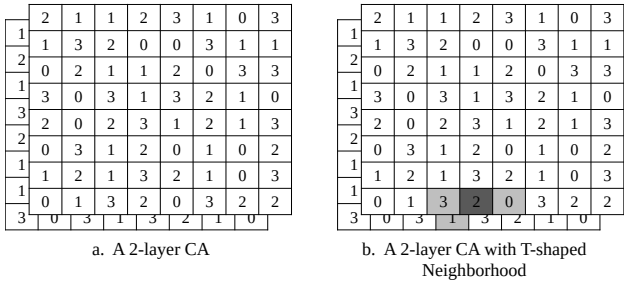


Figure 2: 1D CA with different boundaries, where "A" is the leftmost cell state, "B" is the rightmost cell state, and "0/1" is the fixed cell state.

Reversibility. If the transition rule of a CA is reversible, we say the CA is Reversible CA (RCA)[16]. Otherwise, the CA is called irreversible. In specific, a CA is reversible, if and only if each configuration has only one succeeding state and one preceding state. Due to the reversibility, many RCA systems have been designed for symmetric cryptosystems [5, 7, 17, 26, 29], where the same transition rule serves as the secret key applying into both encryption and decryption operations. However, irreversible CA, due to irreversibility, is not as popular as the RCA in designing CA-based cryptosystems.

2.3.2 Layered Cellular Automata

Layered CA (LCA) is a special CA, which can be regarded as a highly parallel system consisting of layers and each layer is formed by rows of 1D CA, as shown in Figure 3. The stacked structure of LCA enables the cells in LCA to hold more complex and various neighborhoods, which has brought more theoretical interest [2, 12, 23, 28]. Jaberi et al. [12] use two-layer CA to imitate Pseudo-Neumann neighborhood structure and generate trackable random numbers. Kishore et al. [28] propose a block encryption scheme by using a 8-layer CA, which observably possesses better confusion and diffusion properties compared with the well-known AES [22].



a. A 2-layer CA

b. A 2-layer CA with T-shaped Neighborhood

Figure 3: 2-layer CA with 1-radius T-shaped neighborhood.

A 2-layer CA with 1-radius T-shaped neighborhood is shown in Figure 3, where the state of each cell is changed based on not only itself and its left and right neighbors, but also the cell at the same position in the other layer. This neighborhood structure unites two layers of the CA as a unified system, which can effectively improve the diffusion property. In this work, we will present a new digital signature scheme based on the LCA with T-shaped neighborhood structure.

Security Assumption. In order to construct a new digital signature scheme from the layered cellular automata, we should define the computational hard problem on which we can rely. Kari [15] has proven that the reversibility of 2D CA is undecidable, i.e., there does not exist any efficient algorithm that can decide whether a given two-dimensional transition rule is reversible or not [16]. Thus, for a given 2D transition rule, we can't decide its reversibility, and then we also can't compute its reverse. The 2D transition rule of a 2-layer CA can be constructed from

several 1D reversible transition rules [5]. Given these 1D reversible transition rules, we can generate the 2D transition rule and the 2-layer CA is reversible. However, only given the 2D transition rule, we cannot gain these 1D reversible transition rules, and the 2-layer CA is irreversible. We call it as LCA Reversibility (LCAR) Problem.

Definition 2 (LCAR Problem). *Let $f_i : S_1 \to S_1$, $i \in \{1, 2, 3, \ldots, n\}$, be n reversible transition rules of 1D RCAs, where S_1 is state set of these RCAs. Define $f_{ca} : S_2 \to S_2$ be the transition rule of a 2-layer CA, where S_2 is state set of the 2-layer CA, and f_{ca} is constructed by the compound operations of transition rules f_i, $i \in \{1, 2, 3, \ldots, n\}$, i.e., $f_{ca} = f_1 \circ f_2 \circ \cdots \circ f_n$, and then we set $S_2 = S_1$. Given any configuration $S_2^t = (s_0^t, s_1^t, \cdots, s_i^t, \cdots)$ of time t of the 2-layer CA, where $s_i^t \in S_2$, we evolve S_2^t by the transition rule f_{ca}, and obtain $S_2^{t+1} = f_{ca}(S_2^t)$. The LCAR problem is that for given (S_2^{t+1}, f_{ca}), computing S_2^t is impossible.*

Base on the above problem, we give the security assumption of LCA as follows.

Definition 3 (LCAR Assumption). *Given any configuration $S_2^t = (s_0^t, s_1^t, \cdots, s_i^t, \cdots)$ of a 2-Layer CA, we evolve S_2^t by the transition rule f_{ca} and obtain $S_2^{t+1} = f_{ca}(S_2^t)$. Let $\mathcal{A}$ be a probabilistic polynomial-time (PPT) adversary, which takes (S_2^{t+1}, f_{ca}) as input and outputs S_2^t. We consider the following random experiment on LCAR problem of LCA:*

Experiment $\mathbf{Exp}_{\mathcal{A}}^{LCAR}$
$S_2^{t+1} \leftarrow f_{ca}(S_2^t)$,
$S_2^\star \leftarrow \mathcal{A}(S_2^{t+1}, f_{ca})$
if $S_2^\star = S_2^t$, return 1; and return 0 otherwise

We define the success probability of $\mathcal{A}$ via

$$\mathbf{Succ}_{\mathcal{A}}^{LCAR} = \Pr[\mathbf{Exp}_{\mathcal{A}}^{LCAR} = 1]$$

Let $\tau \in \mathbb{N}, \epsilon \in [0, 1]$, we say that LCAR is (τ, ϵ)-secure if no PPT adversary $\mathcal{A}$ running in time τ has a success $\mathbf{Succ}_{\mathcal{A}}^{LCAR} \geq \epsilon$.

3 Proposed LCA-based Digital Signature Scheme

In this section, we propose our digital signature scheme based on CA with T-shaped neighborhood, which mainly consists of three algorithms, namely: Key Generation (KG), Signature Generation (SG), and Signature Verification(SV).

- **KG**: Given a security parameter $k \in \mathbb{N}$. First, we define some 1D RCAs with periodic boundary, labeled CA_1, CA_2,..., CA_n, and $CA_i = (1, S_1, N_r, f_i)$, for $i \in \{1, 2, \ldots, n\}$, where state set $S_1 = \{0, 1, 2, 3\}$ and N_r is the neighboring state set with radius r. The transition rule $f_i : S_1 \to S_1$, for $1 \leq i \leq n$ of the reversible CA_i is reversible, and the reverse rule of f_i, denoted f_i^{-1}, is also the map between the state set S_1, i.e. $f_i^{-1} : S_1 \to S_1$, for $1 \leq i \leq n$.

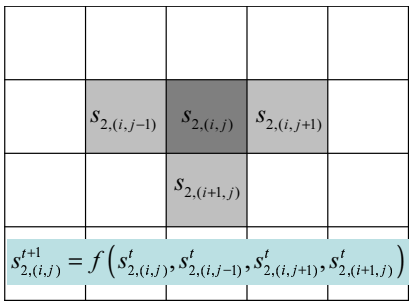


Figure 4: 2D CA with 1-radius T-shaped neighborhood, where $s_{2,(i,j)}^t$ denotes the state of the cell at i-th row j-column.

Next, we define a 2-layer CA also with periodic boundary, denoted by $CA' = (2, S_2, N', f_{ca})$, where the state set $S_2 = \{0, 1, 2, 3\} = S_1$ and the transition rule f_{ca} is constructed by the compound operations of transition rules f_i, $i \in \{1, 2, \ldots, n\}$, i.e.,

$$f_{ca} = f_1 \circ f_2 \circ \cdots \circ f_n$$

The neighborhood structure of CA' is set as T-shaped neighborhood with radius $r' = 1$. In addition, we set each layer in the 2-layer CA has 64 cells, and then the 2-layer CA has total 128 cells. Specifically, we use f_i to generate the 2D transition rule f_{ca} by a 2D CA with 1-radius T-shaped neighborhood structure, as shown in Figure 4. We define the states of the cells in the CA are come from S_2, and let

$$S_{2,(i,j)}^t = (s_{2,(i,j-1)}^t, s_{2,(i,j)}^t, s_{2,(i,j+1)}^t, s_{2,(i+1,j)}^t)$$

denote the configuration of the cell at i-th row j-column at time t, where $s_{2,(i,j)}^t \in S_2$. As each cell has four possible states and together with three neighbors, there are total $4^4 = 256$ possible configurations of each cell. Take each configuration as the input of the compound operations $f_{ca} = f_1 \circ f_2 \circ \cdots \circ f_n$, the corresponding output is the new state of the central cell. This procedure can be presented as follows:

we first compute

$$s_{1,(i,j)}^{t+n} = f_n(f_{n-1}(\cdots(f_2(f_1(S_{1,(i,j)}^t)))))$$

and then let $S_{2,(i,j)}^t = S_{1,(i,j)}^t$ and $s_{2,(i,j)}^{t+1} = s_{1,(i,j)}^{t+n}$, where $s_{1,(i,j)}^{t+n} \in S_1, s_{2,(i,j)}^{t+1} \in S_2$. Since

$$f_{ca} = f_1 \circ f_2 \circ \cdots \circ f_n$$

we have

$$s_{2,(i,j)}^{t+1} = f_{ca}(S_{2,(i,j)}^t)$$

The map $f_{ca} : S^t_{2,(i,j)} \to s^{t+1}_{2,(i,j)}$ is the 2D transition rule we need. We define a function $F_{ca} : S_1 \to S_1$, where $F_{ca} = f_n^{-1} \circ \cdots \circ f_2^{-1} \circ f_1^{-1}$ and set the private key as $sk = F_{ca}$.

It is obvious that $f_{ca} = (F_{ca})^{-1}$, i.e., given the f_i^{-1}, for $i = 1, 2, \cdots, n$, f_{ca} is reversible and we can compute its reverse. However, if we only know the 2D transition rule f_{ca}, we cannot decide its reversibility, to say nothing of computing its reverse. Therefore, we set the f_{ca} as the corresponding public key pk, i.e., $pk = f_{ca}$.

Let $\mathbb{S}$ denote the message space, owing to the 2-layer CA with 128 cells, the size of $\mathbb{S}$ is $|S_1|^{128} = 4^{128} = 2^{256}$, where $|S_1|$ is the cardinality of the state set S_1, the message space is large enough to against exhaustive attack. Besides, we define a secure one-way hash function H, where $H : \{0,1\}^* \to \mathbb{S}$.

- **SG**: On input of a message m, we compute R_1 and R_2, where

$$R_1 = H(m) \in \mathbb{S}$$
$$R_2 = F^k_{ca}(R_1) \in \mathbb{S}$$

i.e. $H(m)$ is evolved by the transition rules in the private key $sk = F_{ca}$ for k times, where $k \in \mathbb{N}$ is a large security parameter. Then we set the signature of m as $\sigma = R_2$.

- **SV**: For the message m and a purported signature σ, together with the public key $pk = f_{ca}$ and security parameter k, we compute R'_1, where

$$R'_1 = f^k_{ca}(\sigma) = f^k_{ca}(R_2) = (f_1 \circ f_2 \circ \cdots \circ f_n)^k(R_2)$$

Then, we check the following equality

$$R'_1 = H(m)$$

If it does hold, output '1', the signature σ will be accepted, and rejected otherwise.

4 Security Analysis

In this section, we will formally prove our proposed signature scheme satisfies the requirements stated in Section 2.2.

Theorem 1. *Let $\mathcal{A}$ be an adversary which can produce an existential forgery under chosen-message attacks [10] within a time τ and success probability ϵ, after q_H and q_S queries to the hash function H (modeled as random oracle $\mathcal{O}_H$) and the signing oracle $\mathcal{O}_S$ respectively. The LCAR problem can be resolved with another probability ϵ' within time τ', where $\epsilon' \approx \frac{1}{q_h+q_s+1}\epsilon$, $\tau' = \tau + (q_h + q_s + 1) \cdot \Theta$ with Θ the time for an $f^k_{ca}(\cdot)$ computation.*

Proof. We define a sequence of games $\mathbf{G_1}, \mathbf{G_2}, \cdots$, of modified attack games starting from the actual game $\mathbf{G_0}$. Then, with these incremental games, we reduce a LCAR problem instance (i.e. given f_{ca} and S^{t+1}_2, where $S^{t+1}_2 = f_{ca}(S^t_2)$, compute S^t_2) to an attack against the proposed signature scheme. We show that the adversary $\mathcal{A}$ can help us to resolve the LCAR problem.

GAME $\mathbf{G_0}$. This is an actual game, in the random oracle model [3]. The adversary $\mathcal{A}$ is allowed to access a random oracle $\mathcal{O}_H$ and a signing oracle $\mathcal{O}_S$. Moreover, the public key $pk = f_{ca}$ is also available to $\mathcal{A}$.

To break the signature scheme, the adversary $\mathcal{A}$ outputs its forgery $(\sigma^\star, m^\star)$ that $m^\star$ has not been asked for $\mathcal{O}_S$, one then checks whether it is a valid signature or not. Note that the adversary $\mathcal{A}$ asks q_s queries to the signing oracle $\mathcal{O}_S$ and q_h queries to the random oracle $\mathcal{O}_H$, at most $q_s + q_h + 1$ queries are asked to the random oracle during this game, since each signing query may make such a new query, and the last verification step does too. We set $\mathbf{Forge}_0$ denotes the event that the forged signature is valid, and set the same notation $\mathbf{Forge}_n$ in any game $\mathbf{G_n}$. By definition, the success probability ϵ can be represented as follows:

$$\epsilon = \mathbf{Succ}^{\mathsf{EF\text{-}CMA}}_{\mathsf{DS},\mathcal{A}} = \Pr[\mathbf{Forge}_0]$$

GAME $\mathbf{G_1}$. In this game, we will simulate the hash oracle $\mathcal{O}_H$ by maintaining a hash list $L_{\mathcal{H}}$.

For a new hash query $\mathcal{O}_H(m)$, we randomly choose a new random element $r \in \mathbb{S}$, create and append a record $(m, h = f^k_{ca}(r), r)$ in $L_{\mathcal{H}}$, and respond with $H(m) = h$.

In order to implant the challenge $S^{t+1}_2 = f_{ca}(S^t_2)$ into the hash answer, for some query on m^*, we insert a record $(m^*, h^* = f^{k-1}_{ca}(S^{t+1}_2), \sqcup)$ into the list $L_{\mathcal{H}}$, and respond with $H(m^*) = h^*$.

From the above simulation, we can see this game is indistinguishable from the actual attack. Consequently,

$$\Pr[\mathbf{Forge}_1] = \Pr[\mathbf{Forge}_0]$$

GAME $\mathbf{G_2}$. In this game, we simulate the signing oracle $\mathcal{O}_S$. For a signing query $\mathcal{O}_S(m)$, if $m \neq m^*$, we first look up the record $(m, h = f^k_{ca}(r), r)$ in $L_{\mathcal{H}}$, and return $\sigma = r$ as the signature to the adversary $\mathcal{A}$. In the eye of $\mathcal{A}$, $\sigma = r$ is valid, as it satisfies the verification equation.

However, if $m = m^*$, the corresponding record in $L_{\mathcal{H}}$ is $(m^*, h^* = f^{k-1}_{ca}(S^{t+1}_2), \sqcup)$, we cannot return a valid value. Thus, we have to terminate the game and report failure.

Unless the signing query fails, this game is indistinguishable from the previous game. Therefore,

$$\Pr[\mathbf{Forge}_2] = (1 - \frac{1}{q_h + q_s + 1})^{q_s} \Pr[\mathbf{Forge}_1]$$

GAME $\mathbf{G_3}$. In this game, we take a close look at the valid forgery $(\sigma^\star, m^\star)$. If $m^\star \neq m^*$, we have to terminate the game again, as the returned is irrelevant to the implanted challenge. However, $m^\star = m^*$, we can convert the adversary $\mathcal{A}$'s capability to solve the challenge " given f_{ca} and S_2^{t+1}, where $S_2^{t+1} = f_{ca}(S_2^t)$, compute S_2^t" as follows.

Since $\sigma^\star$ is valid, i.e., $f_{ca}^k(\sigma^\star) = f_{ca}^{k-1}(S_2^{t+1})$, we calculate $S_2^t = \sigma^\star$ as the challenge. Therefore, we have

$$\mathbf{Succ}_{\mathcal{A}}^{\mathsf{LCAR}} = \Pr[\mathbf{Forge}_3]$$

By observing $\mathbf{G_3}$ and $\mathbf{G_2}$, we can see $\mathbf{G_3}$ won't terminate unless $m^\star = m^*$. Therefore, we have

$$\Pr[\mathbf{Forge}_3] = \frac{1}{1+q_h}\Pr[\mathbf{Forge}_2]$$

As mentioned in **GAME $\mathbf{G_0}$**, the success probability of attacking the signature scheme is

$$\mathbf{Succ}_{\mathsf{DS},\mathcal{A}}^{\mathsf{EF\text{-}CMA}} = Pr[\mathbf{Forge}_0] = \epsilon.$$

By combining all above games, we have

$$\begin{aligned}\epsilon' =& \mathbf{Succ}_{\mathcal{A}}^{\mathsf{LCAR}} = \Pr[\mathbf{Forge}_3]\\ =& \frac{1}{1+q_h}\Pr[\mathbf{Forge}_2]\\ =& \frac{1}{1+q_h}(1-\frac{1}{q_h+q_s+1})^{q_s}\Pr[\mathbf{Forge}_1]\\ \approx& \frac{1}{q_h+q_s+1}\cdot\epsilon\end{aligned}$$

Besides, there are total q_h+q_s+1 operations of computing $f_{ca}^k(\cdot)$ in the above games, thus it costs $(q_h+q_s+1)\Theta$. Plus the time τ of running the adversary $\mathcal{A}$, the time τ' of resolving LCAR problem is bounded by $\tau+(q_h+q_s+1)\Theta$ in the end. Thus, this completes the proof. □

5 A Simple Example

In this section, we give a simple example to demonstrate the feasibility of our proposed signature scheme. We use the transition rules of three 1D RCAs to generate the rules of a 2D CA with T-shaped neighborhood. And set the reverse rules of the 1D transition rules as the private key and the constructed 2D rules as the corresponding public key. Then we use the private key to generate signature and the public key to verify whether the signature is valid or not.

- **KG**: First, we choose a security parameter $k = 3$, in fact, k should be a large number, but here we only choose a small one to simply demonstrate our scheme. We define three 1D RCAs, labeled CA_1, CA_2 and CA_3, and $CA_i = (1, S_1, N_r, f_i)$, for $i \in \{1,2,3\}$, where state set $S_1 = \{0,1,2,3\}$ and N_r is the neighboring state set with radius $r = 1/2$. The reversible transition rule $f_i : S_1 \to S_1$, $i \in \{1,2,3\}$ is shown in Table 1.

  It can be proved that rule f_1, f_2 and f_3 all self-reversible, i.e. the reverse of f_i is itself, $f_i^{-1} = f_i$. Since the radius of 1D RCA is 1/2, there is only one neighbor in its neighborhood besides itself, for each cell in 1D RCA, we set the right one besides it as its neighbor. In addition, we specify a direction for each f_i, it is shown in Figure 5.

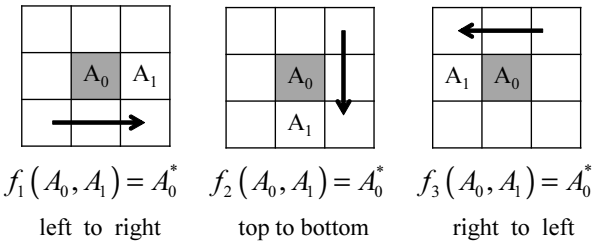


Figure 5: The neighborhood and direction of three 1D rules, where A_0 is the state of central cell and A_1 is the state of its neighbor, A_0^* is the new state of central cell.

Then we define a 2-layer CA also with periodic boundary, denoted by $CA' = (2, S_2, N', f_{ca})$, where $S_2 = \{0,1,2,3\}$ and the neighborhood structure of CA' is set as T-shaped neighborhood with radius $r' = 1$. The transition rule f_{ca} constructed by the compound operations of transition rules f_i, $i \in \{1,2,3\}$, i.e.

$$f_{ca} = f_1 \circ f_2 \circ f_3$$

Specifically, we first define a $S_{2,(i,j)}^t$, where

$$S_{2,(i,j)}^t = (s_{2,(i,j-1)}^t, s_{2,(i,j)}^t, s_{2,(i,j+1)}^t, s_{2,(i+1,j)}^t)$$

denotes the configuration of the cell at i-th row j-column at time t, and $s_{2,(i,j)}^t \in S_2$. Take each possible configuration $S_{2,(i,j)}^t$ as the input of the compound operations $f_{ca} = f_1 \circ f_2 \circ f_3$, the corresponding output is the new state of the central cell.

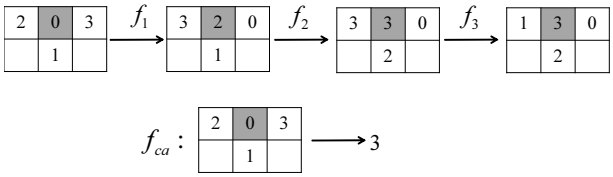


Figure 6: A example of generating a 2D transition rule

There is a concrete example of the rule generation process in Figure 6, and $f_{ca} : 2031 \to 3$ is a 1-radius 2D rule. Table 2 shown some 2D rules generated in this algorithm.

Next, we define a function $F_{ca} : S_1 \to S_1$, where $F_{ca} = f_3^{-1} \circ f_2^{-1} \circ f_1^{-1}$, and set it as the private key

Table 1: The reversible transition rules of three 1D RCAs

(s_i^t, s_{i+1}^t) \ s_i^{t+1}	f_1	f_2	f_3
00	1	0	2
01	0	1	1
02	3	0	3
03	2	2	0
10	0	1	3
11	2	0	0
12	2	2	1
13	3	3	2
20	3	3	0
21	1	3	3
22	1	1	2
23	0	0	1
30	2	2	1
31	3	2	2
32	0	3	0
33	1	1	3

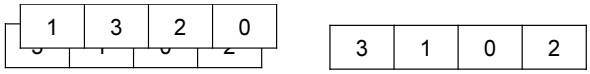
Table 2: Part of the generated 1-radius 2D rules, f_{ca} : $S^t_{2,(i,j)} \rightarrow s^{t+1}_{2,(i,j)}$

$S^t_{2,(i,j)} \rightarrow s^{t+1}_{2,(i,j)}$	$S^t_{2,(i,j)} \rightarrow s^{t+1}_{2,(i,j)}$	$S^t_{2,(i,j)} \rightarrow s^{t+1}_{2,(i,j)}$
$0133 \rightarrow 3$	$1232 \rightarrow 3$	$3221 \rightarrow 2$
$1321 \rightarrow 2$	$2330 \rightarrow 3$	$2222 \rightarrow 3$
$3200 \rightarrow 0$	$1313 \rightarrow 2$	$2210 \rightarrow 0$
$2012 \rightarrow 0$	$3121 \rightarrow 3$	$2121 \rightarrow 2$
$2311 \rightarrow 0$	$3202 \rightarrow 1$	$1122 \rightarrow 1$
$3103 \rightarrow 1$	$2033 \rightarrow 0$	$1202 \rightarrow 0$
$1022 \rightarrow 1$	$0313 \rightarrow 1$	$2012 \rightarrow 0$
$0230 \rightarrow 0$	$3121 \rightarrow 3$	$1012 \rightarrow 2$

of the signature scheme, i.e. $sk = F_{ca}$, set f_{ca} as the public key pk, i.e. $pk = f_{ca}$.

Besides, we define a secure one-way hash function H, where $H : \{0,1\}^* \rightarrow \mathbb{S}$, $\mathbb{S}$ denotes the message space of the signature scheme.

- **SG**: For a message $m = 01100101$ and security parameter $k = 3$, we first compute $R_1 = H(m) = 13203102$, and arrange the 13203102 into a 2-layer CA, which has four cells in each layer, as shown in Figure 7. Then, for each cell in the 2-layer CA, taking its configuration as the input of the function $F_{ca} = f_3^{-1} \circ f_2^{-1} \circ f_1^{-1} = f_3 \circ f_2 \circ f_1$, and evolved $k = 3$ times, the corresponding output is its new state, all new states make up of the signature. So, the signature of m is $\sigma = F^3_{ca}(R_1) = 12322113$.



(a). The structure of 2-layer CA (b). The second layer

Figure 7: 2-layer CA

- **SV**: For the message $m = 01100101$ and a signature $\sigma = 12322113$, together with the public key $pk = f_{ca}$ and security parameter $k = 3$, we compute R'_1, where

$$R'_1 = f^3_{ca}(\sigma) = f^3_{ca}(12322113) = 13203102.$$

It is obvious that the following equality is hold, so the signature $\sigma = 12322113$ is valid.

$$R'_1 = H(m).$$

6 Comparison

The simple example in the last section has shown the feasibility of the proposed signature scheme. In this section, we will exhibit its strengths by giving a comparison between the proposed scheme and RSA signature algorithm.

Table 3: The key space and timing analysis between the proposed scheme and RSA, where 1D and 2D denote the 1D and 2D CAs used in **KG** algorithm, respectively

	State number	Radius		Key space	Time (ms)
		1D	2D		
The proposed scheme	2	$r = 1$	$r' = 1$	2^{16}	
			$r' = 2$	2^{128}	15.6
			$r' = 3$	2^{1024}	218.4
	4	$r = \frac{1}{2}$	$r' = 1$	2^{512}	31
			$r' = 2$	2^{32768}	4274
RSA				2^{1024}	4708

Since the number and radius of the CAs in our proposed signature scheme are not appointed, we can achieve different size key space by changing the radius and state

Table 4: Average execution time for the proposed scheme and RSA-1024

	proposed scheme	RSA-1024
Signature	3.91 ms	4.26 ms
Verification	2.35 ms	2.77 ms

number. In the proposed scheme, we use n reversible rules of some 1D CAs with r-radius to generate the transition rule of a 4-state and r'-radius 2D CA, so there will be $4^{4^{(3r'+1)}}$ possible rules generated as the public key, i.e. the size of the key space is $4^{4^{(3r'+1)}}$. Of course, the state number can be changed according to the concrete applications. Table 3 shows the different key space size and the time of generating the public key with the state number and radius r and r' changed. It's observed that we can get a larger key space in less time when compared with RSA-1024.

Because the key space of the RSA-1024 algorithm is 2^{1024}, as well as the plaintext space and the ciphertext space, here we set $n = 4$, $r' = 3$ and the state number is 2 such that the key space of the proposed scheme is $2^{2^{(3r'+1)}} = 2^{1024}$. Now, we randomly choose 100 messages from the plaintext space and sign them to get the signatures, and then verify these signatures. All the signature and verification processes are executed by the RSA-1024 and the proposed scheme on an Intel Core 2 Duo 2.0 GHZ, in C++ platform. The average execution time of the 100 signature and verification processes are calculated separately and the results are tabulated in Table 4. It's obvious that the time taken by our proposed signature scheme is less than RSA-1024 algorithm, which obviously shows the efficiency of our proposed signature scheme.

7 Conclusions

In this paper, we have formally defined the digital signature, then proposed a new CA-based digital signature scheme based on the hardness assumption of the LCAR problem. We use the transition rules of some 1D RCAs to construct the transition rules of a 2D CA, as the reversibility of 2D CA is undecidable, we set the constructed 2D transition rules as the public key, the rules of 1D RCAs as the private key. And we have formally shown the proposed signature scheme is semantically secure against chosen-message attacks in the oracle model. Moreover, the proposed scheme is developed with a simple example, and analysis of the key space and efficiency are also carried out along with RSA-1024 algorithm, the results show that the proposed signature scheme is more efficient than RSA-1024.

References

[1] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 1, pp. 136–147, 2013.

[2] R. Ayanzadeh, K. Hassani, Y. Moghaddas, H. Gheiby, and S. Setayeshi, "Multi-layer cellular automata for generating normal random numbers," in *IEEE 18th Iranian Conference on Electrical Engineering (ICEE'10)*, pp. 495–500, 2010.

[3] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.

[4] Z. Cinkir, H. Akin, and I. Siap, "Reversibility of 1D cellular automata with periodic boundary over finite fields $\mathbb{Z}_p$," *Journal of Statistical Physics*, vol. 143, no. 4, pp. 807–823, 2011.

[5] A. Clarridge and K. Salomaa, "A cryptosystem based on the composition of reversible cellular automata," in *Language and Automata Theory and Applications*, pp. 314–325, Springer, 2009.

[6] J. Coron, J. Patarin, and Y. Seurin, "The random oracle model and the ideal cipher model are equivalent," in *Advances in Cryptology (CRYPTO'08)*, pp. 1–20, Springer, 2008.

[7] D. Das and A. Ray, "A parallel encryption algorithm for block ciphers based on reversible programmable cellular automata," *arXiv preprint arXiv:1006.2822*, 2010.

[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology*, pp. 10–18, Springer, 1985.

[9] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[10] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[11] H. Gutowitz, "Cryptography with dynamical systems," in *Cellular Automata and Cooperative Systems*, pp. 237–274, Springer, 1993.

[12] A. Jaberi, R. Ayanzadeh, and A. Z. Mousavi, "Two-layer cellular automata based cryptography," *Trends in Applied Sciences Research*, vol. 7, no. 1, pp. 68–77, 2012.

[13] N. Jamil, R. Mahmood, M. R. Zába, Z. A. Zukamaen, and N. I. Udzir, "An observation of cryptographic properties of 256 one-dimensional cellular automata rules," in *Informatics Engineering and Information Science*, pp. 409–420, Springer, 2011.

[14] J. Jin, "An image encryption based on elementary cellular automata," *Optics and Lasers in Engineering*, vol. 50, no. 12, pp. 1836–1843, 2012.

[15] J. Kari, *Cryptosystems Based on Reversible Cellular Automata*, Manuscript, Apr. 16, 1992. (`http://users.utu.fi/jkari/CACryptoScanned.pdf`)
[16] J. Kari, "Reversibility and surjectivity problems of cellular automata," *Journal of Computer and System Sciences*, vol. 48, no. 1, pp. 149–182, 1994.
[17] J. Kari, "Undecidable properties on the dynamics of reversible one-dimensional cellular automata," in *Proceedings of the First Symposium on Cellular Automata'Journées Automates Cellulaires'*, pp. 3–14, 2008.
[18] R. S. Katti and R. G. Kavasseri, "Nonce generation for the digital signature standard," *International Journal of Network Security*, vol. 11, no. 1, pp. 20–29, 2010.
[19] C. Yu Liu, C. C. Lee, and T. C. Lin, "Cryptanalysis of an efficient deniable authentication protocol based on generalized elgamal signature scheme," *International Journal of Network Security*, vol. 12, no. 1, pp. 58–60, 2011.
[20] R. Lu and Z. Cao, "A directed signature scheme based on rsa assumption.," *International Journal of Network Security*, vol. 2, no. 3, pp. 182–186, 2006.
[21] N. A. Moldovyan, "Blind signature protocols from digital signature standards," *International Journal of Network Security*, vol. 13, no. 1, pp. 22–30, 2011.
[22] NIST, *Advanced Encryption Standard*, Federal Information Processing Standard, FIPS-197, vol. 12, 2001.
[23] C. S. Rao, S. R. Attada, M. J. Rao, and K. N. Rao, "Implementation of object oriented encryption system using layered cellular automata.," *International Journal of Engineering Science & Technology*, vol. 3, no. 7, 2011.
[24] P. R. Piedras, "Cellular automaton public-key cryptosystem," *Complex Systems*, vol. 1, pp. 51–57, 1987.
[25] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[26] M. Seredynski and P. Bouvry, "Block encryption using reversible cellular automata," in *Cellular Automata*, pp. 785–792, Springer, 2004.
[27] S. Ho Shin, D. S. Kim, and K. Y. Yoo, "A 2-dimensional cellular automata pseudorandom number generator with non-linear neighborhood relationship," in *Networked Digital Technologies*, pp. 355–368, Springer, 2012.
[28] J. N. Rao, and A. C. Singh, "A novel encryption system using layered cellular automata," *International Journal of Engineering Research and Applications*, vol. 2, no. 6, pp. 912–917, 2012.
[29] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.
[30] S. Wolfram, *A New Kind of Science*, Wolfram Media Champaign, 2002.

Xing Zhang received the B.S.degree from Xuchang University, China, in 2010. From 2010 to now, she is working her Ph.D. degree in Computer Application from Nanjing University of Science and Technology (NUST), Jiangsu, China. During the period from November 2013 to May 2014, she was also a visiting Ph.D. student at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Her research interests include information security and cryptography, and the encryption scheme based on cellular automata.

Rongxing Lu received the Ph.D degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006 and the Ph.D. degree (awarded Canada Governor General Gold Medal) in electrical and computer engineering from the University of Waterloo, Waterloo, Ontario, Canada, in 2012. Since May 2013, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, as an Assistant Professor. His research interests include computer, network and communication security, applied cryptography, security and privacy analysis for vehicular network, eHealthcare system, and smart grid communications. He won the IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award in 2013.

Hong Zhang is a professor in the Department of Computer Science, Nanjing University of Science and Technology. His current interests are in the areas of theory and technology of information security, data mining and network fault diagnosis.

Chungen Xu received the M.S. degree from East China Normal University, Shanghai, China, in 1996 and the Ph.D degree from Nanjing University of Science and Technology in 2003. He is a professor in the Department of Applied Mathematics, School of Sciences, Nanjing University of Science and Technology. His current interests are in the areas of computer and network security, cryptography and coding.

An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card

Tanmoy Maitra[1], Ruhul Amin[2], Debasis Giri[3], and P. D. Srivastava[4]
(Corresponding author: Tanmoy Maitra)

Department of Computer Science & Engineering, Jadavpur University, Kolkata-700032, India[1]
Department of Computer Science & Engineering, Indian Schools of Mines University, Dhanbad-826004, Jharkhand, India[2]
Department of Computer Science & Engineering, Haldia Institute of Technology, Haldia-721657, India[3]
Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur-721302, India[4]
(Email: *tanmoy.maitra@live.com*) *(Received May 13, 2014; revised and accepted Aug. 20 & Nov. 3, 2014)*

Abstract

The cluster heads in hierarchical wireless sensor networks gather real time data from the other ordinary sensor nodes and send those data to a nearest base station. But, the main important issue is that how a user will get the real time data directly from a cluster head securely. To solve this problem, many user authentication schemes have been proposed in literature. In 2012, Das et al. proposed a dynamic password-based user authentication scheme for hierarchical wireless sensor networks and showed that their scheme is secure against all possible attacks. In this paper, we have pointed out that Das et al.'s scheme is insecure against insider attack, theft attack and session key recovery attack, and their scheme also suffers from dynamic cluster head addition overhead problem, limited number of cluster heads access problem and clock synchronization problem. To overcome these drawbacks, we have proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card in this paper. We have also shown that our scheme provides better tread-off among security and communication overhead compare to the Das et al.'s scheme.

Keywords: Authentication, Password, Smart Card, HWSN

1 Introduction

There are no proper ad hoc infrastructures in wireless sensor networks where a large number of sensor nodes are deployed by truck or plane on a target field. After deployment of sensor nodes, they communicate to other neighboring nodes within their communication range to form clusters. After that, one cluster head or gateway node is selected by base station or sensor nodes for each cluster on the basis of energy, signal strength, degree, capability, mobility etc. All the sensor nodes sense raw data from environment and send to their nearest cluster head by single-hop or multi-hop communication [21]. Cluster heads gather the raw data and send to nearest base station or sink node by multi-hop or single-hop communication [21]. Finally, data are collected from base station. The collected data is not always real time data because all cluster heads send data to base station after a certain periodic time. But, there is needed to collect real time data for taking immediate action in some application like Defense Advanced Research Project Agency (DARPA) [2]. If we collect data directly from cluster heads, we can get real time data. This is possible if it is allowed to access those real time data directly from cluster head, when demanded. Hence, it is needed to first authorize the accessors and then allows to access to do secure communication among accessors and cluster heads [7]. It should be noted that user authentication in wireless sensor networks satisfies all the following requirements:

1) Users can freely choose and update their passwords.
2) Low computational, storage and communication cost.
3) Session key agreements between cluster head and user.
4) Mutual authentication between users and base station and also between base station and cluster head.
5) Prevention of possible attacks.
6) Without maintaining password verification tables at server end.

The main goal in this paper is to design authentication scheme in such a manner that the designed protocol is better tread-off among security and communication cost than the previously published scheme. There exist many user authentication protocols in literature for wireless sensor network [3–5, 8, 9, 11, 14, 22–27].

In 2004, Watro et al. [25] proposed a user authentication scheme for wireless sensor networks, called Tinypk based on RSA [19] and Diffie-Hellman [6] protocols. In 2006, Wong et al. [26] described a user authentication scheme based on one way hash function and password. In 2007, Tseng et al. [22] proposed a dynamic user authentication scheme for wireless sensor networks. In 2009, Vaidya et al. [24] showed that Wong et al.'s scheme [26] suffers from forgery and replay attack, and Tseng et al.'s scheme [22] cannot thwart replay attack and man-in-the-middle (MITM) attack. Vaidya et al. [24] also proposed a robust dynamic user authentication scheme for wireless sensor networks. In the same year, M.L. Das [5] proposed an improved efficient scheme over Wong et al.'s scheme [26] based on user password and time stamp. But in 2010, Khan and Alghathbar [11] showed that M.L. Das's scheme [5] is insecure against gate-way node bypassing attack and privileged-insider attack. In 2010, He et al. [9] proposed an improved scheme over M.L. Das's scheme [5]. Later, Vaidya et al. [23] pointed out the insider attack and impersonation attack in both M.L. Das' scheme [5] and Khan and Alghathbar's scheme [11] and also proposed an improved two-factor user authentication scheme. In the same year, Fan et al. [8] proposed a user authentication scheme for two-tiered [13] wireless sensor networks. In 2010, Yuan et al. [27] pointed out that Watro et al.'s scheme [25] cannot resist forgery attack and proposed a biometric-based user authentication scheme for wireless sensor networks which is similar concept as in M.L. Das's scheme [5]. In 2011, Kumar and Lee [14] pointed out that He et al.'s scheme [9] is susceptible to information leakage attack and scheme [9] cannot preserve user anonymity, mutual authentication between a sensor and a user and does not establish the session key between the user and the sensor node. Kumar and Lee [14] also pointed out that Khan and Alghathbar's scheme [11] does not provide mutual authentication between the sensor and the user and does not establish the session key between the user and the sensor node with no confidentiality to their air messages.

In 2012, Das et al. [4] proposed a dynamic password-based user authentication scheme for hierarchical wireless sensor networks. In this paper, we have pointed out that their scheme is insecure against some attacks such as insider attack and session key recovery attack. Further, it is noted that base station uses user's secret parameter in the user's registration phase which is impossible. Additionally, their scheme suffers from dynamic cluster head addition overhead problem, limited number of cluster head access problem and clock synchronization problem. To overcome their weaknesses, we have proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. Our scheme provides better security with low computational over head and low communication cost than Das et al.'s scheme [4].

The remainder of this paper is organized as follows: Section 2 shows network model concept. Section 3 shows brief review of Das et al.'s scheme. In Section 4, we show security weaknesses of Das et al.'s scheme. In Section 5, we propose our scheme. Section 6 shows security analysis of our proposed scheme. In Section 7, we compare the performances of our scheme with previously published scheme. Finally, we conclude the paper in Section 8.

2 Network Model

In hierarchical wireless sensor network (HWSN) (shown in Figure 1), there is a hierarchy among the nodes based on their capabilities namely, base station, cluster heads and sensor nodes. Usually, the ordinary sensor nodes are inexpensive, limited capabilities like, low battery power, low memory size, short transmission range, slow data processing etc. Cluster heads are little more expensive and has little more computational capability, battery power, memory size, transmission range than ordinary sensor nodes. However base station has unlimited battery power, huge memory size, extremely long transmission range with high computational capability and also an access point for human interface.

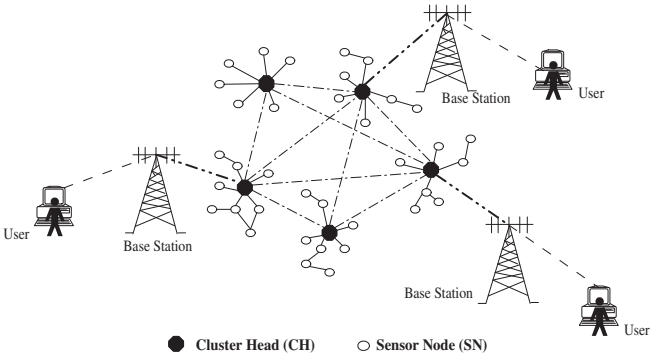


Figure 1: A hierarchical wireless sensor network (HWSN) architecture

In HWSN, all ordinary sensor nodes sense data from environment and send those sensed data to cluster head by single-hop or multi-hop communication [21]. Cluster head eliminates the redundancy data and aggregates all data and sends to base station via other cluster heads or directly. Then, a valid user can access those transmitted data from base station. Once the sensor nodes and cluster head are deployed, there is a problem for wireless sensor networks to maintain them. Limited battery power is responsible for limited life time of this networks. To maximize the life time of network it is necessary to design such a protocol that minimize the computational and communication cost of each node.

We consider the HWSN model for developing our proposed scheme due to the following reasons. Wireless sensor networks are distributed environment-driven systems that differ from traditional wireless networks in several ways, for examples, extremely high number of sensor nodes, data-centric network, broadcast communication paradigm and co-related data passing.

2.1 Assumptions

We have considered the following assumptions:

- There is a well established MAC protocol [18] to transmit data in networks.
- Base station can be considered as a trusted authority.
- The compromised (captured) nodes can be detected by base station and as a result, the base station, cluster head and sensor nodes know the identities of the compromised nodes. Consequently, the base station alerts the users with the compromised cluster heads.

3 Brief Review of Das et al.'s Scheme

In this section, we briefly describe Das et al.'s a dynamic password-based user authentication scheme for hierarchical wireless sensor networks [4]. The notations are used throughout this paper are summarized in Table 1.

Table 1: List of notation used

Symbol	Description
U_i	*i-th* User
BS	Base station
SN_j	Sensor node j
CH_j	Cluster head j in the *j-th* cluster
pw_i	Password of user U_i
ID_i	Identity of user U_i
ID_{CH_j}	Identity of cluster head CH_j
ID_{SN_j}	Identity of sensor node SN_j
S_{CH_j}	Shared secret key between CH_j and BS
S_{SN_j}	Shared secret key between SN_j and BS
MK_{CH_j}	Unique shared master key randomly generated by the BS for CH_j
SK	Shared session key between U_i and CH_j
$h(\cdot)$	Cryptographic One-way hash function
E	Symmetric key encryption algorithm
D	Symmetric key decryption algorithm
s	Secret information of the base station
X_A	Shared secret between U_i and BS
T	Current time stamp
$\|$	Concatenation operation
$\oplus$	Bit wise XOR operation

In Pre-deployment phase, base station assigns a unique identity, ID_{CH_j} and ID_{SN_j} for each cluster heads CH_j and each sensor node SN_j respectively. Base station also randomly selects unique master key MK_{CH_j} and MK_{SN_j} for each cluster heads CH_j and each sensor node SN_j respectively. These unique master keys MK_{CH_j} is shared between cluster head and base station, whereas MK_{SN_j} is shared between sensor node and base station. Then $\{ID_{CH_j}, MK_{CH_j}\}$ is stored into the memory of cluster head CH_j, and also $\{ID_{SN_j}, MK_{SN_j}\}$ is stored into the memory of sensor node SN_j. Finally these cluster heads and sensor nodes are dropped in a target field. Now for user authentication, their scheme consists of four phases namely, registration phase, login phase, authentication phase and password change phase.

3.1 Registration Phase

A user U_i selects a random number y_i, an identity ID_i and a password pw_i, and then computes $pwr_i = h(pw_i \| y_i)$. Then, U_i sends ID_i and pwr_i to the base station via a secure channel. After getting registration request message $\{ID_i, pwr_i\}$, base station computes $f_i = h(ID_i \| s)$, $x = h(pwr_i \| X_A)$, $r_i = h(y_i \| x)$, $e_i = f_i \oplus x$. Base station then selects $m + m'$ number of deployed cluster heads with $m + m'$ number of key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 < j \leq m + m'\}$, where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| s)$. Finally, base station stores $\langle ID_i, y_i, X_A, r_i, e_i, h(\cdot)$ and $m + m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 < j \leq m + m'\}\rangle$ into the memory of a tamper-proof smart card of user U_i and issues that smart card for user U_i.

3.2 Login Phase

User U_i inserts his/her smart card to the card reader and then provides ID_i and pw_i. The card reader computes $pwr'_i = h(y_i \| pw_i)$, $x' = h(pwr'_i \| X_A)$, $r'_i = h(y_i \| x')$ and checks whether computed r'_i equals stored r_i or not. If equal, card reader further computes $N_i = h(x' \| T_1)$, where T_1 is the current time stamp of user U_i and a ciphertext $E_{K_j}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)$, where ID_{CHj} is chosen by the user U_i. Finally, U_i sends the login request message $msg = \{ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)\}$ to the base station over a public channel.

3.3 Authentication Phase

After receiving the login request message $msg = \{ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)\}$ from the user U_i, the base station computes key $K = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| s)$ and by the computed key K, base station decrypts ciphertext $E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)$ and thus, $D_K(E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1))$ and verifies the validity of ID_i, ID_{CH_j} and T_1. If all are correct then base station further computes $X = h(ID_i \| s)$, $Y = e_i \oplus X$ and $Z = h(Y \| T_1)$ and verifies

whether $Z = N_i$ or not. If it holds then base station computes $u = h(Y \parallel T_2)$, where T_2 is the current time stamp of base station and produces a ciphertext message encrypted using the master key MK_{CH_j} of the cluster head CH_j as $E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i)$ and sends the message $\{ID_i \parallel ID_{CH_j} \parallel E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i)\}$ to the corresponding cluster head CH_j. After receiving message from base station, CH_j decrypts this message by computing $D_{MK_{CH_j}}(E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i))$ and checks the validity of ID_i, ID_{CH_j} and T_2. If all are valid then, CH_j further computes $v = e_i \oplus X$ and $w = h(v \parallel T_2)$ and checks whether $w = u$ or not. If it is true, then the user U_i is considered as a valid user and authenticated by CH_j and computes a session key $SK = h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$. Finally, CH_j sends an acknowledgment to the user U_i via other cluster heads and the base station, and responds to the query of the user U_i. After receiving the acknowledgment from CH_j, the user U_i agrees with the same secret session key SK, shared with CH_j by computing $SK = h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$ and they will use SK for securing communications in future.

3.4 Password Change Phase

This phase is invoked when user U_i wants to change his/her password. U_i inserts the smart card to the card reader and submits ID_i and pw_i. The card reader computes $pwr'_i = h(y_i \parallel pw_i)$, $x' = h(pwr'_i \parallel X_A)$, $r'_i = h(y_i \parallel x')$ and checks whether computed r'_i equals stored r_i or not. If equal, U_i enters a new password pw_i^{new}. Then the card reader further computes $M_1 = e_i \oplus x'$, $M_2 = h(y_i \parallel pw_i^{new})$, $r_i^{new} = h(y_i \parallel M_2)$, $M_3 = h(M_2 \parallel X_A)$, $e_i^{new} = M_1 \oplus M_3$. Finally, replace r_i with r_i^{new} and e_i with e_i^{new} into the memory of the smart card.

4 Weaknesses of Das et al.'s Scheme

In this section, we first describe the security weaknesses and then discuss the advantages of Das et al.'s scheme [4].

4.1 Security Weaknesses

In this section, we will analyze the security of Das et al.'s scheme [4]. In 2013, Li et al. [15] showed that Das et al.'s scheme [4] is insecure against off-line password guessing attack, impersonation attack, compromised cluster head attack and many logged-in users' attack. Except these attacks, Das et at.'s scheme [4] is insecure against insider attack, session key recovery attack and theft attack. To analyze the above weaknesses, we will assume that an attacker can obtain the secret parameter stored in the smart card by monitoring power consumption [12, 16] and can intercept all communicating message among user, base station and cluster head.

4.1.1 Insider Attack

A random number y_i is chosen by user U_i and y_i is not send by the user U_i to base station in registration phase of Das et al.'s scheme [4]. But in their scheme, base station uses y_i to compute $r_i = h(y_i \parallel x)$ which is impractical. Now, if we assume that user U_i also sends y_i to the base station, insider attack will be mounted against in their scheme because system manager or privileged insider of the base station knows pwr_i, y_i and $h(\cdot)$. So, easily system manager or privileged insider of the base station can guess the user's correct password by performing the following:

Computes $pwr_i^* = h(y_i \parallel pw_i^*)$ after choosing a guessed password pw_i^* and then, checks pwr_i^* and pwr_i are equal or not. If not equal, chooses another pw_i^* and repeats $pwr_i^* = h(y_i \parallel pw_i^*)$ until correct password is obtained. Otherwise pw_i^* is the correct password of the user U_i. That is after some guessing, system manager or privileged insider of the base station can find out the correct password of the user U_i as it is low entropy.

4.1.2 Theft Attack

We assume that an attacker knows valid password pw_i of a user U_i as shown in [15] and stored secret parameters of the smart card by monitoring power consumption [12,16]. To get success on the theft attack, an attacker have to steal user's smart card and computes the following steps:

Step 1. Attacker can compute $h(ID_i \parallel s)$ by computing $h(ID_i \parallel s) = e_i \oplus h(h(y_i \parallel pw_i) \parallel X_A)$, where attacker knows correct password pw_i and stored smart card's parameters X_A, e_i and y_i.

Step 2. Then, attacker chooses new password $pw_i^\dagger$ and random number $y_i^\dagger$ and, computes $pwr_i^\dagger = h(y_i^\dagger \parallel pw_i^\dagger)$, $x^\dagger = h(pwr_i^\dagger \parallel X_A)$, $r_i^\dagger = h(y_i^\dagger \parallel x^\dagger)$ and $e_i^\dagger = h(ID_i \parallel s) \oplus x^\dagger$.

Step 3. Finally, attacker loads $r_i^\dagger$, $y_i^\dagger$ and $e_i^\dagger$ into the memory of his/her smart card and keeps all other parameters $\langle ID_i, X_A, h(\cdot)$ and $m + m'$ key-plus-id combinations $(K_j, ID_{CH_j})\rangle$ unchanged. Then, uses his/her smart card as it is used by U_i.

4.1.3 Session Key Recovery Attack

We assume that an attacker can extract the secret information by monitoring power consumption [12, 16] from user U_i's smart card and also can intercept the all $i-th$ communicating messages among user U_i, base station BS and cluster head CH_j. After getting (K_j, ID_{CH_j}) combinations by monitoring the power consumption, an attacker can perform the session key recovery attack successfully as follows:

Step 1. An attacker intercepts the user U_i's login message $\{ID_i \parallel ID_{CH_j} \parallel E_{K_j}(ID_i \parallel ID_{CH_j} \parallel N_i \parallel e_i \parallel T_1)\}$.

Step 2. Attacker decrypts ciphertext $E_{K_j}(ID_i \parallel ID_{CH_j} \parallel N_i \parallel e_i \parallel T_1)$ by using K_j to get e_i and T_1, where K_j is stored into the memory of smart card of U_i.

Step 3. Attacker computes session key SK^* between user U_i and cluster head CH_j by performing $h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$ which is equal to session key between user U_i and cluster head CH_j.

Hence, the above procedure shows that Das et al.'s scheme [4] is insecure against the session key recovery attack.

4.2 Disadvantages of Das et al.'s Scheme

In this subsection, we will point out some disadvantages of Das et al.'s scheme [4].

4.2.1 Dynamic Cluster Head Addition Over Head Problem

In dynamic node addition phase of scheme [4], it is mentioned that no other information regarding cluster heads addition is required to store in the user's smart card. But, whenever new cluster heads are deployed, base station has to store their key-plus-id combinations $(K_{m+j}, ID_{CH_{m+j}})$ into the memory of user U_i's smart card, because user U_i cannot compute $\{K_{m+j} = E_{MK_{CH_{m+j}}}(ID_i \parallel ID_{CHm+j} \parallel s) \mid (m+j) > (m+m')\}$ without knowing the secret key s of base station and shared secret key $MK_{CH_{m+j}}$ between newly added cluster head CH_{m+j} and base station. Hence, dynamic cluster head addition increases the computation overhead of base station for storing key-plus-id combinations for each users.

4.2.2 Limited Number of Cluster Head Access Problem

Das et al. [4] mentioned that $(m+m')$ is chosen according to the memory availability of the smart card. Let, memory availability of the smart card is for 200 cluster heads' key-plus-id combinations. Thus, we can store key-plus-id combinations of 200 cluster heads into the memory of the smart card. It can be assumed that already 200 cluster heads are present into the network. Later, if we deploy more sensor nodes (including cluster heads) in the network for some reason then users cannot get real-time data from the newly deployed cluster heads because there are no memory space to store key-plus-id combinations of newly deployed cluster heads into the memory of smart card. Hence, the main objective of this architecture will be hampered.

4.2.3 Time Synchronization Problem

As Das et al. [4] used time stamp in their scheme, there is a probability of time synchronization problem between base station and user. Also same problem can be occurred between cluster head and base station during communication.

5 Our Proposed Scheme

In this section, we will propose an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. Our scheme consist of seven phases, namely pre-deployment phase, post-deployment phase, user registration phase, user login phase, authentication phase, password change phase and dynamic node addition phase.

5.1 Pre-deployment Phase

Base station performs following steps before deployment of cluster heads and ordinary sensor nodes on a target field. Figure 2 shows the pre-deployment phase of our proposed scheme.

Step 1. Base station chooses a random number c_j and an identity ID_{CH_j}, $(1 \leq j \leq m)$ for each cluster head CH_j. Then, it computes $S_{CH_j} = h(s \parallel ID_{CH_j} \parallel c_j)$ and stores $\{ID_{CH_j}, S_{CH_j}\}$ into the memory of CH_j as tamper resists.

Step 2. It chooses a random number w_p and an identity ID_{SN_p}, $(1 \leq p \leq x)$ for each ordinary sensor node SN_p. Then, it computes $S_{SN_p} = h(s \parallel ID_{SN_p} \parallel w_p)$ and stores $\{ID_{SN_p}, S_{SN_p}\}$ into the memory of SN_p as tamper resists.

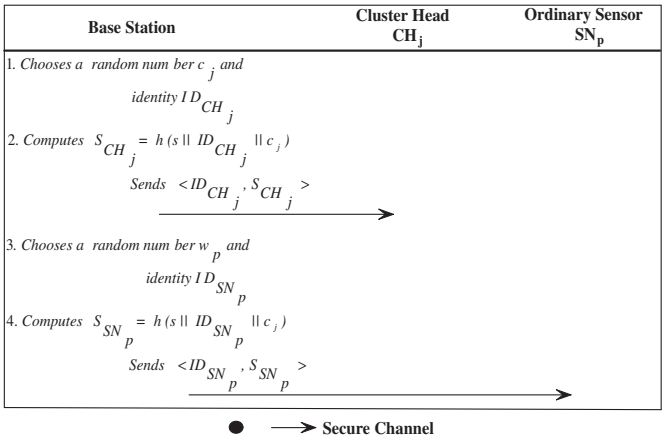


Figure 2: Pre-deployment phase

5.2 Post-deployment Phase

After deployment of cluster heads and ordinary sensor nodes on a target field, they form clusters such a way [10] that for each cluster, there will be a cluster head. The main objective in this paper is that how a valid user U_i, where $(1 \leq i \leq z)$ securely communicates to a cluster head CH_j to get real time data from target field.

5.3 User Registration Phase

In this phase, a user U_i chooses a random number y_i, his/her identity ID_i and password pw_i. Then, U_i computes $pwr_i = h(pw_i \parallel y_i)$ and sends $\{ID_i, pwr_i\}$ to the base station BS through a secure channel. After getting message $\{ID_i, pwr_i\}$ from the user U_i, base station computes $X_i = h(ID_i \parallel s) \oplus pwr_i$ and $B_i = h(h(ID_i \parallel s) \parallel pwr_i)$. Then base station issues a smart card for user U_i by storing $\{X_i, B_i, h(\cdot)\}$ into the memory of smart card. After getting his/her smart card, user U_i stores y_i into the memory of smart card. Figure 3 shows the user registration phase of our proposed scheme.

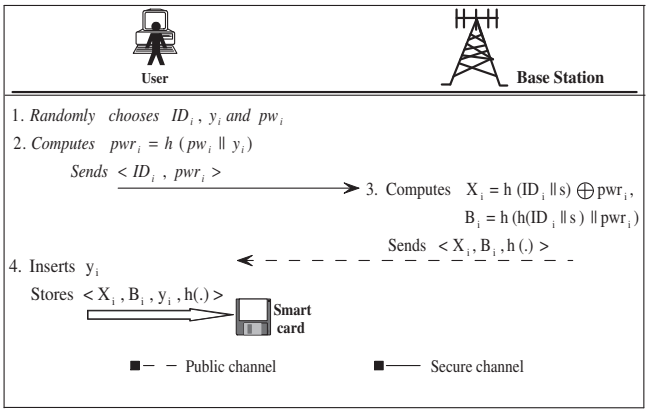


Figure 3: User registration phase

5.4 User Login Phase

In this phase, user U_i provides his/her identity ID_i and password pw_i to the card reader. Then card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether computed B'_i equals stored B_i. If true, proceed to next otherwise 'rejects' user U_i. Then, user U_i chooses ID_{CH_j} and submits it to the card reader. Then, card reader further chooses a random number N_1 and computes $P_i = h(Y'_i \parallel ID_{CH_j} \parallel N_1 \parallel pwr'_i)$ and $R_i = N_1 \oplus pwr'_i$ and sends $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ to the base station. Figure 4 shows the user login phase of our proposed scheme.

5.5 Authentication Phase

In this phase, after getting login request message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ from user U_i, base station computes $Y_i^* = h(ID_i \parallel s)$, $pwr_i^* = Y_i^* \oplus X_i$, $N_1^* = pwr_i^* \oplus R_i$ and $P_i^* = h(Y_i^* \parallel ID_{CH_j} \parallel N_1^* \parallel pwr_i^*)$ and, it checks whether computed P_i^* equals sending P_i or not. If it holds good, base station further chooses a random number N_2 and computes $Z_i = pwr_i^* \oplus N_2$, $D_i = h(Y_i^* \parallel N_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1^*)$. Then, it sends $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ to the user U_i. Again base station computes $N_3 = N_2 \oplus N_1^*$, $V_i = h(ID_{CH_j} \parallel S_{CH_j})$, $E_i = V_i \oplus N_3$, $A_i = h(Y_i^* \parallel N_3 \parallel pwr_i^*)$, $L_i = A_i \oplus V_i$ and

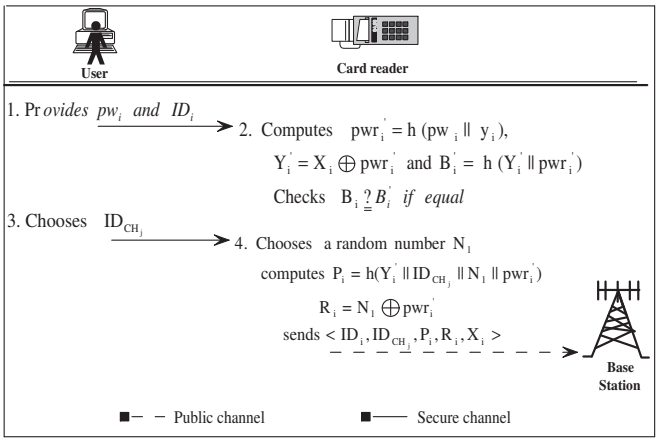


Figure 4: User login phase

$G_i = h(S_{CH_j} \parallel N_3 \parallel A_i \parallel ID_i \parallel ID_{CH_j})$ and, sends $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ to the cluster head CH_j. After that the following computations are performed:

1) After getting reply message $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ from base station, card reader computes $N'_2 = Z_i \oplus pwr'_i$, $D'_i = h(Y'_i \parallel N'_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1)$ and checks whether computed D'_i equals sending D_i or not. If it holds good then computes $N'_3 = N_1 \oplus N'_2$, $A'_i = h(Y'_i \parallel N'_3 \parallel pwr'_i)$ and session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N'_3 \parallel A'_i)$.

2) After receiving message $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ from base station, cluster head CH_j computes $V_i^\star = h(ID_{CH_j} \parallel S_{CH_j})$, $N_3^\star = V_i^\star \oplus E_i$, $A_i^\star = L_i \oplus V_i^\star$ and $G_i^\star = h(S_{CH_j} \parallel N_3^\star \parallel A_i^\star \parallel ID_i \parallel ID_{CH_j})$ and checks weather computed $G_i^\star$ equals sending G_i or not. If true, then it computes session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3^\star \parallel A_i^\star)$.

Now, both parties (user U_i and cluster head CH_j) are agreed with common shared session key SK and can communicate securely to each other by shared secret session key SK in future. Figure 5 shows the authentication phase of our proposed scheme.

5.6 Password Change Phase

In this phase, user U_i provides his/her identity ID_i and password pw_i to the card reader. Card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether B'_i equals B_i or not. If equal, proceed to next otherwise 'rejects' user U_i. Then, user U_i provides new password pw_i^{new} to the card reader. Card reader computes $pwr_i^{new} = h(pw_i^{new} \parallel y_i)$, $X_i^{new} = Y'_i \oplus pwr_i^{new}$, $B_i^{new} = h(Y'_i \parallel pwr_i^{new})$. Then U_i replace old values of X_i and B_i by the new value of X_i^{new} and B_i^{new} respectively into the memory of smart card. Thus, U_i can change the password without taking any assistance from base station.

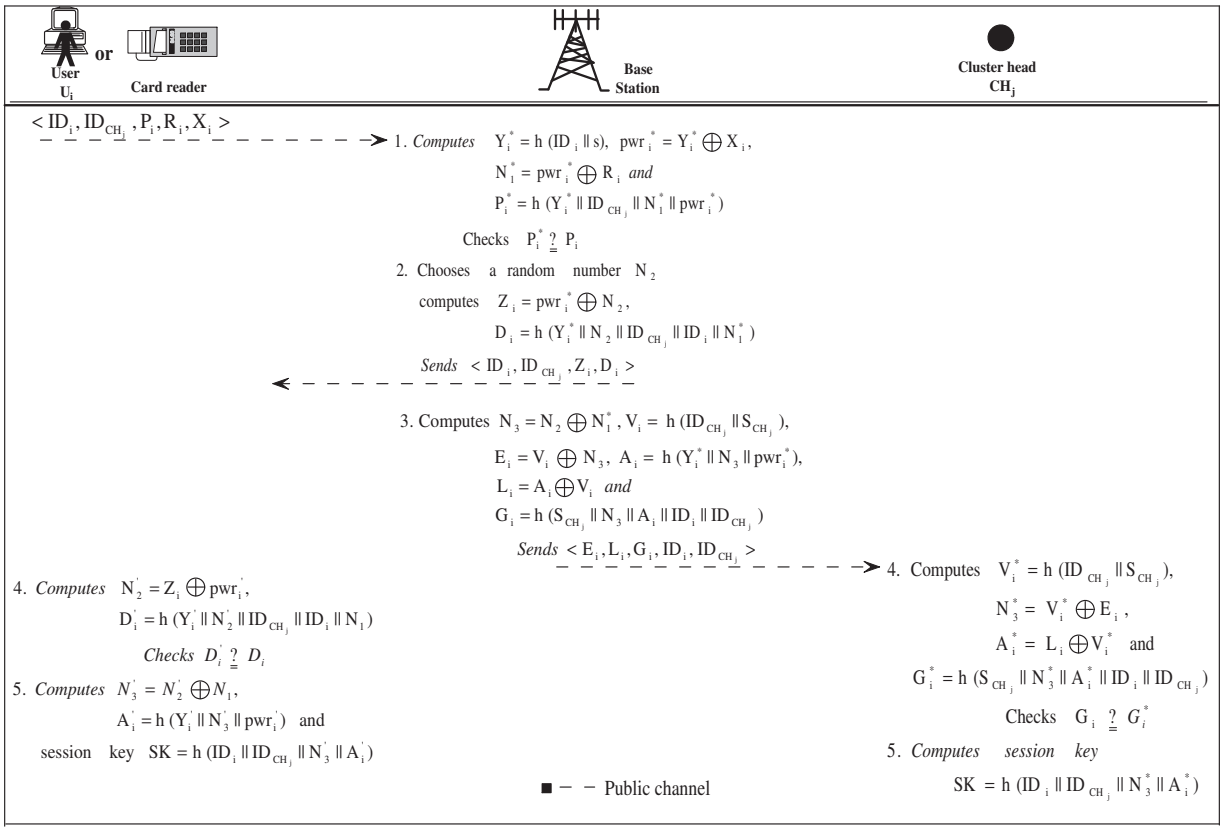


Figure 5: Authentication phase

5.7 Dynamic Node Addition Phase

In this phase, we describe the addition or replace procedure of new nodes into the networks of our scheme. This phase is needed to replace or add new nodes which are either dead for energy loss or captured by an attacker. Base station performs following steps:

Step 1. It chooses a random number c_l and an identity ID_{CH_l}, $(1 \leq l \leq m_1)$ for each cluster head CH_l. Then computes $S_{CH_l} = h(s \parallel ID_{CH_l} \parallel c_l)$ and stores $\{ID_{CH_l}, S_{CH_l}\}$ into the memory of CH_l as tamper resists.

Step 2. It chooses a random number w_v and an identity ID_{SN_v}, $(1 \leq v \leq x_1)$ for each ordinary sensor node SN_v. Then it computes $S_{SN_v} = h(s \parallel ID_{SN_v} \parallel w_v)$ and stores $\{ID_{SN_v}, S_{SN_v}\}$ into the memory of SN_v as tamper resists.

Step 3. All new nodes are deployed into the target field and then base station informs to the users about the addition of new nodes.

The above procedure shows that it is not needed to store information regarding new nodes into the memory of user's smart card.

6 Security Analysis of Our Proposed Scheme

In this section, we will analyze the security of our proposed scheme. We may assume that an attacker could obtain the values which are stored in the memory of smart card by monitoring the power consumption [12,16]. Further, attacker can intercept communicating messages among user, server and cluster head. Under these assumptions, we will show that the proposed scheme resists different possible attacks.

6.1 Smart Card Stolen Attack

We assume that user U_i has either lost his/her smart card or stolen by an attacker. After getting the smart card, an attacker can extract the parameters X_i, B_i, y_i and $h(\cdot)$ from the smart card of the user U_i. After getting all these parameters, it is hard to derive or guess user's correct password pw_i and base station's secret key s by the attacker as shown in following.

1) From parameter $X_i = h(ID_i \parallel s) \oplus pwr_i = h(ID_i \parallel s) \oplus h(pw_i \parallel y_i)$, given ID_i and y_i, attacker cannot guess s and pw_i because it is hard to guess two unknown parameters in polynomial time as shown by Sood et al. [20].

2) The attacker cannot compute s and pw_i from parameter $B_i = h(h(ID_i \parallel s) \parallel pwr_i) = h(h(ID_i \parallel s) \parallel h(pw_i \parallel y_i))$, given ID_i and y_i because it is computationally hard due to inverse of cryptographic one-way hash function.

So, the attacker cannot compute any secret information from parameters which are stored into the memory of smart card. Hence, the proposed scheme resists smart card stolen attack.

6.2 Impersonation Attack

To impersonate as a legitimate user, an attacker attempts to make a forged login request message $\{ID_i, ID_{CH_j}, P_i^a, R_i^a, X_i\}$ by computing following steps, given $\{X_i, B_i, y_i, h(\cdot), ID_i, ID_{CH_j}\}$

1) The attacker chooses random number N_1^a and also chooses a password pw_i^a.

2) Computes $pwr_i^a = h(pw_i^a \parallel y_i)$.

3) Computes $R_i^a = N_1^a \oplus pwr_i^a$.

But, to compute parameter $P_i^a = h(Y_i' \parallel ID_{CH_j} \parallel N_1^a \parallel pwr_i^a)$, where $Y_i' = h(ID_i \parallel s)$, attacker have to know secret key s of base station. In our scheme, secret key s of base station is used as $h(ID_i \parallel s)$. So, attacker cannot compute s from $h(ID_i \parallel s)$ because it is hard due to inversion of cryptographic one-way hash function. Thus, the attacker cannot produce forged login request message $\{ID_i, ID_{CH_j}, P_i^a, R_i^a, X_i\}$ in our scheme.

6.3 Privileged Insider Attack

If the system manager or privileged insider of the base station knows user's password, he/she may try to access user U_i's other accounts of other base stations. But in our scheme, $pwr_i = h(pw_i \parallel y_i)$, where random number y_i is unknown to the system manager or privileged insider of the base station is transmitted instead of pw_i to the base station in registration phase. From parameter pwr_i, privileged insider of the base station cannot compute correct pw_i because it is computationally hard due to inversion of cryptographic one-way hash function. So, the proposed scheme resists privileged insider attack.

6.4 Replay Attack

An attacker intercepts a valid login message $\{ID_i, ID_{CHj}, P_i, R_i, X_i\}$ and stores it for further use. After completion of user's transaction, base station stores this login message. Suppose, then the attacker sends the same stored login message to the base station. After receiving it, base station will check sending login message with stored login message and if both are equal then base station will reject the attacker's login request. In our scheme, $P_i = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel pwr_i')$ and $R_i = N_1 \oplus pwr_i'$. Our scheme resists replay attack because login message is changed in every session due to random number N_1.

6.5 Off-line Password Guessing Attack

We have shown in smart card stolen attack (Subsection 6.1) of our scheme that adversary cannot extract user U_i's password pw_i from smart card's parameters $\{X_i, B_i, y_i\}$. Again, the adversary try to guess user U_i's password pw_i from login message $\{ID_i, ID_{CHj}, P_i, R_i, X_i\}$ between user U_i and base station. But, we will show that the adversary cannot guess user U_i's password pw_i from login message which is as follows:

1) From parameter $P_i = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel pwr_i') = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel h(pw_i \parallel y_i))$, given ID_i, ID_{CHj} and y_i, adversary cannot guess password pw_i because it is hard due to inversion of cryptographic one-way hash function.

2) From parameter $R_i = N_1 \oplus pwr_i' = N_1 \oplus h(pw_i \parallel y_i)$, given y_i, adversary cannot guess user U_i's password because he/she have to solve parameter R_i without knowing two unknown values pw_i and N_1 which is computationally hard.

The above explanation shows that our proposed scheme resists off-line password guessing attack.

6.6 Theft Attack

If an adversary can store valid smart card's parameters into the memory of his/her smart card then the authentication scheme will be insecure against theft attack. In our scheme, to compute smart card's parameters, an adversary have to know valid user's password pw_i and secret key s of the base station. But, we have shown in smart card stolen attack (Subsection 6.1) that an adversary cannot compute base station's secret key and user's password from valid user's smart card. As a result, the proposed scheme is secure against theft attack.

6.7 Session Key Recovery Attack

In our scheme, an attacker cannot compute secret session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel A_i) = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel h(Y_i \parallel N_3 \parallel pwr_i)) = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel h(h(ID_i \parallel s) \parallel N_3 \parallel h(pw_i \parallel y_i)))$ between user U_i and cluster head CH_j except captured cluster heads because, in our scheme, computation of session key depends on user's password pw_i, random number N_3 and secret key s of base station. We have shown in smart card stolen attack (Subsection 6.1) and off-line password guessing attack (Subsection 6.5) that the adversary has no way to get secret key s of base station and user's password pw_i. So, our scheme is secure against session key recovery attack.

Table 2: Comparison of computational cost of our scheme with Das et al.'s scheme

Schemes	Registration Phase		Login Phase	Authentication Phase		
	User	Base station	User	Base station	Cluster head	User
Das et al. [4]	$1T_h$	$(m+m')T_{enc}+3T_h$	$4T_h+1T_{enc}$	$3T_h+2T_{enc}+1T_{dec}$	$2T_h+1T_{dec}$	$1T_h$
Our	$1T_h$	$2T_h$	$3T_h$	$6T_h$	$3T_h$	$3T_h$

6.8 Denial of Service Attack

In password change phase of our proposed scheme, card reader first checks the validity of provided old password of any user say, U_i. If provided password is valid then only card reader allows user U_i to provide his/her new password. So, an adversary have to know the correct password of user U_i to change U_i's password. But, off-line password guessing attack (Subsection 6.5) shows that there is no chance to compute U_i's password. So, adversary cannot change password of user U_i. Thus, only valid users get service from cluster heads via base station. So, our scheme is secure against denial of service (DoS) attack.

6.9 Cluster Head Capture Attack

When a cluster head is compromised by an attacker then it compromises its own secret key and shared session key. Moreover, secure communication with users and with its neighbor sensor nodes are compromised. But in our scheme, there are a unique secret key is given for each node (including cluster head). Thus, if an attacker captures a cluster head, he/she will get secret key of that captured cluster head only. As a result, all other non-compromised cluster heads can still communicate securely with other nodes in the networks and with users. Hence, our scheme provides security against cluster head capture attack.

7 Performance Analysis of Our Proposed Scheme

In this section, we compare the performance of our proposed scheme with Das et al.'s scheme [4]. We assume that Das et al.'s scheme consist of $m+m^{'}=200$ nodes in the wireless sensor network. Table 2 shows the computation over head of user, base station and cluster head of our proposed scheme with the related scheme. Table 3 shows the communication cost and storage cost of our scheme and related scheme. In Table 2, T_h is the time required for hashing operation, T_{enc} is the time required for encryption operation and T_{dec} is the time required for decryption operation. In scheme [4], computational over head is directly proportional to number of cluster heads. But in our scheme, computation over head is independent on the number of cluster heads. Our proposed scheme takes less computational cost than that of Das et al.'s scheme.

For comparison purpose, we assume that the length of ID_i, ID_{CH_j}, X_A are 64 bits each, random nonce and message digest $h(\cdot)$ are 128 bits each. We may assume that AES-128 symmetric key encryption/decryption algorithm [17] are used in scheme [4]. In Table 3, we have shown the communication cost (capacity of transmitting message) of our scheme and scheme [4] is 1408 bits and 1536 bits respectively. So our scheme takes $(1536-1408) = 128$ bits less than that of the scheme of Das et al. [4]. Also the storage cost (stored in the memory of smart card) of our scheme and Das et al.'s scheme [4] are 512 bits and 32640 bits respectively. So, Das et al.'s scheme [4] takes $(32640-512) = 32128$ bits more than that of our scheme. Note that, storage cost dependent on the number of cluster heads in Das et al.'s scheme.

Table 3: Comparison of communication cost, storage cost and security attacks of our scheme with Das et al.'s scheme

Cost & Attack	Das et al. [4]	Our
Communication Cost	1536 bits	1408 bits
Storage Cost	32640 bits	512 bits
A1	√	×
A2	√	×
A3	√	×
A4	×	×
A5	√	×
A6	√	×
A7	√	×

A1: Insider Attack, A2: Off-line Password Guessing Attack, A3: Smart Card Stolen Attack, A4: Replay Attack, A5: Theft Attack, A6: Password Change Attack and A7: Session Key Recovery Attack

Most wireless sensor networks suffers from power consumption of cluster head. So low computation cost of cluster head is desirable. In Table 2, we have shown that the computation overhead of cluster head of our scheme with Das et al.'s scheme [4]. Das et al.'s scheme [4] takes more computation cost than that of our scheme.

In Table 3, we have shown that our scheme provide strong authentication system compared to Das et al.'s scheme [4]. Hence, our scheme provides batter security, low computational cost, low communication cost and storage cost than Das et al.'s scheme [4].

We will discuss the advantages of our proposed scheme over Das et al.'s scheme [4].

Mutual Authentication. Our scheme provides strong mutual authentication between a user and base station. Even if attacker can extract the secret information from the memory of user's smart card and intercepting login message between the user and base station, attacker cannot compute the valid login message and reply message without knowing the secret password pw_i of user U_i, secret key s of base station and random number N_1. So our scheme provides mutual authentication between a user and base station.

Early Wrong Password Detection. If the user U_i inputs a wrong password by mistake in password change phase or login phase, it will be quickly detected by the card reader itself since card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether computed B'_i equals stored B_i into memory of smart card. Hence our scheme provides early wrong password detection.

Solves Time Synchronization Problem. Our proposed scheme uses randomly generated nonce N_1 and N_2 instead of time stamps to avoid time synchronization problem.

Unlimited Number of Cluster Head Access. In our scheme, we do not need to store any key-plus-id combinations for each cluster heads into the memory of user's smart card. In our scheme, stored parameters of user's smart card are independent of cluster head's secret information. Thus in our scheme, a user can access all the cluster heads (including newly deployed cluster heads) in the networks.

No Dynamic Cluster Head Addition Over Head. In our scheme, smart card's stored information are independent from any cluster head's information. Thus for addition of new nodes, base station does not need to compute further information regarding newly deployed cluster heads for user's smart card.

8 Conclusion

We have shown that Das et al.'s scheme suffers from some security weaknesses. To over come these weaknesses, we have proposed our scheme. Further, in security analysis, we have shown that our scheme is more efficient in terms of computational, communication and storage cost than that of Das et al.'s scheme. We have also shown that in our scheme, users can access all the cluster heads and no need to compute any parameter for the user's smart card after adding new cluster heads into the network. In future, validation of the proposed scheme will be evaluated by Automated Validation of Internet Security Protocols and Applications (AVISPA) [1], a security tool. Further, it can be incorporated biometric features into the proposed scheme to achieve high security in remote user authentication scheme.

References

[1] AVISPA, *Automated Validation of Internet Security Protocols and Applications*, Project funded by the European Community under the Information Society Technologies Programme, IST-2001-39252, 2001. (`http://www.avispa-project.org/`)

[2] DARPA, *Defense Advanced Research Projects Agency*, Section 2352, Title 10 of the United States Code, 2015. (`http://www.darpa.mil/our-research`)

[3] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," *International Journal of Network Security*, vol. 14, no. 1, pp. 1–21, 2012.

[4] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," *International Journal of Network Security*, vol. 7, no. 1, pp. 61–68, 2008.

[8] R. Fan, L. di Ping, J. Q. Fu, and X. Z. Pan, "A secure and efficient user authentication protocol for two-tiered wireless sensor networks," in *Second Pacific-Asia Conference on Circuits, Communications and System (PACCS'10)*, vol. 1, pp. 425–428, 2010.

[9] D. He, Yi Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 4, pp. 361–371, 2010.

[10] L. Jia, R. Rajaraman, and T. Suel, "An efficient distributed algorithm for constructing small dominating sets," *Distributed Computing*, vol. 15, no. 4, pp. 193–205, 2002.

[11] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[12] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'99)*, pp. 388–397, 1999.

[13] V. A. Kottapalli, A. S. Kiremidjian, J. P. Lynch, E. D. Carryer, T. W. Kenny, K. H. Law, and Y. Lei, "Two-tiered wireless sensor network architecture for structural health monitoring," in *Smart Structures and Materials*, pp. 8–19, 2003.

[14] P. Kumar and H. J. Lee, "Cryptanalysis on two user authentication protocols using smart card for

wireless sensor networks," in *Wireless Advanced (WiAd'11)*, pp. 241–245, 2011.

[15] C. Ta Li, C. Y. Weng, C. C. Lee, C. W. Lee, P. N. Chiu, and C. Yi Wu, "Security flaws of a password authentication scheme for hierarchical wsns," *Journal of Advances in Computer Network*, vol. 1, no. 2, pp. 121–124, 2013.

[16] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[17] NIST, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, National Institute of Standards and Technology (NIST), U. S. Department of Commerce, 2001. (`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`)

[18] S. Ray, I. Demirkol, and W. Heinzelman, "ATMA: Advertisement-based tdma protocol for bursty traffic in wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, 2010.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communnications of ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[20] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011.

[21] M. T. Thai, F. Wang, D. Liu, S. Zhu, and D. Z. Du, "Connected dominating sets in wireless networks with different transmission ranges," *IEEE Transactions on Mobile Computing*, vol. 6, no. 7, pp. 721–730, 2007.

[22] H. Ru Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'07)*, pp. 986–990, 2007.

[23] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'10)*, pp. 600–606, 2010.

[24] B. Vaidya, J. Silva, and J. J. P. C. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'09)*, pp. 88–91, 2009.

[25] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, pp. 59–64, 2004.

[26] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, pp. 244–251, 2006.

[27] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272–276, 2010.

Tanmoy Maitra received his B.E. degree in computer science and engineering from Burdwan University, India in 2009 and his M.Tech degree in computer science and engineering from WBUT, India in 2013. Now, he is pursuing Ph.D from Jadavpur University, India. He has qualified GATE in computer science in 2011 and 2012 respectively. He has published few international journal papers on remote user authentication system. His research interest includes wireless sensor networks and applied cryptology.

Ruhul Amin received his B.Tech and M.Tech degree from West Bengal University of Technology, India in computer science and engineering department in 2009 and 2013 respectively. Now, he is pursuing Ph.D from Indian Schools of Mines University, India. He has qualified GATE 2011 in computer science. He has published few international journal papers on remote user authentication system. His research interest includes remote user authentication and security in wireless sensor network.

Dr. Debasis Giri is presently Professor in the Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia-721657, India. He received his Ph. D on Cryptanalysis and Improvement of Protocols for Digital Signature, Smart-Card Authentication and Access Control from Indian Institute of Technology, Kharagpur 721 302, India in 2009. He did his masters (M. Tech and M. Sc) both from Indian Institute of Technology, Kharagpur in 2001 and 1998 respectively. He has tenth All India Rank with percentile score 98.42 in the Graduate Aptitude Test in Engineering (GATE) Examination in 1999. Dr. Giri has published more than 30 technical papers in several international journals/proceedings. He taught several courses such as Discrete Mathematics, Cryptography, Information Security, Coding Theory and Advanced Algorithms etc. His current research interests include cryptography, Network security, Security in Wireless Sensor Networks and Security in VANETs. Further, he is Editorial Board Member and Reviewer of many reputed International Journals. He is also Program Committee member of many International Conferences.

Dr. P. D. Srivastava has joined the Department of Mathematics, Indian Institute of Technology, Kharagpur as faculty in the year 1980 and became Professor in 1998. Dr. Srivastava has a very bright academic career. He has obtained his B.Sc., M.Sc. degree from Kanpur university in the year 1973 & 1975 respectively and Ph.D from I.I.T. Kanpur in the year 1980. Dr. Srivastava is not only an established researcher in his area but also a teacher par excellence. His style of lecture presentation and full command on the subject impress the students, which is reflected by the students in "Students' Profile

Forms" (teaching Assessment by the Students. During his 34 years teaching career, he taught several courses such as Functional Analysis, Topology, Numerical Analysis, Measure Theory, Real Analysis, Complex Analysis, Calculus etc. to undergraduate and postgraduate students. Besides teaching, Professor Srivastava is equally devoted to research Approximately 51 Papers published in very good and reputed journals of mathematics, are credited to his account. He has supervised 10 research scholars for Ph.D. Degree in mathematics and one for PDF. Various universities have invited him for Lectures/Key note address in the conferences. Various universities invite him as an expert in the Faculty selection as well as an expert to adjudicate the Ph.D. theses. He is also reviewer for the Mathematical Reviews as well as Paper referee for many journals.

A Study on E-Taiwan Promotion Information Security Governance Programs with E-government Implementation of Information Security Management Standardization

Chien-Cheng Huang[1] and Kwo-Jean Farn[2]
(Corresponding author: Chien-Cheng Huang)
Department of Information Management, National Taiwan University[1]
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan, Republic of China
Taiwan Internet Protection Association[2]
3F.-6, No. 155, Sec. 1, Keelung Road, Taipei 11070, Taiwan, Republic of China
(Email: chienchenghuang@ntu.edu.tw)
(Received Aug. 16, 2014; revised and accepted Oct. 3 & Nov. 10, 2014)

Abstract

The promotion of Information Security Governance (ISG) has become an important factor in the implementation of e-government and information security management within the "National Information and Communications Technology Security Development Program (2009˜2012)" in continuing the "Plan for Establishment of Information and Communication Technology Infrastructure Security Mechanism (2001˜2008)" in Taiwan; in July 2013, the working outline of the project was adjusted. And, it was asked all departments of Executive Yuan and local government to process aggressively by regulation on December 25, 2013. This study examines information security development program, and strategies for meeting e-government and information security management requirements within the implementation of information security development programs through information security management systems (ISMS). Moreover, an action program for improved ISMS performance, using an approach combining ISG and ISMS, is proposed. Based on this, this research employs history analysis and in-depth interview methodologies to develop insights into e-Taiwan information security management. Furthermore, the research objective is to examine the relevance between the execution of e-government and information security management framework and ISMS implementation by using the ISG project approach.

Keywords: E-government, ISG, ISMS, standardization

1 Introduction

Information technology has taken the world by storm. Its emergence has given rise to a new level of digital knowledge systems. Its application has been catalytic to the rapid changes taking place in the way people work, live and think, and is facilitating the development of our society and civilization in a new era. However, along with the tremendous benefits and development of information technology comes the challenging problem of e-government and information security management [6, 8, 12, 25, 35, 36, 37, 44, 45].

The "Plan for Establishment of Information and Communication Technology Infrastructure Security Mechanism" in Taiwan was approved by the Executive Yuan on January 17, 2001. As a result, information security management system (ISMS) certifications have been the focus of the first two phases (2001˜2008). Third phase programs (2009˜2012) from the "National Information and Communications Technology Security Development Program" (simplified as "Information Security Development Programs") were renamed by dispatch document No. 0980080376 on January 20, 2009 [30]. Among the approved nine measures and thirty action programs mentioned earlier, the strengthening of information security audits and ISMS certification remained one of the nine key action programs in e-government and information security management implementation.

On Feb. 5, 2009, the National Information and Communications Technology Security Taskforce (NICST) formally notified various departments under the Executive Yuan that they were required to put the action pro-

grams into practice. The aim was to achieve the four policy objectives of "Strengthen the overall response capacity", "Provide reliable information services", "Improve the competitiveness of enterprises" and "Create an enabling environment for a culture of information security" listed in the information security development programs [30]. In the information security development programs, strengthening information security audits and ISMS certification were important actions in the implementation of e-government and information security management, where each governmental department had taken on these security responsibilities, as shown in Table 1. However, the ISMS effectiveness has often been questioned [17]. In addition, all elements of the action programs had been explicitly defined under the idea that "The scope of certification is limited to core businesses" in the important measures of "Strengthen Information Security Audits and ISMS Certification" for the information security development programs [30].

Although "information security management differs due to its standard, and information security standard may change due to implementation", it complies with ISO/IEC 27001:2005(E) requirements, and was implemented in terms of core businesses as listed in ISO/IEC 27001:2005(E) relevant clauses of limited core businesses for the ISMS certification scope, Section 1.1 and Section 4.2.1(a) [30]. Organizations should then be covered by the ISMS. However, a large number of organizations that have passed ISMS certification have still failed to provide the necessary ISMS policy documents requested in ISO/IEC 27001:2005(E), Section 3.1(a). Because of this failure, it must be acknowledged that such shortcomings within Taiwans ISMS authentication and certification system require urgent attention [9]. Furthermore, in view of the discussion on the ISMS certification effectiveness, relevant authorities expect that this issue will be dealt with through the information security governance (ISG) action programs, as listed in Table 1. Due to the change, we understand that the motive power which doesnt want to change, so we offer the promotive product of national vulnerability database (NVD) and security content automation protocol (SCAP) of security configuration management which are from National Institute of Standards and Technology (NIST) in the technology application category of ISMS standardization. However, in July 2013, the ISMS working outline mentioned above was modified; the detailed ongoing working process will be explained in this work through an in-depth interview (see Appendix A). After three years, it has become the policy of National Information and Communications Technology Security Development Program (2013˜2016) officially on December 25, 2013 [32].

This research employs history analysis and in-depth interview methodologies to develop insights into e-Taiwan information security management. In addition to the interviews, other documents and materials were obtained during the fieldwork period (see Appendix A). The remainder of this paper is arranged as follows. Section 2 examines information security development programs and ways of meeting of e-government and information security management requirements through ISMS. In Section 3, an action program using a combination of ISG and ISMS is proposed in order to improve ISMS performance. Discussion of the findings, conclusions and implications of this research, and the new requirement added in 2013, are given in Section 4.

2 Analysis of E-Taiwan Information Security Management

2.1 E-government Information Security Management and ISMS

"Regulatory or Legal requirements" are the key to the establishment of an ISMS, as prescribed under ISO/IEC 27001:2005(E) Sections 3.16, 4.2.1(b)(2), 4.2.1(g), 5.1(d), 5.2.1(c), 6(a) and 7.3(c)(4). It was ruled in Section 161 of the Administrative Procedure Act that "effective administrative regulations have to bind authority to the issuing department and its subordinate agencies". Moreover, information security development programs are classified as administrative regulations [10]. The governmental departments must comply with the nine action programs listed under the important measures of e-government and information security management, given in Table 1. In addition, the important action program measures and performance indicators of ISG promotion are listed in the information security development programs [30]. The important measures also explain that the ISG projects and ISMS are closely linked. In the practical guidelines of the ISMS control measures for the healthcare sector, it is clearly stated that ISG should be included in information governance or information assurance [15].

Lee and Kim [26] illustrated the scope of ISMS program integration for streamlining its effectiveness, as shown in Figure 1. However, whether or not the management structure of the organization area is applied depends on whether it is possible to establish legitimacy within the environment area. The question of whether it will continue to function in the governance area can be answered by checking the maintenance efficiency of the legitimacy. If the leading structure legitimacy is based on power, it will directly or indirectly influence the behavior of the individual and the group. On the other hand, if the system includes complete feedback and adjustment protocols, it can react accordingly to various situations, extending the system lifespan; otherwise, modification would be necessary. While the principles of a private department usually focus on achieving a set target, in a public department, the interests of the whole community are the main goal, not the organization itself. The influencing factors mentioned are complementary, or to be more precise, "the policy field" feature exceeds the importance of the "problem solving field" of a private unit, while the risk area includes managerial, social and information technology (IT)

Table 1: The important measures and action programs of the providing reliable information services in the information security development programs [30]

Goals	Important Measures	Action Programs
Provide reliable information services	E-government information security management implementation	The regulations and guidelines on development and maintenance of information security process in governmental departments. Promote ISG (information security governance). Promote information and information system classification/grading. Strengthen e-government information, communication security and implementation official data protection. Promote security certification of the information and communication devices for the agency. Enrich information security personnel. Enhance information security protection technique and quality of the services. Strengthen information security literacy and training ability. Strengthen information security audits and ISMS certification.
	Promote network security of the critical information infrastructures	The development of the critical information infrastructure protection strategy.

risk. Although Figure 1 is not accepted by ISO, its theory becomes the example in the launched project which is from Presidential Policy Directive (PPD)-21 and Executive Order (EO) 13636 of the United States. Therefore, it is still valuable.

The implementation of ISMS is more than an event or a condition, it is a series of activities scattered across the ISMS operation. These activities can even be found in the way management runs a business. The ISMS process is governed via the basic management process of "Plan", "Do", "Check" and "Act". On the other hand, on June 1, 2008, the International Organization for Standardization (ISO) published ISO/IEC 38500:2008(E), which consisted of six principles for information technology governance (ITG): responsibility, strategy, acquisition, performance, conformance and human behavior [18]. Table 2 shows the corresponding standard sessions offered by ISO/IEC 38500:2008(E) and ISO/IEC 27001:2005(E). On the other hand, the ISO/IEC 27001:2013(E), new version, has been launched on October 1, 2013 and ISG has been already in the requirement of ISMS [22].

In addition, ISO had already published a standard of the ISG for ISO/IEC 27014 [16, 20, 21]. Leaders must apply the principles of the ITG through the ISG framework (as indicated in ISO/IEC 27014:2013(E)) in ISMS. An ISG framework consists of objectives, focus areas and implementation models. The objectives of an ISG include business alignment, accountability and compliance. Business alignment focuses on enabling an alignment between business and information security objectives. Accountability aims to ensure that an entity takes responsibility for its actions and decisions. Compliance serves to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any information security requirements.

ISG needs to focus on five areas: strategic alignment, risk management, resource management, performance measurement and value delivery. In addition, when implementing ISG, the following four aspects must be considered: ISG processes, organization, architecture and investment management issues. Furthermore, ISG processes include the sub-categories: "Evaluate", "Direct", "Monitor", "Communicate" and "Assure" [21].

In Taiwan, the Information Management Center of the Directorate-General of Budget, Accounting and Statistics (DGBAS) was requested to handle the business continuity plan (BCP) of the ISMS by dispatch document No. 0980021063 on February 16, 2009, by the Executive Yuan. A Local Tax Bureau therefore performed an analysis of the ISG, as shown in ISO/IEC 27014. However, in terms of performance management, the Financial Data Center (FDC) of the Ministry of Finance (MOF) uses quality management systems for the procurement of software, and is more effective than Local Tax Bureaus, in addition to handling both the risk management and resource management as well. In terms of strategic alignment and value delivery, the MOF and various local governments must comply with the ISG for e-government services proposed by Lee and Kim [26], as shown in Figure 1, and stated in the e-government information transformation development plan by the Research, Development and Evaluation Commission (RDEC), and Article 111 of the Constitution as "Distribution of Competencies between Central and Local Governments". Finally, the chief information security officer (CISO) of a Local Tax Bureau establishes implementation models (as indicated in Table 3) and incorporates the ISMS policies [14].

Therefore, Local Tax Bureaus were requested by the central government to oversee the planning of offsite backups. After six months, the Taxation Agency then specified conditions within the "Integrated Local Tax Information Application Platform Program" promulgated by dispatch document No. 09822003350 on November 4, 2009, by the MOF. The FDC thus became the kernel responsible for the offsite backups. This is an instance of ISG application.

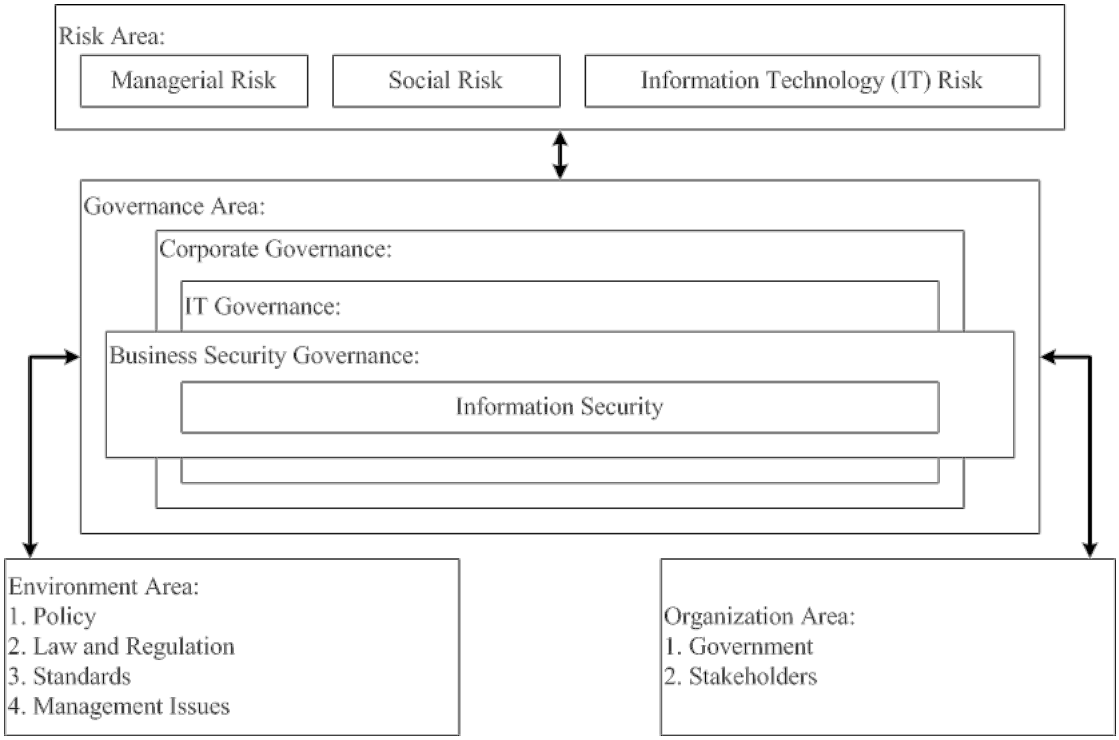


Figure 1: The scope of the ISG for e-government services

Table 2: A Comparison between ITG (ISO/IEC 38500:2008(E)) and ISMS Requirements (ISO/IEC 27001:2005(E))

Principles	**ISO/IEC 38500:2008(E) Session Number**	**ISO/IEC 27001:2005(E) Session Number**	**ISO/IEC 27001:2013(E) Session Number**
1. Responsibility	2.1.1, 3.2	4.2.1 (d), 4.2.3 (a)(3), 5.2.2	6.1.1, 6.1.2, 7.2 (a) , 7.2 (b) , 7.2 (c) , 7.2 (d), 7.3 (b), 7.3 (c), 9.1 (a)
2. Strategy	2.1.2, 3.3	4.2.1 (b)(3), 7	4.2 (b), 5.2 (a)
3. Acquisition	2.1.3, 3.4	5.2	4.2 (b), 7.1, 8.1, 9.3
4. Performance	2.1.4, 3.5	4.2.2 (b), 4.2.2 (h), 7	7.1, 8.1, 9.3
5. Conformance	2.1.5, 3.6	4.2.2 (e), 6	7.3 (b), 7.3 (c), 9.2
6. Human Behavior	2.1.6, 3.7	4.2.1 (b), 4.2.3 (a)(3)	5.1 (a), 9.1

Note: Descriptions of the six principles and guideline of ISG is in ISO/IEC 38500:2008(E).

Table 3: Illustration of the offsite backup implementation models of the ISMS risk treatment plan for a Local Tax Bureau

Implementation Models ISO/IEC 1st WD 27014 :2009-12-01	**ISO/IEC 27014 :2013-05-15**	**Description**
Process/Metrics	Communicate/Assure	Strive for the offsite backups to subsume efficient sharing work items of centralized management and response of the high quality network services of the e-government plan.
Organization/Role and Responsibilities	Direct/Evaluate	CISO is the kernel responsible. The information security officer is responsible to provide analysis reports.
Security Architecture	Proposals	Incorporate into "Integrated Local Tax Information Application Platform Program".
Investment Management	Communicate/Assure	Subsume "Local Tax Information Application Platform" and simplify administrative operations. Therefore, it shall be able to save the cost over 50%.

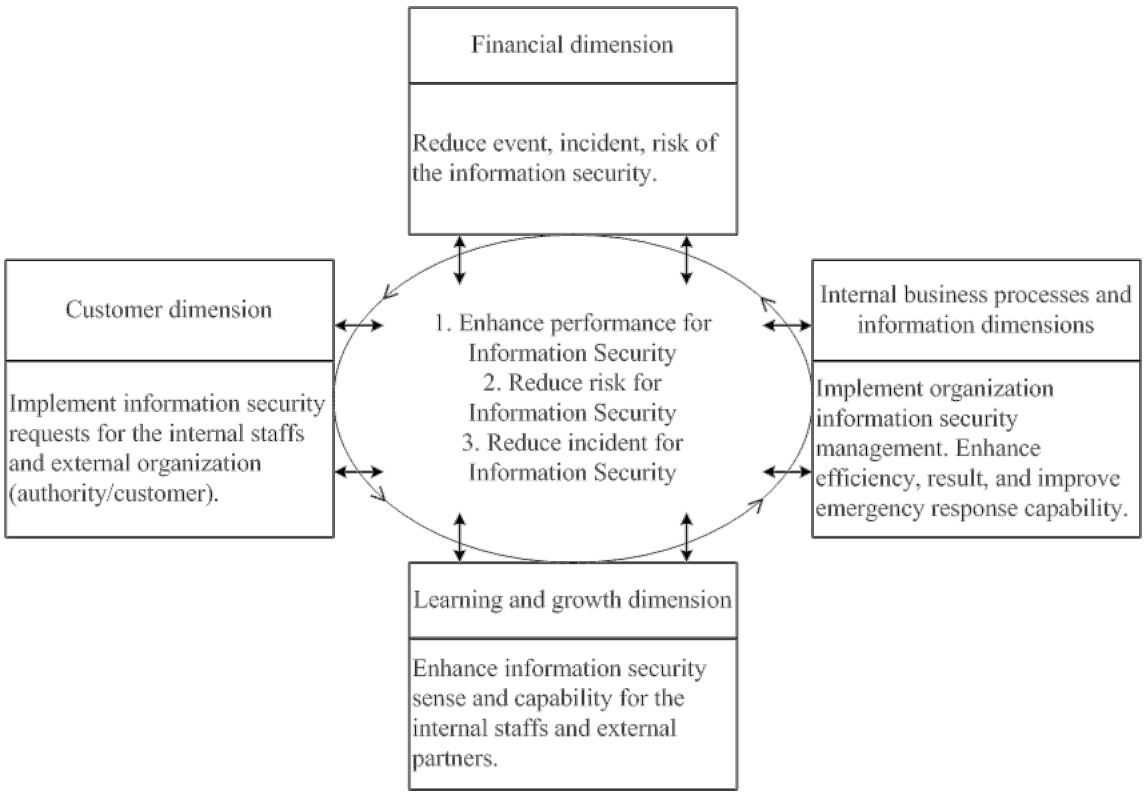


Figure 2: Balanced scorecard and ISG maturity indicators

2.2 E-government ISG of ISMS

One of the United States Federal Governments ISMS regulations is that "ISG can be defined as to establish and maintain the framework, to support the management structure and procedure, and to provide the following certified processes: under risk management, to ensure that the objectives of information security strategy and business objectives are the same, to support business objectives through stringent policy and internal control to ensure they comply with relevant regulations, and to assign duties." [5]. Based on this, requirements for action programs for regulations and guidelines, in terms of the development and maintenance of information security processes in government departments, were included in the ISG programs. Therefore, ISG projects were included in the ISMS implementation, such as "ISMS policy and organizational strategic risk management context in which the establishment and maintenance of the ISMS will take place", along with "Internal ISMS audits", as described in ISO/IEC 27001:2005(E) Section 4.2.1(b)(3) and 6. In addition, the four dimensions of the maturity evaluation of the ISG were included in Section 7.2(f) (Results from effectiveness measurements) of Section 7 (Management review of the ISMS), as shown in Figure 2. They consist of "Financial", "Customer", "Learning and growth" and "Internal business processes and information". These were used as a basis to derive the various requirements listed in Section 7.3 (Review output). They shall be feasible and valid [9, 10, 15, 17, 18].

For example, Taiwans Personal Data Protection Act adopted principles such as the prevention of damage, inform, collection restrictions, the use of personal data, restriction of autonomy, protection of personal data integrity, security management, inspection and correction, and imputable [27]. Moreover, information security development programs were asked to work in conjunction with the legislative process of Personal Data Protection in setting/amending the management regulations for personal data protection, as shown in the "Strengthen e-Government Information, Communication Security and Implementation Official Data Protection", for the information security development programs [30].

However, it remains a challenge to establish relevant indicators in accordance with the requirements in ISO/IEC 27001:2005(E) Sections 4.2.2(d) and 4.2.3(c), while also meeting the requirements of Section 7.2 (f) (Results from effectiveness measurements) in the "Assessment of the ISMS management". Achieving this would not only enable management to evaluate whether Section A.15.1.4 (Data protection and privacy of personal information) of the "Compliance with legal controls" in the ISMS fulfills the decisions and measures of the Personal Data Protection Act, but it would also allow management to assess whether its protection requirements are in full compliance with the requirements of ISO/IEC 27001:2005(E) Section 4.2.1(c)(2) (Develop criteria for accepting risks and identify the acceptable levels of risk). Furthermore, it would

allow management to determine whether the requirements to "Promote information and information system classification/grading" within the information security development programs are indeed being met [30].

Accordingly, after other e-government information security management action programs had been integrated with the ISG action programs, the relevant ISG projects were included in the implementation of the ISMS requirements, as described in Sections 4, 5, 6 and 7 of ISO/IEC 27001:2005(E), and shown in Table 2. It then became feasible to achieve improved results through the integration of the ISG with the ISMS implementation, as shown in Table 4 [19].

2.3 E-government Implementations of ISMS

Given the fact that there are still a large number of institutions that comply with ISMS certification as prescribed in ISO/IEC 27001:2005(E), but have failed the "business" requirements, NICST, in the "Implementation Program on Information Security Responsibility Classification in Governmental Departments" promulgated by information security dispatch document No. 0980100328 on June 1, 2009, by the Executive Yuan, specified that The scope of ISMS certification should initially cover organizational core business information systems, and gradually be expanded to cover the entire organization [29] (see Appendix B). On the other hand, ISO/IEC 27003:2010(E) was proposed to provide a checklist of the activities required to establish and implement an ISMS, and to support progress monitoring for ISMS implementation [19].

ISMS establishment is still one of the main factors in the above plans; however the deadline for obtaining three-party ISMS certifications for Level A and B institutions was postponed for two years. The institutions were required to complete these certifications by 2009 and 2011, respectively [29]. In addition, in order to better enforce ISMS, and to strengthen the action programs for information security quality and capability training, as shown in the "Implementation Program on Information Security Responsibility Classification in Governmental Departments", Note 3, NICST proposed a planning framework for civil servants information security awareness, and is currently preparing the training materials [34] (see Appendix B).

Therefore, the implementation effectiveness of e-government information security management measures can be improved with the establishment of an information technology security assessment framework (ITSAF), as shown in Figure 3. It is built into the action programs of the "Promote information and information system classification/grading". The relevant knowledge and skills are included in the aforementioned curriculum planning.

The cryptographic module validation program (CMVP), including the cryptographic algorithm validation program (CAVP) and common criteria evaluation and validation scheme (CCEVS), are shown in Figure 3. The main (assisting) organizers have already been established for action programs for information security development programs; however, this is not the case for the SCAP. Thus, this issue must be dealt with as soon as possible in order to fully construct a developmental environment for the implementation of e-government information security management. However, according to Figure 3, the work timetable for December 2012 remained incomplete except for CAVP, stopping the advance of the project. In other words, the root cause of this issue is the lack of ISMS design regarding technical rules in Table 4 [19]. However, Figure 3 is still the policy of security validation in the United States, but it is hard to use in the practical case. So far, it is asked to finish the assessment framework by the requirements from PPD-21 and EO 13636 by February 2016.

3 ISG Approach for E-government and Information Security Management

In the studies related to ISG, Abu-Musa [1] introduced an ISG framework that enables organizations to better understand, analyze, implement and evaluate ISG practices in order to achieve business success. The proposed ISG framework was developed based on the ISG conceptual framework proposed by the IT Governance Institute [23] and other ISG models and frameworks available in the literature [28, 33, 38, 39, 40, 41, 42, 43].

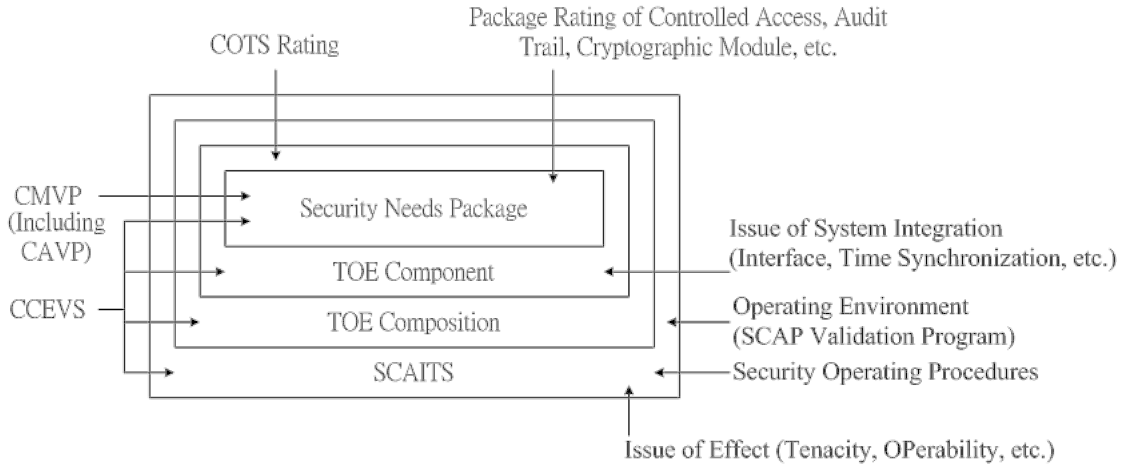
Based on the six aforementioned ITG principles and the four ISG dimensions described in Table 2 and Figure 2, as well as ISMS standards, this study proposes elements for evaluating the maturity of ISG. The specifications for policies, procedures, implementation, testing and integration in question are described as follows:

1) Policies:

- Provide all personnel with a set of formal and current policy guidelines that sets out ISMS directions.
- Establish a sustainable cycle framework and ISMS plan policy that are able to assess risks and implementation.
- Provide a policy document that covers the primary facilities and operations of regulated ISMS information assets.
- All policies must be approved in writing by management and relevant departments.
- The scope of the policy must include ISMS structure and clear division of responsibility, as well as its progress and adopted trustworthiness monitoring.
- The policy must clearly define disciplinary measures for any noncompliance.

Table 4: Description of the integration of the ISG planning sketch and phasing results in the ISMS [19]

Phase		**Obtaining management approval for initiating an ISMS project**	**Defining ISMS Scope and ISMS Policy**	**Conducting Information Security Requirements Analysis**	**Conducting Risk Assessment and Risk Treatment planning**	**Designing the ISMS**
Standard Compliance		1. ISO/IEC 27001 2. ISO/IEC 27000 3. ISO/IEC 9001, ISO/IEC 14001, and ISO/IEC 20000	1. ISO/IEC 27001 2. ISO/IEC 27005	1. ISO/IEC 27001 2. ISO/IEC 27002	1. ISO/IEC 27001 2. ISO/IEC 27002 3. ISO/IEC 27005	1. ISO/IEC 27001 2. ISO/IEC 27002 3. ISO/IEC 27004
Output	ISMS	1. Management approval for implementing the ISMS	1. The ISMS scope and boundaries 2. ISMS policy	1. Information security requirements 2. Information assets 3. The preliminary results from the information security risk assessment	1. Risk assessment reports 2. Risk treatment plan 3. Written notice of the management approval for implementing the ISMS 4. Management acceptance of residual risks 5. The Statement of the applicability	1. Information security policy 2. ISMS records and document control 3. The ISMS project implementation plan
	ISG		3. ISG principle	4. ISG assessment reports		4. ISG policy 5. The ISG project implementation plan 6. ISG records and document control



Notes:
1. CAVP: Cryptographic Algorithm Validation Program.
2. CMVP: Cryptographic Module Validation Program.
3. CCEVS: Common Criteria Evaluation and Validation Scheme.
4. COTS: Commercial Off-The-Shelf.
5. TOE: Target of Evaluation.
6. SCAITS: Security Certification and Accreditation of Information Technology Systems.
7. SCAP: Security Content Automation Protocol.,

Figure 3: United States Federal Government information technology security assessment framework

2) Procedures:

- Be able to provide a formal and current program set on the ISMS implementation control measures of a ready-defined policy
- Each program contained in the set must clearly define its applicable circumstance, method, time, object, and application details.
- The programs contained in the set are designed for the asset owners and users, information resource management and data processing personnel, management and information security administrators. Information security responsibilities and expected behaviors must be clearly defined.
- All program files must clarify the use of the ISMS control measures for action.
- All program files must be approved in writing by management and relevant departments.

3) Implementation:

- Every individual who is part of a program from the regulated program set must be fully aware of its program content.
- Programs and control measure implementation from the ISMS program collection must be integrated with organizational daily operation, and must be consistent with program application. Regular training must be provided to strengthen this implementation.
- There must be an established approach mechanism that ensures effective ISMS control measures geared toward operation efficiency.
- ISMS policies and program sets must be incorporated into ISMS awareness and training programs.
- Awareness of required knowledge and skills of ISMS personnel is required, and training and education mechanisms must be established.

4) Testing:

- Build and run creditable routine evaluation and testing mechanisms on ISMS implementation effectiveness.
- Establish ISMS control measures of appropriate information and information system level in line with policies and programs, and credible evaluation and testing capability.
- Establish credible evaluation on continuous improvement and corrective action of the ISMS implementation, and testing capability on preventive measures.
- Establish assessment and testing capability for the credibility of "Management and Respond" and "Response and Restore" of the ISMS security events and incidents.
- As the implementation of the evaluation and testing depends on risks for the ISMS operation effectiveness, such plans must be approved in writing by management and relevant departments.

5) Integration:

- The ISMS has become part of the organizational management system.
- The ISMS is part of the capital planning and investment control (CPIC).
- A review and improvement mechanism for the ISMS policies, procedures, implementation and testing has been established.
- An appropriate organizational culture geared toward promoting ISMS has been established.
- There is understanding and management of ISMS vulnerability.
- Re-evaluate and appropriately adjust ISMS control measures according to changes in the information security environment.
- Make decisions based on appropriate measured risks and costs, information security incidents and their results.

Based on Figure 4 and the ISMS standards [18, 20, 21], the subject and scope of the ISG, such as information, system and process that are necessary in the operating process must be verified. Once a consensus and conclusions are reached between the operator, personnel and relevant professionals on the standards, benchmarks and legislations to be used during the ISG process, the ISG process can be set in motion. Furthermore, the five vital components and their inter-relationships necessary for the launch of the ISG were listed in the IT assurance guide using COBIT [24].

The ISG process can be divided into three stages: planning, scoping and execution, as illustrated in the IT assurance guide using COBIT [24]. Planning is the first stage of the ISG process. In this stage, the ISG principles compatible with business and ISMS objectives are established. This indicates the link between enterprise information infrastructure and control objectives, conduct risk assessment, evaluation of threats, vulnerability, and possible impact on the business, and diagnoses risks associated with each related project. It also illustrates that it helps to think in terms of IT and ISMS resources in order to translate business goals into IT and ISMS goals, and in terms of infrastructure and human resources required to provide and support the services and information needed. Moreover, an ISG launch plan is based on risk. The identification of key business processes is based on value factors. It also assesses the degree of maturity of the ISMS process.

The second stage is scoping. It involves planning based on the area of the ISG launch, selecting control objectives

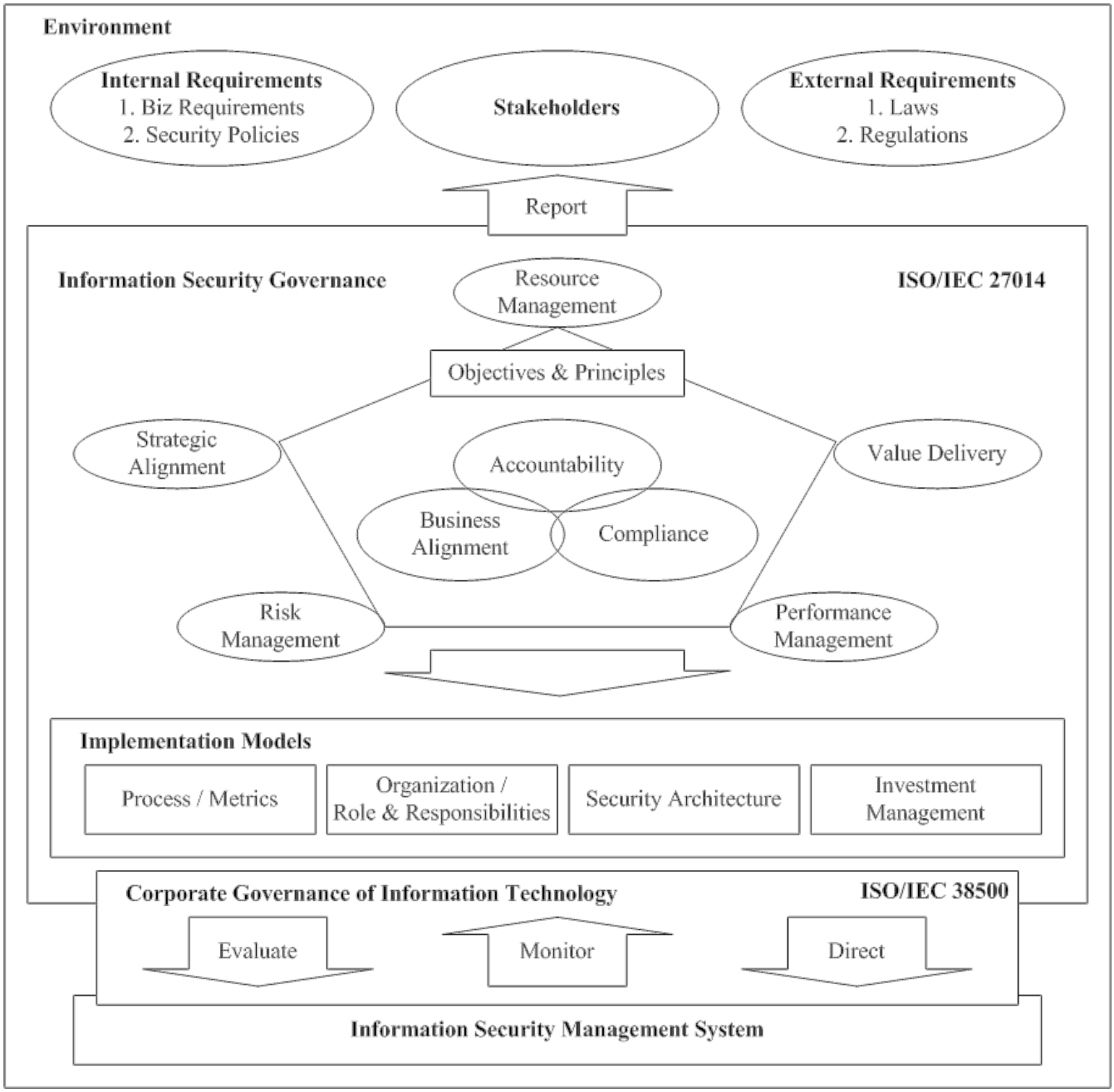


Figure 4: Elements of the ISG maturity evaluation

for key processes, and designing detailed plans according to these control objectives.

The third stage is execution. It subdivided into six steps:

Step 1. Identify or confirm key ISMS processes and self-assess the degree of maturity for the key ISMS processes.

Step 2. Update the choice of control objectives, customize the control objectives, and establish detailed audit programs.

Step 3. Test and evaluate control measures, update the level of maturity of the assessment process.

Step 4. Self-assess control measures, test and evaluate control measures.

Step 5. Diagnose residual risks in running a project; substantiate the fact that risks are under control.

Step 6. Report ISG conclusions.

From the above, it can be seen that, apart from its top-down direction, the ISG process has a great deal of overlap with the establishment of the ISMS. Therefore, it is appropriate to integrate these two processes. It is possible to achieve improved results by integrating the projects of the ISG with the ISMS implementation programs.

4 Discussion and Conclusion

A solid supply chain and functionality are crucial to the implementation of any management plans. Taking as an example the illustration of the important measures and performance indicators of "Promote Information and Information System Classification/Grading" for the information security development programs, the first point (1) "classification" is the standard of real initialization [31]. It was officially announced on July 5, 2010, during the testing period, that the investigation bureau of the ministry of justice had already confirmed the resource allocation for the financial dimension (as indicated in Figure 2), but in the working outline (2), "establish basic information security parameter criteria", the classification was only finished in September 2013.

In July 2013, the minister without portfolio, Executive Yuan, of the information and communications technology security stated that the fourth period (2013˜2016) did not have a confirmed "development project", and that this process would therefore be frozen, while the top priority work was actually the technical structure of the security operation center. On the other hand, the gradual promotion of information technology service management (ITSM) has already started, and the new policies incorporated into the security regulations have been officially adopted [31].

In order to avoid repeating the same error, these new policies should take "Backhouse et al.s circuits of power framework" into consideration. One of the main aims of this project is also to create a standard regulated environment for information security [4, 7, 13]. Scheduled in September 2013, the project already includes the IT risk cited in the technical checking section (as indicated in Figure 1), making it top priority as the first step of this long process.

The whole context of information security management is to address its diversity, mobility and complexity. The leader of different internal or external organizations will also be the main action initiator (see ISO/IEC 20000-1, Section 4.2). This section concretizes ISMS requirements through various levels or fields, using diverse equations and tools. These actions are connected in simultaneously building the ISG structure. In a four year plan, the vulnerability of standardization in ISG toward information security techniques has become an issue that ISMS must now face.

The process of ISMS standardization requires sympathy and reasoning. Sympathy refers to putting oneself in the shoes of standard creators, and seeing the standard in its entirety. A standard becomes alive when reasoning comes into play with sympathy. A standard is formed by an infinite number of chances, whether it is the cause or caused, an opportunity or the result of a trend, but it is never an accident. From a long-term perspective, one will begin to see that a standard is an unstoppable flow of trends. The reading and reasoning of ISMS standards requires the integration of both natural science and social science contexts to blend into a whole with culture and e-Taiwan.

More in-depth exploration into the establishment of top-down action programs on the ISG integrated with ISMS implementation in accordance with the framework of ISO/IEC 38500:2008(E) and ISO/IEC 27003:2009(E) is required. When the ISMS standardization process showed signs of "BananaVpeel words" and received no accusation, how to face the subject of ISMS standardization squarely became a natural phenomenon. Nevertheless, the deterioration of the ISMS quality culture will only lead to its loss of credibility in society. Confusion should be avoided on certification or the "Golden handcuffs syndrome", as that would clearly disregard the requirements of the standard. What is more important is reestablishing the fundamental value of the ISMS standardization, and restoring public faith in ISMS credibility. This should be governments top priority in the development of information security standards.

Consequently, as part of the action programs of the ISG published in the third phase of the National Information and Communications Technology Security Development Program, mentioned earlier, and due to the fact that the players that shaped ISMS decisions and mechanisms were involved with complex, multi-level governance issues, the implication is that the ISMS standardization process had developed into the realm of information security management system knowledge [2, 3]. A method of capitalizing on this opportunity should become the next

topic of key action programs in Taiwan ISMS standardization improvement [11].

Acknowledgments

The authors would like to express our appreciation to the anonymous reviewers for their useful suggestions. Besides, the authors would also like to thank the support from the Office of Information and Communication Security, Executive Yuan, Taiwan, Republic of China, and the Local Tax Bureau, Hsinchu City, Taiwan, Republic of China, for their assistance in the material.

References

[1] A. A.-Musa, "Information security governance in saudi organizations: an empirical study," *Information Management & Computer Security*, vol. 18, no. 4, pp. 226–276, 2010.

[2] I. Bache and M. Flinders, *Multi-level Governance*, Richmond, TX, USA: Oxford University Press, 2005.

[3] A. Back, G. V. Krogh, A. Seufert, and E. Enkel, *Putting Knowledge Networks into Action: Methodology, Development, Maintenance*. Berlin, Heidelberg, Germany: Springer-Verlag, 2005.

[4] J. Backhouse, C. Hsu, and L. Silva, "Circuits of power in creating de jure standards shaping the international information systems security standard," *MIS Quality*, vol. 30, pp. 413–438, 2006.

[5] P. Bowen, *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology (NIST) Special Publications 800-100, 2006.

[6] H. Chen, "Digital government: technologies and practices," *Decision Support Systems*, vol. 34, no. 3, pp. 223–227, 2003.

[7] S. R. Clegg, *Frameworks of Power*, London, UK: Sage Publications, 1989.

[8] E. Donna and D. C. Yen, "E-government: An analysis for implementation: framework for understanding cultural and social impact," *Government Information Quarterly*, vol. 22, no. 3, pp. 354–373, 2005.

[9] Executive Yuan, *Dispatch Document No. 096000567*, Taiwan, Republic of China, 2007.

[10] Executive Yuan Law and Regulation Commission, *Administrative Agency Legal Operation and Practice*, Taiwan, Republic of China, 2005.

[11] K. J. Farn, S. K. Lin, and C. C. Lo, "A study on e-taiwan information security classification and implementation," *Computer Standards & Interfaces*, vol. 30, no. 1-2, pp. 1–7, 2008.

[12] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[13] C. Hsu, "Frame misalignment: interpreting the implementation of information security certification in an organization," *European Journal of Information Systems*, vol. 18, no. 2, pp. 140–150, 2009.

[14] C. C. Huang, K. J. Farn, and F. Y. S. Lin, "A study on ISMS policy: importing personal data protection of ISMS," *Journal of Computers*, vol. 23, no. 1, pp. 35–41, 2012.

[15] ISO, *Health Informatics - Information Security Management in Health Using ISO/IEC 27002*, ISO 27799, 2008.

[16] ISO, *Resolutions of the 38th SC27 WG1 Plenary Meeting Hold in Beijing, China*, ISO/IEC JTC 1/SC 27 WG1 N17800, 2009.

[17] ISO/IEC, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, ISO/IEC 27001, 2005.

[18] ISO/IEC, *Corporate Governance of Information Technology*, ISO/IEC 38500, 2008.

[19] ISO/IEC, *Information Technology - Security Techniques - Information Security Management System Implementation Guidance*, ISO/IEC 27003, 2010.

[20] ISO/IEC, *Text for ISO/IEC 3rd WD 27014: Information Security Governance Framework*, ISO/IEC/JTC1/SC27 N8712, 2010.

[21] ISO/IEC, *Information Tchnology - Security Techniques - Governance of Information Security*, ISO/IEC 27014, 2013.

[22] ISO/IEC, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, ISO/IEC 27001, 2013.

[23] IT Governance Institute, *Information Security Governance, Guidance for Boards of Directors and Executive Management (2nd edition)*, IL, USA: Rolling Meadows, 2006.

[24] IT Governance Institute, *IT Assurance Guide Using COBIT*, IL, USA: Rolling Meadows, 2007.

[25] B. Khoo, P. Harris, and S. Hartman, "Information security governance of enterprise information systems: an approach to legislative compliant," *International Journal of Management and Information Systems*, vol. 14, no. 3, pp. 49–55, 2010.

[26] S. Lee and J. D. Kim, "A framework of business security governance," in *Proceedings of the 3rd Joint Workshop on Information Security*, pp. 213–224, 2008.

[27] Ministry of Justice, "Personal information protection act," Taiwan, Republic of China, 2010.

[28] R. Moulton and R. S. Coles, "Applying information security governance," *Computers & Security*, vol. 22, no. 7, pp. 580–584, 2003.

[29] National Information and Communication Security Taskforce, *Implementation Program on Information Security Responsibility Classification in Governmental Departments*, Information Security Dispatch Document No. 0980100328, Taiwan, Republic of China, 2009.

[30] National Information and Communication Security Taskforce, *National Information and Communications Technology Security Development Program (2009˜2012)*, Information Security Dispatch Document No. 0980100055, Taiwan, Republic of China, 2009.

[31] National Information and Communication Security Taskforce, *Reference Manual for Information Systems Classification/Grading and Authentication Mechanism*, Information Security Dispatch Document No. 0990100394, Taiwan, Republic of China, 2010.

[32] National Information and Communication Security Taskforce, *National Information and Communications Technology Security Development Program (2013˜2016)*, Information Security Dispatch Document No. 1020157911, Taiwan, Republic of China, 2013.

[33] S. Posthumus and R. von Solms, "A framework for the governance of information security," *Computers & Security*, vol. 23, no. 8, pp. 638–646, 2004.

[34] Research, Development and Evaluation Commission, *Planning Framework for Civil Servants Information Security Awareness*, Taiwan, Republic of China, 2009.

[35] S. Smith, D. Winchester, D. Bunker, and R. Jamieson, "Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization," *MIS Quarterly*, vol. 34, no. 3, pp. 463–486, 2010.

[36] G. Strejcek and M. Theil, "Technology push, legislation pull? e-government in the European Union," *Decision Support Systems*, vol. 34, no. 3, pp. 305–313, 2003.

[37] C. W. Tan and S. L. Pan, "Managing e-transformation in the public sector: an e-government study of the Inland Revenue Authority of Singapore (IRAS)," *European Journal of Information Systems*, vol. 12, no. 4, pp. 269–281, 2003.

[38] A. Da Veiga and J. H. P. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007.

[39] B. von Solms, "Information security governance: COBIT or ISO 17799 or both?," *Computers & Security*, vol. 24, no. 2, pp. 99–104, 2005.

[40] R. von Solms and S. H. von Solms, "Information security governance: a model based on the direct-control cycle," *Computers & Security*, vol. 25, no. 6, pp. 408–412, 2006.

[41] R. von Solms and S. H. von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, no. 7, pp. 494–497, 2006.

[42] S. H. von Solms, "Information security governance - compliance management vs operational management," *Computers & Security*, vol. 24, no. 6, pp. 443–447, 2005.

[43] S. H. von Solms and R. von Solms, *Information Security Governance*, New York, USA: Springer, 2008.

[44] H. Xu, H. H. Teo, B. C. Y. Tan, and R. Agarwal, "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services," *Information Systems Research*, vol. 23, no. 4, pp. 1342–1363, 2012.

[45] M. Yildiz, "E-government research: reviewing the literature, limitations, and ways forward," *Government Information Quarterly*, vol. 24, no. 4, pp. 646–665, 2007.

Chien-Cheng Huang received his M.S. degree in information management from the National Chiao Tung University in 2008, and his Ph.D. degree in information management from the National Taiwan University in 2014. He is an adjunct assistant professor with the National Taipei University of Nursing and Health Sciences. His current research interests include data mining, business intelligence, information security, and cyber/network forensics.

Kwo-Jean Farn is an adjunct associate professor with the National Chiao Tung University in Taiwan. He received his Ph.D. degree in 1982. He has had a 30-year career at Information Technology and about 20-year career at Information Security. He was the chair of the Implementation National Critical Information Infrastructure Protection Project at the Computer & Communications Research Laboratories/Industrial Technology Research Institute (CCL/ITRI) from 1999 to 2000. He had worked at the ITRI for more than 18 years until the summer of 2001. He has 9 patents in the information security area. He also received the National Standardization Award in 2009.

Appendix A: Interviewees and Documents

Position	Role	Interview method
Director, Office of Information and Communication Security, Executive Yuan	Decision Maker	Face-to-face interview
Director, Information & Communication Security Division, Investigation Bureau, Ministry of Justice	Manger	Face-to-face interview
Special Agent, Information & Communication Security Division, Investigation Bureau, Ministry of Justice	Executor	Face-to-face interview, e-mail, telephone follow-up
Associate Researcher, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Assistant Researcher, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Specialist, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Senior Advisor, National Security Council	Advisor and decision	Face-to-face interview
Commissioner, National Communications Commission (NCC)	Decision maker	Telephone interview
Deputy Director, Technologies Administration Department, NCC	Manger	Face-to-face interview, telephone follow-up
Minister without Portfolio, Executive Yuan	Decision maker	E-mail
Deputy Director, Office of Information and Communication Security, Executive Yuan	Manger	Face-to-face interview, telephone follow-up
Project Consultant, Security Technology Center, Office of Information and Communication Security, Executive Yuan	Planner	Face-to-face interview
Technical Director, Security Technology Center, Office of Information and Communication Security, Executive Yuan	Executor	Telephone interview
Specialist, National Security Council	Executor	Face-to-face interview, telephone follow-up
Chief, System Design Section/Information Division, National Immigration Agency	Manger	Telephone interview

Documents	Websites
IA (Information Assurance) Policy Chart	http://iac.dtic.mil/csiac/ia_policychart.html
FISMA (Federal Information Security Management Act) Implement Project	http://csrc.nist.gov/groups/SMA/fisma/index.html
CC (Common Criteria)	http://www.commoncriteriaportal.org/
NVD (National Vulnerability Database)	http://nvd.nist.gov/
ITIL (Information Technology Infrastructure Library)	http://www.itil-officialsite.com/
IT (Information Technology) Security Evaluation Standards (in Chinese)	http://www.ncc.gov.tw/chinese/
National information and communications technology security development program (2009˜2012) (in Chinese)	
Reference manual for information systems classification/grading and authentication mechanism (in Chinese)	
National information and communications technology security development program (2013˜2016) (in Chinese)	
Audit operational planning on information and communications technology security in governmental departments (2013) (in Chinese)	

Appendix B: Implement work requirements of "Implementation Programs on Information Security Responsibility Classification in Governmental Departments" [29]

Operating Name	Defense-in-Depth	ISMS Operating Promotion (Note 1)	Audit Modes	Educational Training of the Information Security	Professional Certificates (Note 4)	Detect Vulnerability in the Website of the Agencies
Class A	NSOC (Direct Protection) / SOC (Insourcing or Outsourcing), IDS, Firewall, Anti-Virus, E-mail Filter	Obtain third-party certification	Internal audit at least twice per year	① At least 3, 6, 18, 3 hours per year. (They fall into four categories in Note 2.); ② Obtain information security competence authentication, including information personnel and information security personnel (Note 3)	Maintain least two information security professional certificates	Twice per year
Class B	SOC (Option), IDS, Firewall, Anti-Virus, E-mail Filter	Obtain third-party certification	Internal audit at least once per year.	① At least 3, 6, 16, 3 hours per year. ② Obtain information security competence authentication, including information personnel and information security personnel (Note 3)	Maintain least one information security professional certificate	Once per year
Class C	Firewall, Anti-Virus, E-mail Filter	Self-establish the Team to Planning Operation	Self-review	At least 2, 6, 12, 3 hours per year.	Information security professional training	Once per year
Class D	Firewall, Anti-Virus, E-mail Filter	Advocacy to promote ISMS Concept	Self-review	At least 1, 4, 8, 2 hours per year.	Information security professional training	Once per year
Note 1	The scope of the ISMS certification shall cover information systems of the organizations core businesses, and be gradually expanded to cover the entire organization					
Note 2	(1) General Chief: Relevant personnel takes charge of the chief position, e.g.: president, vice-president, department chair, chief information security officer, and etc. (2) Information Personnel: Relevant personnel takes charge of the information operation, e.g.: system analysis and design personnel, system develop personnel, system management personnel, and system operation personnel, and etc. (3) Information Security Personnel: Relevant personnel takes charge of the information and communication security, e.g.: information security management personnel, information security audit personnel, and etc. (4) General User: Information system is used by the users, e.g.: administrator, accounting personnel, and etc.					
Note 3	Information security competence authentication subject includes information & communication management system, information system risk assessment, information & communication audit, government information operation outsourcing security, information security incident operation, electronic document protection, e-mail security and web application security, and etc. The information and information security personnel of the class A and B agencies take trainings of the information security and obtain certifications from the planning and holding for Research, Development and Evaluation Commission, Executive Yuan.					
Note 4	Information security professional certificates are published by the independent certification and authentication institution at home and abroad. The information security class includes ISO 27001 Lead Auditor (LA), Certified Information Security Manager (CISM), Systems Security Certified Practitioner (SSCP), Certification for Information System Security Professional (CISSP), Certified Ethical Hacker (CEH), Global Information Assurance Certification (GIAC), and etc.					

SMPR: A Smartphone Based MANET Using Prime Numbers to Enhance the Network-nodes Reachability and Security of Routing Protocols

Govand Kadir, Torben Kuseler, and Ihsan Alshahib Lami
(Corresponding author: Torben Kuseler)

Department of Applied Computing, The University of Buckingham
Hunter Street, Buckingham, MK18 1EG, United Kingdom
(Email: torben.kuseler@buckingham.ac.uk)
(Received July 25, 2014; revised and accepted Nov. 3 & Dec. 13, 2014)

Abstract

Mobile Adhoc Networks (MANETs) emerge as an effective solution for networking Smartphones to enable wireless communication when other alternatives such as cellular networks are not available, e.g. in rural areas. Available MANET routing protocols are either conservative (reactive protocols, e.g. AODV) to control overheads and so do not have any knowledge beyond neighboring nodes, or too expensive (proactive protocols, e.g. OLSR) on resources for Smartphone based MANET networks. Irrespective, all these protocols have limited protection against threats from malicious nodes in the vicinity. This paper proposes SMPR that enables nodes in the network to gain knowledge about the identity of their neighboring nodes. This is achieved by a process of mathematical factorisation of prime numbers performed during the route discovery process. The gained knowledge about their neighboring nodes addresses is then used to validate the participating nodes during data transmission. SMPR is a thin layer code slotted on top of the used MANET routing protocol. Simulation results using OPNET and AODV prove the advantages of SMPR and show that the introduced performance overhead is negligible.

Keywords: AODV, MANET, prime numbers, smartphone networks

1 Introduction

Current mobile devices like Smartphones can handle many networking communication methods (e.g. cellular 2G/3G/4G, Wi-Fi, Bluetooth, NFC) whilst users are on the move. MANETs can be setup between Smartphones easily as no infrastructure is required. This is especially helpful in rural or disaster areas, where infrastructure-based networks (e.g. cellular) are not available. Rescue teams in disaster scenarios, remote scientific missions or ramblers, who want to communicate with each other, can also benefit from this type of networking. However, MANETs lack important secure network requirements like identity of all connected nodes and security of the data communication. This is because any device can join a MANET and MANET routing protocols have limited capabilities beyond establishing communication within the signal range.

To get over these limitations, devices normally rely on information collected about other nodes identity during previous communication, or through the knowledge made available by others inside the network, to achieve "trust" in nodes joining the network. This simple "trust" model is not sufficient when the presences of many security threats that can forge or misuse this information are considered. Moreover, protection for both: a) the route discovery process, and b) all subsequent data transmissions should be kept in mind, too.

In general, MANET routing protocols can be classified into two main types (i.e. proactive and reactive) based on the timing of route discovery. A third class (hybrid) combines algorithms of the other two types [7]. Proactive routing protocols, e.g. OLSR (Optimum Link State Routing), establish routes amongst present nodes in the vicinity prior to any data transmission. These routes are stored in tables and exchanged between nodes regularly, which allow establishing data communication routes quickly. A drawback of proactive protocols is the large overhead to maintain up-to-date routing information about the nodes, which makes proactive protocols not useful in larger networks of mobile devices. The required overhead would drain the resources and battery of these devices rapidly. On the other extreme, reactive routing protocols establish connectivity on demand, whenever a node has data to transmit. The source node floods the air with route requests in an attempt to find a route to the destination. This flooding is propagated via other nodes until it reaches the desired destination. The destination then

sends a traced route reply back to the source. As an example of such reactive protocols, AODV (Ad-Hoc ON Demand Distance Vector) introduces only little overhead but requires much longer establishing a route compared to proactive protocols. In addition, both protocol types do not provide any knowledge about the network structure beyond neighboring nodes. This is a major cause for delay and can introduce security vulnerabilities [1].

Our literature survey (cp. Section 2) of enhancements to reactive and hybrid protocols to overcome these vulnerabilities without adding the overhead of reactive protocols has concluded that prime number algorithms can be a good candidate for improvements. We have further concluded that a proper implementation needs to be a thin crossover layer sitting on the top of any existing reactive protocol controlling the authenticity of the participating nodes without altering the functionality of the protocol itself. This allows using the protocol enhancement with any protocol without the need to alter the protocol implementation or standard. Therefore, SMPR bases on passing Prime Product Numbers (more specifically PPN1 and PPN2) of nodes prime IP-addresses between the nodes during route discovery. This shall provide higher security and better operation especially in larger networks, with only small overhead added to the routing protocol. AODV is chosen to prove our SMPR implementation, but any other reactive protocol [11] could also be used.

The proposed SMPR algorithm bases on the well-known mathematical concept of factoring prime numbers. For this purpose, we use IP-addresses that have a unique prime host part as the ID as further explained in Section 3. In this paper, we introduce the design and implementation of SMPR algorithm in detail and compare its performance with the standard AODV routing protocol.

The rest of this paper is organized as follows: Section 2 presents the literature review. Section 3 explains the SMPR algorithm, while Section 4 details the implementation of SMPR using the OPNET Simulator for various scenarios. Section 5 discusses and analysis the simulation results. Finally, we conclude on the SMPR performance and identify future work in Section 6.

2 Literature Review

Performance and security of MANET routing protocols grabbed the focus of many researchers. Reliability improvements in terms of data integrity and transmission accuracy, as well as reducing the communications overhead (i.e. processing time and resource power usage) were proposed. For example, AODV has the advantage of adding very little overhead to mobile nodes with their limited resources and heavy routing duties. However AODV lacks the knowledge about the transmission path node addresses beyond the next neighboring node, which may cause a security threat to the entire MANET routing protocol. Yet, adding extra knowledge of other nodes identity in the network, as in the OLSR, results in large processing time and power consumption overhead. Therefore, secure/unique identification, location information, and energy consumption are some of the targeted areas for current research, resulting in various enhancements to MANET protocols.

A prime numbers based scheme that helps avoiding malicious node attacks during route discovery by using a clustering mechanism with elected heads has been recently proposed [3]. Nodes have unique prime IDs stored with the cluster head ID in a special table that is used to validate any intermediate node that wants to forward data. The cluster head supports the source node to check the validity of the Prime Product Number (PPN) and decides the trustworthiness of the node. However, trust obtained from previous experience during data transmission is used to decide the trust factor of nodes. Nodes inside the network then pass around this trust to other nodes. This limits the ability to check the trust information passed on by other nodes and as a result, malicious nodes can pass on misleading information about trust factors.

On another vain, prime IP-addresses were used to eliminate nodes enquiry for duplicate IP-addresses by using a prime-DHCP [6]. This eliminates the need to check duplicate addresses and increases the performance by reducing the overhead and latency. Experimenting with this algorithm proofed the concept of prime IP-addresses to be useful for SMPR. Experimental results indicated that SMPR performance can be enhanced by reducing the used prime number to be the host part of the IP-address only. This will minimise the calculation overhead because the calculated PPN values will increase slower as the prime IP-address values are smaller. This avoids extra computational load on any of the involved nodes, especially in larger networks.

Furthermore, prime number based keys are used to secure the nodes ID in MANETs by using a "bilinear paring signature scheme" to reduce attacks [4]. These prime keys act as public keys and sign the RREQ and RREP messages with private keys generated by each node. However, signature based solutions are generally implemented in higher layers, which leads to extra overhead and delay. Such routing algorithms can be further enhanced to use the same prime IP-based keys from the route discovery stage to reduce attacks during the data transmission stage.

It is evident from the reviewed literature that solutions using unique IP-address mechanisms can provide knowledge beyond neighboring nodes. This will enable reactive protocols such as AODV to be more secure and reliable with a negligible introduced overhead.

Location information provided by GPS enabled nodes in a MANET can reduce the overhead of the flooding process during route discovery [5]. This is achieved as nodes can now predict the direction of the destination node and are able to drop RREQ messages passed on to the opposite direction or far away from the destination node. Doing this dynamically by directing messages in a tri-

angle shape and allowing expansion in case of failure to find a destination will improve the AODV performance and reduce the delay. However, this has major security issues, because GPS information passed around can be forged or falsified. We believe integrating GPS information with prime numbers can offer major advantages for both a) securing the route and data communication, and b) reducing the routing overhead.

Power and energy resources are also critical factors in MANET operation, as most mobile nodes are battery-powered devices. Therefore, extra networking activity caused by selfish and uncooperative nodes in MANETs, or caused by added authentication processes during the route discovery or data communication will drain their battery faster. Therefore, algorithms that consider battery power in the route discovery and/or offer added protection with minimum overhead as part of route discovery (which is one of the main ideas behind the proposed SMPR) are desirable to save energy and minimise disruption. To enhance the energy usage, a consumption reputation system can be used [9]. This system checks the energy level of nodes and passes information around using a signature-based scheme. This prevents time synchronisation problems, and extends consequently the lifetime of MANETs but adds extra processing and overhead to the nodes, too.

3 SMPR Algorithm

AODV relies on the routing table to obtain information about other nodes identity in the network when a packet arrives. During a route request (RREQ), AODV stores information about the previous node address (i.e. the node that has send the message), and uses this information later to forward the route reply (RREP) back to the original message source. In addition, AODV stores the address of the sender of the RREP message as the next node address in its routing table. These two addresses are then used during the following data transmissions between the source and destination node of the now successfully established communication route. However, relying on stored information is a potential security concern as malicious nodes may have passed wrong address information around with the aim to interrupt the data transmissions between genuine nodes [12].

To overcome this problem, the proposed SMPR adds a thin check-up process on the top of AODV to force each node in the network to use an address from a mathematical formula rather than relying on a stored address from its routing table. It is important to notice that the SMPR algorithm does not intervene in the functionality of the underlying routing protocol. It is therefore possible to use SMPR with other reactive protocols like DSR, too.

The SMPR algorithm consists of two steps; the first step is executed when a RREP message is received. The second step executes during the subsequent data transmissions. In both steps, PPN1 and PPN2 values

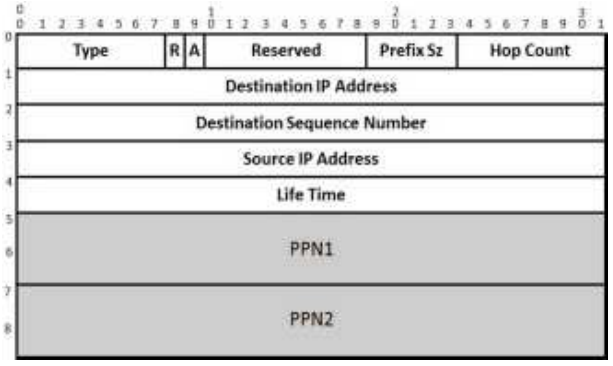


Figure 1: Extended AODV route reply (RREP) header

are used to verify the identity of the involved nodes. The core functionality of these two PPN values depends on the following mathematical factorisation formulas [2]:

Nodes: $p_1, p_2, p_3, \ldots, p_n$

$$PPN1 = p_1 * p_2 * p_3 * \cdots * p_n \quad (1)$$

$$PPN2 = (p_1 - 1) * p_2 - 1) * p_3 - 1) * \ldots) * p_n - 1) \quad (2)$$

$$Factors = GCD(PPN1, PPN2) \quad (3)$$

PPN1 (1) represents the multiplication product of prime numbers, where the pi-values are the host part of the prime IP-address of node i. PPN2 (2) represents the previous PPN1 value minus one, and allows back-tracking the original order of the factors by the receiving node. The greatest common divisor (GCD) value of PPN1 and PPN2 finally represents the factorisation of all values (3) and determines the sequence of nodes inside the path to the desired destination.

3.1 SMPR Implementation

The calculated PPN values are stored inside the individual nodes routing table as part of the SMPR thin layer implementation and passed on between nodes using RREP messages. To enable this, two new 64-bit fields containing the PPN1 and PPN2 values are added to an AODV route reply header as shown in Figure 1.

3.2 SMPR operation

Considering the following scenario in Figure 2, where nine nodes form a MANET network. To enable the sending Node S to establish an entire PPN-based route, the following conditions must be met: a) these nodes must not have any previous communication record, b) the AODV "destination only flag" is set on all nodes, and c) "gratitude reply" must be disabled. If "gratitude replies" are not disabled, then any intermediate node (e.g. node N) that have a path to the destination responds with a "gratitude reply" to the sending Node S that relies on routing table information. This should be prevented as the Node S

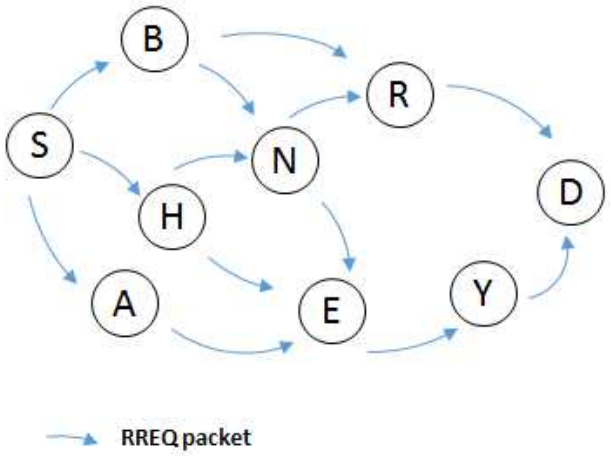


Figure 2: Route request (RREQ) flooding

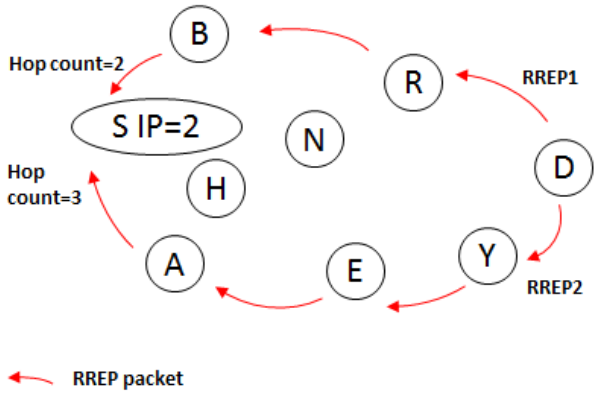


Figure 3: Route reply (RREP) message from Node D to Node S

would not have a full SMPR-based path to the destination in that case.

As mentioned earlier, SMPR does not interfere in any AODV operation. All original AODV route discovery steps are executed normally as detailed in the following paragraphs.

Route Request (RREQ). SMPR is not involved in the broadcasting process of RREQ messages. In the above example of Figure 2, the source Node S holds data that it wants to transmit to the destination Node D. To enable successful data transmission, S creates a RREQ message and broadcasts the message to all nodes that are in transmission range. Once a node receives a RREQ message from one of its neighbors, it compares the destination address to its own IP-address. If they are the same, then the node creates a RREP message. Otherwise, the node will rebroadcast the RREQ. This process continues and the RREQ spreads out inside the network until the RREQ reaches the destination node.

Route Reply (RREP). Once the RREQ has reached its destination, the RREP process starts. The destination Node D creates a RREP message and sends it back to the node from where it has received the RREQ (in our example node R as shown in Figure 3). In addition, Node D keeps a record of node Rs prime IP-address in its routing table to be used in the later data transmission stage to forward data packets.

Once node R receives the RREP, it extracts the destination address (i.e. the originator of the RREQ) from the RREP and compares it to the source address of the RREQ inside its routing table to find the node address where it should forward the RREP to. Node R then adds (or updates it if already exists) the senders IP-Address in its routing table and forwards the RREP to node B. This process continues until the RREP reaches the source Node S.

It is important to note that D receives the RREQs from both nodes, Y and R (cp. Figure 2). Therefore, it creates two separate RREP messages and sends them via the two different paths. This is useful to establish an optimal route as the source Node S can decide later based on the lowest hop count, which route to use for subsequent data delivery. In our example, Node S chooses the RREP route with a hop count of two, i.e. path "S → B → R → D" as shown in Figure 3.

SMPR follows the above-described procedure of AODV with the addition of the following PPN-related steps and calculations.

1) The destination Node D starts the additional SMPR calculations by extracting its own IP-address host part p_{own} (i.e. "11" as shown in Figure 4) as well as the previous nodes IP-address host part p_{prev} (node R with address "5"). Please note that p_{prev} is known to Node D because D received the RREQ from that node.

2) Node D calculates the two PPN values as follows:

$$PPN1 = p_{own} * p_{prev} = 11 * 5 = 55 \quad (4)$$

$$PPN2 = (p_{own} - 1) * p_{prev} - 1 = 10 * 5 - 1 = 49 \quad (5)$$

3) Node D sends the RREP message (cp. Figure 1) including the two calculated PPN values to the next node R.

4) Once the node R receives the RREP, R determines the individual prime factors from PPN1 as described in detail in [2]. PPN2 is used in this calculation to determine the correct sequence of the factor values as PPN1 might have different factor sequences, e.g. PPN1 value of "55" can be factorised as "11*5" or "5*11".

5) Once the factorisation is completed, node R checks if the last value in the calculated factor list is equal to its own IP-address host part, i.e. "5". If this is

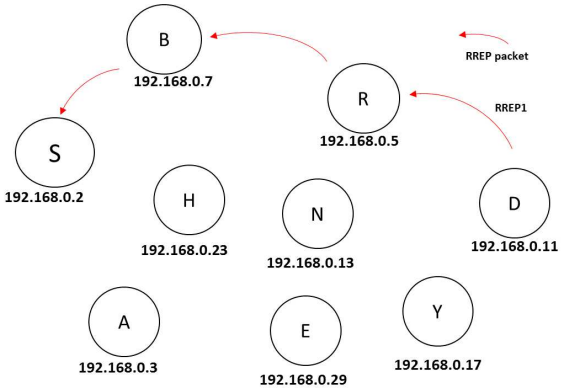


Figure 4: Route for example of PPN values calculation

the case, then the node calculates the new PPN1 and PPN2 values as described before. The only difference is that the node uses the received PPN values instead of its own p_{own} value.

$$PPN1 = PPN1_{rec} * p_{prev} = 55 * 7 = 385 \quad (6)$$

$$PPN2 = PPN2_{rec} * p_{prev} - 1 = 49 * 7 - 1 = 342 \quad (7)$$

6) Finally, node R updates the RREP message with the new PPN values and sends it to the next node, i.e. "B". If the last value of the factor list is not equal to its own IP-address then the node drops the packet. This is to prevent that the node processes a message that is not intended for that node. Lastly, it will store the new PPN values (i.e. 385 and 342) inside the routing table.

7) These steps are repeated by every node inside the path until the RREP message reaches finally the source Node S.

3.3 Data Transmission

In the original AODV, the source node retrieves the data packets from its own buffer and starts the data transmission by sending data to the next node of the previously established route. This next node receives the packet and forwards it to the following node based on the node address retrieved from its routing table. Besides message forwarding, nodes update the expiry time of the particular route entry to avoid that the route will become invalid. This process continues until the data packet reaches the destination Node D as described in Figure 5.

In SMPR, the source node factorises the PPN values to determine the next nodes prime IP-address. The source node then sends the data packet to the next address in the calculated PPN factor list. Upon arrival of the data packet, the next node factorises its own stored PPN, and accepts the packet only if the senders prime IP-address is equal to the number before its own number in the factor list. If this is the case, then the node forwards the packet

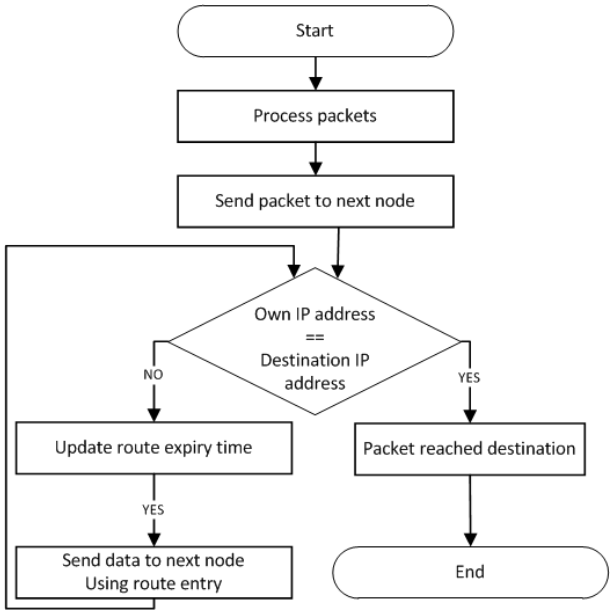


Figure 5: AODV data transmission flowchart

to the next address from the factor list rather than looking for the next address in the routing table. By doing this, SMPR prevents that data packets follow any other path than the path defined via the PPN list. This process continues until the data packet reaches the destination Node D as described in Figure 6.

4 SMPR Implementation

4.1 OPNET Modeller Implementation

SMPR was implemented and tested using the OPNET Modeller [10]. OPNET provides a flexible and highly organised architecture that allows the reusability and extendibility of existing models. OPNET consists of different layers, whereby each layer handles different functionality of the node structure as shown in Figure 7. AODV is a child process of a MANET manager process ("manet_mgr" in Figure 7), which in return is a child of the "ip_dispatch" layer. The added SMPR thin layer is located between the original OPNET AODV implementation and the MANET manager ("manet_mgr").

Integration of this thin SMPR layer requires the following additions and modifications on top of the original AODV process implementation inside the OPNET Modeller:

- Changing the IP-address assignment algorithm to a prime-DHCP algorithm, e.g. [6].
- Adding two extra fields to hold PPN1 and PPN2 in a RREP packet inside the RREP create function.
- Update the RREP send and forward functions to point to values in the PPN factor list, and save the

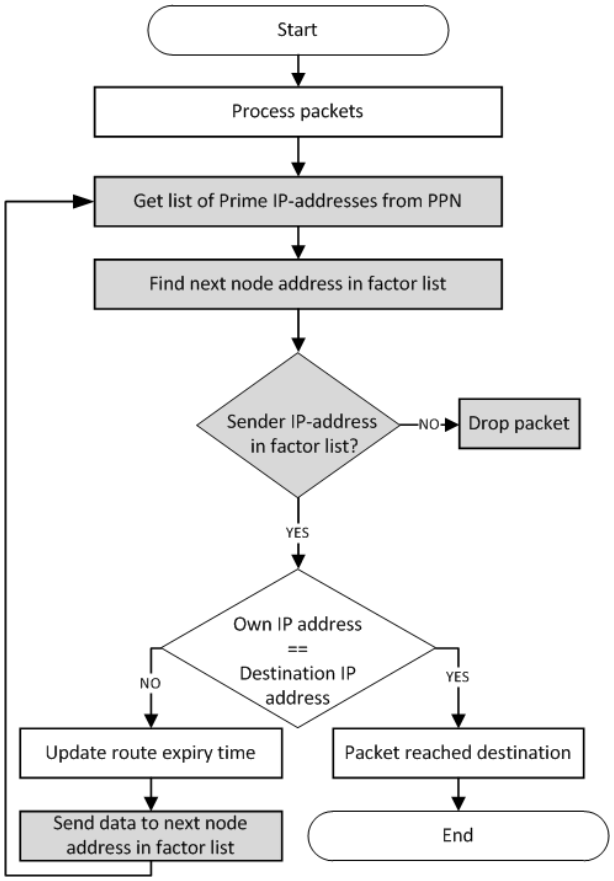


Figure 6: SMPR data transmission flowchart

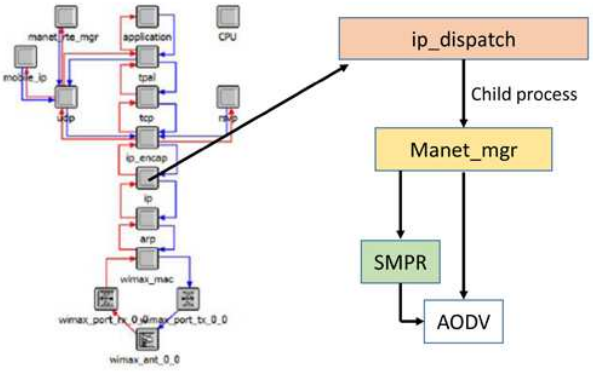


Figure 7: SMPR algorithm inside OPNET WLAN hierarchical architecture

PPN values in the routing table to be used for data transmission.

- Modify the send and forward data packet functions to point to PPN factor values.
- Update the expiry time function to include the PPN values.

4.2 Simulation Setup

Two main scenarios were used to measure the impact of adding SMPR on top of AODV. For each scenario, several node and network characteristics were changed as described below to evaluate the SMPR network performance in terms of introduced overhead and delay:

Node Mobility. Node mobility is defined in OPNET via different configuration parameters like trajectory movement, distance between nodes, and node speeds. Changing these values effects the network performance characteristics like throughput or Packet Delivery Ratio (PDR) [13]. The IEEE 802.11 WLAN standard defines that the distance between two nodes should not exceed 300m. To comply with this condition, the node transmission power in the simulations is set to 0.0005Watt and the packet reception power to -82.65dBm.

Number of Nodes. The network density (i.e. the number of nodes per area unit) has an impact on the network performance, too. A higher network density results normally in nodes having more alternative routes between each other. This can help preventing congestion and can improve the overall performance of the routing [8].

Data Transmission Rate. Mobile nodes feature different data transmission rates and hence, transmission ranges, as describe in the IEEE 802.11g standard. These differences affect the performance of the routing protocol as nodes with a high transmission range might reach nodes that a node with a lower rate cannot reach [14].

In order to assess the effect of the above factors on the performance of our scenarios, the following statistics were collected and evaluated:

Route Discovery Time (RDT). RDT is the time required for the RREQ to reach the destination plus the time required for the RREP to arrive back at the source.

End-to-End Delay (E2E-D). E2E-D represents the time delay that the packet encountered during transmission from the source to the destination.

Packet Retransmission. The average number of packets retransmitted during data transmission.

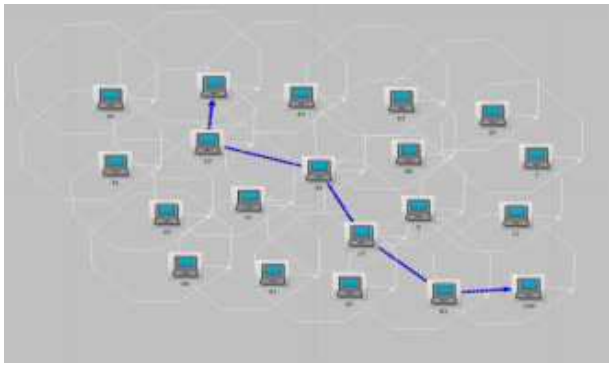


Figure 8: Scenario-I: 20 mobile nodes and their trajectory paths

Two scenarios were used to evaluate SMPR. The first scenario compares the performance of SMPR with normal AODV in a network of twenty 802.11g MANET stations placed in an area with a distance of less than 300m between any two nodes and data rates of 6, 12, 18, 24, and 36Mbps. The simulation considers two nodes sending a data stream in opposite direction as shown in Figure 8. Each transmission will trigger a response back to the sender. Each of these transmissions has an average volume of 500Mbytes per flow. All transmissions are sent concurrently.

The second scenario observes the effect of different node mobility characteristics and network layouts on the performance of AODV and SMPR. This scenario includes 20 nodes placed in five different layouts as shown in Figure 9.

The overall node and traffic characteristics for the first and second scenarios are shown in Table 1.

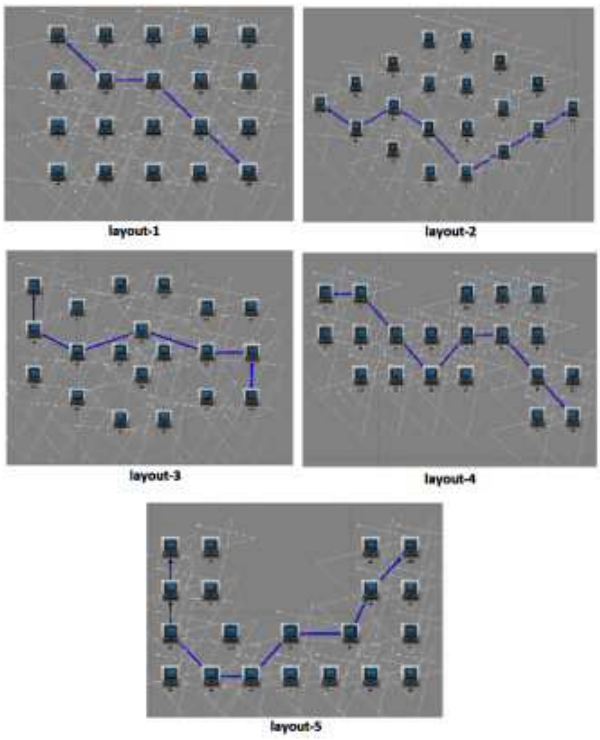


Figure 9: Scenario-II: 20 mobile nodes arranged in 5 different layouts

5 Simulation Result and Analysis

Route Discovery Time (RDT) and Data Transmission (DT) values are used to analyse the collected simulation results and evaluate the effect and performance of SMPR.

Route Discovery Time (RDT) is measured as the average packets round trip time required to successfully receive a RREP from the destination. From the SMPR algorithm design, one can expect that SMPR will introduce a small overhead compared to the original AODV protocol due to the additional PPN values calculations. As can be seen from Figure 10, this introduced RDT overhead is around 0.01msec for data rates of 6, 12, and 18 Mbps respectively. However, this overhead becomes negative for large networks, e.g. for data rates of 24 and 36 Mbps. This is because SMPR already determined the next/previous nodes addresses. Therefore, there will be no need for accessing the AODV routing table to obtain these IP addresses.

The second scenario was further sub-divided into five different layouts as described in section IV.B to evaluate different node setups and network topologies. Table 2

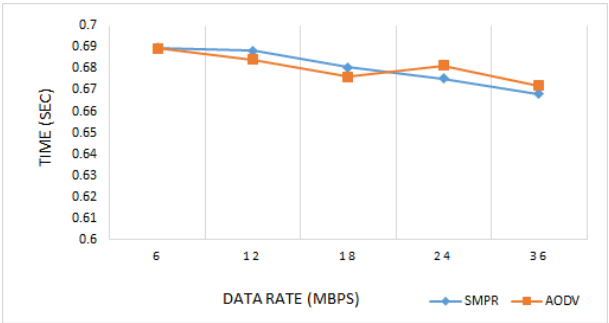


Figure 10: Scenario-I: Route discovery time (RDT)

Table 1: Simulation scenario parameters

Parameter	Value
Trajectory	2 Hexagonal movements: Clockwise & Counter clockwise Movement range: 300m * 300m
Speed	Scenario-I: 2m/s; Scenario-II: 10, 20, 30, 40, and 50 m/s
Distance between two nodes	50, 100, 150, 200, and 250 m (only Scenario-II)
Data rate	Scenario-I: 6, 12, 18, 24, and 36 Mbps Scenario-II: 24 Mbps
Packet interval time variance	1 msec
Node traversal Time	0.04 sec
Packet reception power threshold	-82.65 dBm
Transmission power	0.0005 Watt
Active route timeout	3 sec
Buffer timeout	2 sec
Traffic mix	0.977 GB, all explicit
Simulation Duration	300 sec

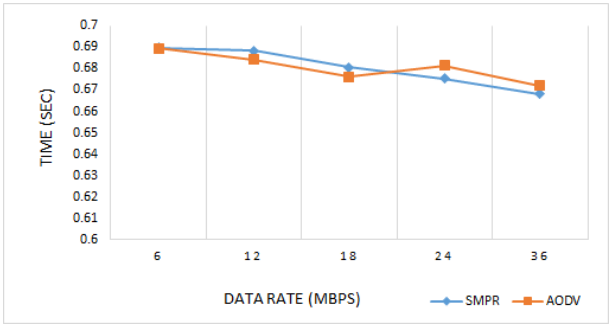


Figure 11: ScenarioII: RDT for the five different layouts

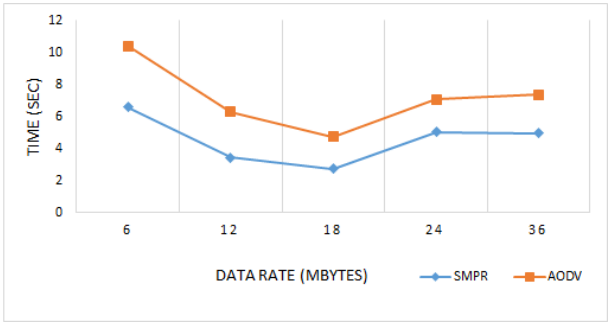


Figure 12: Scenario-II: RDT with different node trajectory speeds

shows the number of hops per route for the five different layouts.

RDT for the first layout is smaller compared to the other layouts as can be seen from Figure 11. This is due to the smaller number of hops in this layout. For the other four layouts, the RDT is very similar as the number of hops is in a similar range, i.e. 6 to 8 hops. In the first layout, SMPR has a slight advantage over AODV (0.453sec RDT compared to 0.456sec for AODV). On average over all five scenarios, SMPR requires only 0.612sec compared to 0.617sec for AODV alone. This is due to the saving achieved by not requiring fetching the IP address of the next node operation.

The nodes speed was the second factor changed to evaluate SMPR. In the simulations, layout-1 was used with five different trajectory node speeds of 10, 20, 30, 40, and 50 m/sec respectively. One can notice from Figure 12 that AODV has a slightly higher RDT compared to SMPR. This is due to the advantage gained by the SMPR factor lists that helps getting the address of the next node faster than accessing this information from the AODV routing table.

The third factor changed was the distance between the different nodes. Layout 1 was used again, this time with a fixed speed. Instead, the distance between two nodes was incremented by 50meters for each simulation. Simulation results show that the RDT increases with increasing distance between any two nodes (cp. Figure 13). This is mainly due to the time it takes the packet to travel on air between the nodes.

Data Transmission (DT) is examined through two statistics: average packet retransmission and end-to-end delay. As mentioned in the scenario setup (cp. Section 4.B), data transmission happens in two opposite directions with the destination nodes sending responses to the source node for each received data packet in the first scenario. These simulations examine the capability of nodes handling different packets in both directions simultaneously. Simulation results show that normal AODV retransmits on average of 7.17 packets compared to an average of 4.65 packets retransmitted using SMPR (cp. Figure 14). This can be explained by the fact that AODV holds only one routing table entry for each route. In our

Table 2: Number of hops per route for simulation II

Layout	Number of hops per route	
	AODV	SMPR
Layout-1	4	4
Layout-2	7	7
Layout-3	6	6
Layout-4	7	7
Layout-5	8	8

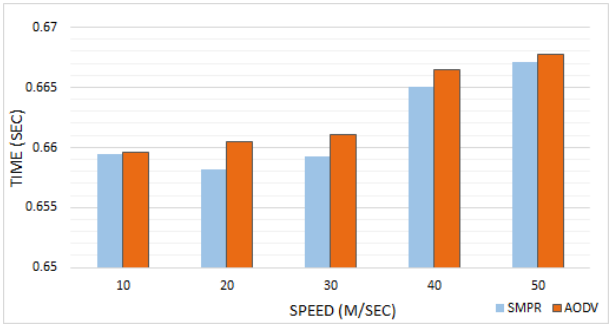


Figure 13: Scenario-II: RDT with different distances between two nodes

Figure 14: Scenario-I: Average packet retransmission

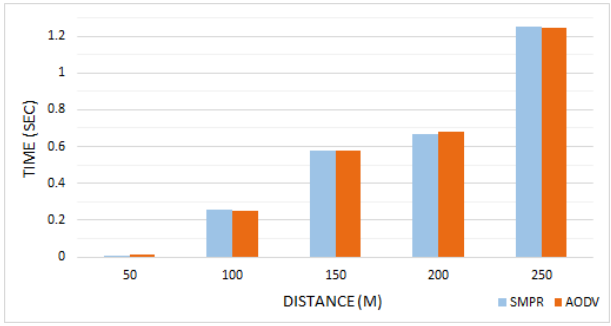


Figure 15: Scenario-I: End-to-End delay

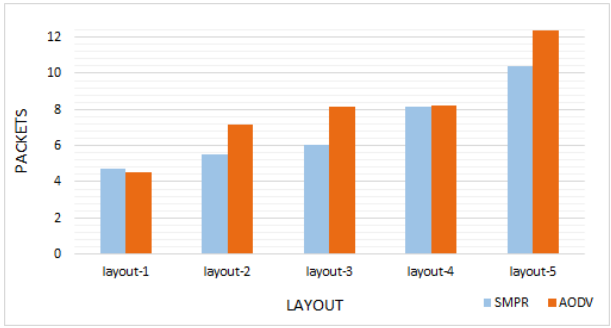


Figure 16: Scenario-II: Average packet retransmission

scenarios, transmissions occur in both directions, which means that AODV needs to figure out the correct direction, i.e. next nodes IP-address from the routing table as there is no check for the senders address. In contrast, SMPR checks the sender nodes IP-address and selects the next nodes IP-address accordingly from the calculated PPN values. As this is faster, SMPR can handle more packets at the same time compared to AODV which results in less packet drops, i.e. packet retransmissions. This clearly shows SMPRs advantage in reducing packet retransmission, as evident in the end-to-end delay times shown in Figure 15 and Figure 17. In scenario two simulation results showed an increase in packet retransmission for the different layouts for both AODV as well as SMPR (cp. Figure 16). This is also due to the increase in the number of hops per route as shown earlier in Table 2.

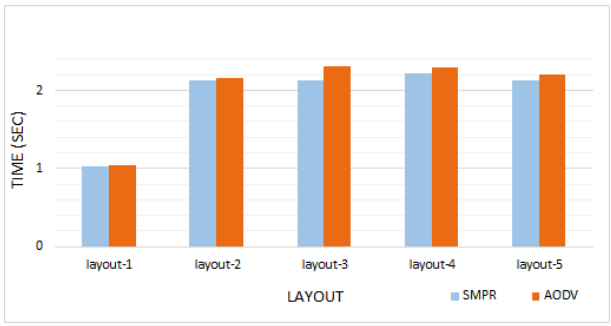


Figure 17: Scenario-II: Average End-to-End delay

6 Conclusion and Future Work

The obtained simulation results clearly show that the implementation of the thin SMPR layer on top of AODV does not introduce a noticeable overhead or delay. Instead, SMPR improves the routing performance by adding certainty about the involved nodes in the transmission, as well as reduces the route discover as well as data transmission time by providing faster access to neighbor node addresses via the PPN lists. It is also important to mention that SMPR helps any node taking part in the communication to gather knowledge knowledge about the identity of nodes beyond their directly neighboring nodes. This information is provided via the PPN factor list and enables the node to identify the direction of packets for two opposite data flows.

Future work will enhance the knowledge beyond neighbors to have the distance between two nodes and the remaining battery power of each node. This will support the source to make crucial decisions about the selected route for transmission. In addition, the algorithm will be enhanced further by permitting already known nodes with prime IP addresses to assign unique identification to newly joined forging nodes that has any IP address and using these IDs instead of their IP addresses. The addition of location information available in wireless enabled devices for example via GPS provides the ability to prevent attacks like wormhole attacks, which is hard to detect when the standard AODV protocol is used.

References

[1] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *15th IEEE International Conference on Computer Modelling and Simulation*, pp. 693–698, 2013.

[2] A. Al-Sherbaz, *Wimax-Wifi Techniques for Baseband Convergence And Routing Protocols*, Ph.D. Thesis, Applied Computing Department, The University of Buckingham, Aug. 2010.

[3] S. Gambhir and S. Sharma, "PPN: Prime product number based malicious node detection scheme for manets," in *2013 IEEE 3rd International Conference on Advance Computing Conference (IACC'13)*, pp. 335–340, 2013.

[4] U. Ghosh, "Identity based schemes for securing mobile ad hoc networks," in *2012 IEEE 26th International Conference on Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12)*, pp. 2514–2517, 2012.

[5] V. Hnatyshin, "Improving manet routing protocols through the use of geographical information," *International Journal of Wireless & Mobile Networks*, vol. 5, no. 2, pp. 19, 2013.

[6] Y. Y. Hsu, C. C. Tseng, et al., "Prime DHCP: A prime numbering address allocation mechanism for manets," *IEEE Communications Letters*, vol. 9, no. 8, pp. 712–714, 2005.

[7] D. Kaur and N. Kumar, "Comparative analysis of aodv, olsr, tora, dsr and dsdv routing protocols in mobile ad-hoc networks," *International Journal of Computer Network and Information Security*, vol. 5, no. 3, pp. 39, 2013.

[8] L. U. Khan, F. Khan, N. Khan, M. N. Khan, and B. Pirzada, "Effect of network density on the performance of manet routing protocols," in *2013 IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT'13)*, pp. 1089–1092, 2013.

[9] G. S. Kumar, M. Kaliappan, and L. J. Julus, "Enhancing the performance of manet using eescp," in *2012 IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME'12)*, pp. 225–230, 2012.

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

[11] L. Pal, P. Sharma, and N. Kaurav, "Performance analysis of reactive and proactive routing protocols for mobile ad-hoc–networks," *ISROSET-International Journal of Scientific Research in Network Security and Communication*, vol. 1, pp. 1–4, 2013.

[12] M. Patel and S. Sharma, "Detection of malicious attack in manet a behavioral approach," in *2013 IEEE 3rd International Conference on Advance Computing Conference (IACC'13)*, pp. 388–393, 2013.

[13] R. Paulus, P. D. Kumar, P. C. Philiips, and A. Kumar, "Performance analysis of various ad hoc routing protocols in manet using variation in pause time and mobility speed," *International Journal of Computer Applications*, vol. 73, no. 8, pp. 35–39, 2013.

[14] P. Ramano, "The range vs. rate dilemma of wlans," *Wireless Net DesignLine*, 2004.

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 Computer Science in 2006 from London south bank university. In 2010, he joined the doctoral program in the Applied Computing Department at The University of Buckingham, UK. While pursuing his degree, Mr. Kadir works since 2007 as a researcher and lecturer for the department of Computer Science and engineering at the University of Kurdistan-Hawler. 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. His research is supervised by Dr Ihsan Lami and Dr Torben Kuseler.

Torben Kuseler is a Lecturer in Computer Science and IT Manager at the University of Buckingham, UK. Torben received a Diploma degree in Information Technology with Business from the Applied University

of Wedel, Germany, in 2003 and a M.Sc. degree in Computer Science from the same University in 2005. After moving to the UK., Torben finished his Ph.D. in 2012 at the Applied Computing Department, University of Buckingham, UK. His research focuses on localisation and software protection techniques to enhance authentication security in mobile applications and wireless networks as well as efficient and secure management of Big Data in the cloud. Torben is also the Technical Director of the Dickens Journals Online (DJO: http://djo.org.uk) project, an open access, online edition of the two journals Dickens edited from 1850 to 1870. Please visit http://uk.linkedin.com/in/tkuseler/en and http://www.buckingham.ac.uk/directory/dr-torben-kuseler/ for more details.

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 Smartphone solutions; (2) LTE and Cognitive wireless networks access/security solutions. Please visit http://www.buckingham.ac.uk/directory/dr-ihsan-lami/ for more details.

Cryptanalysis of Tseng-Wu Group Key Exchange Protocol

Chung-Huei Ling[1], Shih-Ming Chen[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Medical Research, China Medical University Hospital, China Medical University[2]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received Oct. 7, 2014; revised and accepted Feb. 8 & Apr. 16, 2015)

Abstract

Recently, Tseng and Wu pointed out that the second protocol of Biswas's two-party keys scheme based on the Diffie-Hellman technique has a security weakness and proposed a new protocol to remedy the weakness. In this article, we point out that Tseng-Wu's protocol is vulnerable to a man-in-the-middle attack. An attacker could intercept, delete, or modify the communicated messages between two communicating party or among the group members.

Keywords: Diffie-Hellman key-exchange, group key, man-in-the-middle attack, multiple two-party keys

1 Introduction

When two communicating parties want to communicate with each other privately, they first need to establish a session key for secure communication in future. The session key is used to encrypt/decrypt their communicating messages with symmetric-key cryptosystem, such as DES, RC4 [1], or AES. [19]. It's important for securely obtaining the common session key between two communicating parties. In 1976, Diffie and Hellman first proposed a key agreement protocol to solve this problem [6]. Two participants exchange their public parameter through a public channel to generate a shared session key between them [5, 7, 9, 10, 11, 16, 21, 22, 26].

The Diffie and Hellman's key agreement protocol is only applied between two communicating parties. We said that the Diffie and Hellman's key agreement protocol is a 2-party key agreement protocol [2, 6, 12, 17, 25]. Recently, many group key management and distribution protocols had been proposed for multi-party [8, 13, 23, 27]. In the multi-party key agreement protocols, session keys are computed dynamically through cooperation of all participants [4, 15].

In 2008, Biswas [3] proposed two key agreement protocols based on the two-party Diffie-Hellman technique. The Biswas's first protocol allows two participants to generate 15 shared keys through the exchange of two pair of public parameters through a public channel. Although, Biswas's first protocol is superior to Diffie-Hellman protocol which only generates a single shared key through the exchange of one pair of public parameters. However, the Biswas's first protocol is vulnerable to the man-in-the-middle attack [20]. The man-in-the-middle attack is that an attacker secretly relays and alters the communicating messages between two communicating parties [14, 18, 28].

The Bitwas's second protocol is an extension of the two-party Diffie-Hellman technique to generate a group key for participants of a large group. However, Tseng and Wu pointed out that the Bitwas's second protocol has a weakness and proposed a new protocol to remedy the weakness in 2010 [24].

The rest of this paper is organized as follows. In Section 2, we review Tseng-Wu group key exchange protocol. In Section 3, we show a man-in-the-middle attack on Tseng-Wu's Protocol. Finally, our brief conclusions will be drawn in Section 4.

2 Review of Tseng-Wu Group Key Exchange Protocol

In this section, we review the Tseng and Wu's group key exchange protocol based on the two-party Diffie-Hellman technique [24]. The protocol allows a group members to generate a shared group session key K. The detailed steps are described as follows and in Figure 1.

1) Each participant U_i $(i = 1, 2, 3, ..., (n-1))$ selects a random value $x_i \in Z_q^*$, and then computes and sends $X_i = g^{x_i} \bmod p$ to the group controller U_n. The group controller U_n also selects a random value $x_n \in$

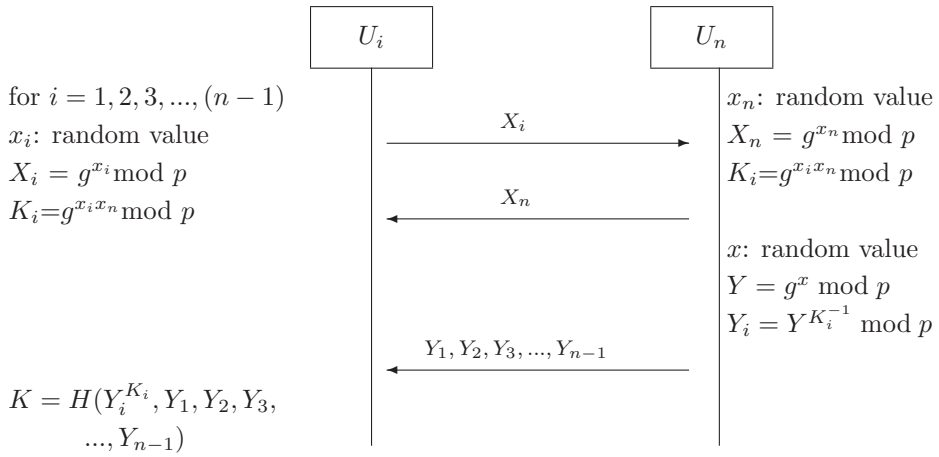


Figure 1: Tseng-Wu group key exchange protocol

Z_q^* and sends $X_n = g^{x_n} \bmod p$ to each participant U_i. Then, each U_i and U_n can compute a two-party shared key $K_i = g^{x_i x_n} \bmod p$ $(i = 1, 2, \cdots, (n-1))$. Here, p is a large positive integer; g is a group generator.

2) U_n selects a random value $x \in Z_q^*$ and computes $Y = g^x \bmod p$ and $Y_i = Y^{K_i^{-1}} \bmod p$, for $i = 1, 2, \cdots, (n-1)$. Then, U_n broadcasts $(Y_1, Y_2, \cdots, Y_{n-1})$ to each participant. Finally, each participant U_i $(i = 1, 2, \cdots, (n-1))$ can compute the group key $K = H(Y_i^{K_i}, Y_1, Y_2, \cdots, Y_{n-1})$.

3 Man-in-the-Middle Attack on Tseng-Wu Protocol

In this section, we show that Tseng and Wu's protocol is not secure against a man-in-the-middle attack. We assume that an adversary U_A could intercept and modify the communications among the group members. Then, the adversary could derive the group key to destroy the Tseng and Wu's protocol. The attack scenario is outlined in Figure 2. A more detailed description of the attack is as follows:

1) An adversary U_A stands the middle between each participant U_i, $i = 1, 2, \cdots, (n-1)$ and the group controller U_n.

2) The adversary U_A randomly chooses a random value x_a. He/she computes $X_a = g^{x_a} \bmod p$.

3) Each U_i wants to send X_i to U_n. U_A intercepts X_i and sends X_a to U_n.

4) U_n then sends X_n to each U_i. In the same way, the adversary U_A also intercepts X_n and sends X_a to each U_i.

5) Then, U_n and U_A can compute a two-party shared key $K_i' = g^{x_n x_a} \bmod p$.

6) Each U_i and U_A can compute a two-party shared key $K_i" = g^{x_i x_a} \bmod p$ $(i = 1, 2, \cdots, (n-1))$.

7) U_n computes Y and Y_i and wants to send Y_i to each U_i, $i = 1, 2, \cdots, (n-1)$. U_A intercepts Y_i and computes $Y_i' = (Y_i^{K_i'})^{K_i"^{-1}} \bmod p$ for each U_i, $i = 1, 2, \cdots, (n-1)$.

8) Then, U_A broadcasts $(Y_1', Y_2', \cdots, Y_{n-1}')$ to each participant U_i.

9) Finally, each participant U_i $(i = 1, 2, \cdots, (n-1))$ can compute the group key $K = H(Y_i^{'K_i"}, Y_1', Y_2', \cdots, Y_{n-1}')$.

10) On the other hand, U_A can also compute the group key

$$K = H(Y_i^{K_i'}, Y_1', Y_2', Y_3', ..., Y_{n-1}').$$

Since $Y_i^{'K_i"} = Y_i^{K_i'}$, the group key K between each U_i and U_A is the same value. Then, the adversary can use the group key to decrypt the communications among the group members. Therefore, the protocol is not secure against the man-in-the-middle attack.

4 Conclusions

In this article, we have showed the security weakness of Tseng-Wu's protocol. Tseng-Wu's protocol cannot resist the man-in-the-middle attack. Through the attack, an attacker can intercept, delete, modify or alter the communicated messages between two communicating party or among the group members.

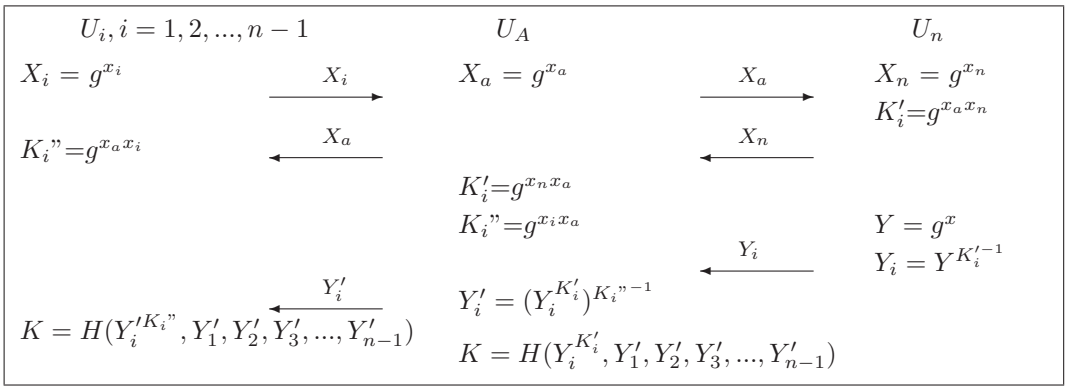


Figure 2: Man-in-the-middle attack on Tseng-Wu protocol

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: MOST 103-2221-E-468 -026, NSC 103-2622-E-468-001-CC2, and NSC 103-2622-H-468-001-CC2.

References

[1] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, A. A. Elngar, "EA based dynamic key generation in RC4 ciphering applied to CMS," *International Journal of Network Security*, vol. 17, no. 4, pp. 405–412, 2015.

[2] K. Azimian, J. Mohajeri, and M. Salmasizadeh, "Weak composite Diffie-Hellman," *International Journal of Network Security*, vol. 7, no. 3, pp. 383–387, 2008.

[3] G. P. Biswas, Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key," *IET Information Security*, vol. 2, no. 1, pp. 12–18, 2008.

[4] C. C. Chang, L. Harn, and T. F. Cheng, "Notes on "Polynomial-Based Key Management for Secure Intra-Group and Inter-Group Communication", *International Journal of Network Security*, vol. 16, no. 2, pp. 143–148, 2014.

[5] K. M. Cheng, T. Y. Chang, and J. W. Lo, "Cryptanalysis of security enhancement for a modified authenticated key agreement protocol", *International Journal of Network Security*, vol. 11, no. 1, pp. 55–57, 2010.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[7] M. S. Farash, M. A. Attari, "A pairing-free ID-based key agreement protocol with different PKGs", *International Journal of Network Security*, vol. 16, no. 3, pp. 168–173, 2014.

[8] A. Gawanmeh, A. Bouhoula, and S. Tahar, "Rank functions based inference system for group key management protocols verification", *International Journal of Network Security*, vol. 8, no. 2, pp. 187–198, 2009.

[9] 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.

[10] L. C. Huang and M. S. Hwang, "An efficient MQV key agreement scheme", *International Journal of Network Security*, vol. 16, no. 2, pp. 157-160, 2014.

[11] Q. Jiang, J. Ma, G. Li, and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy", *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[12] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection", *International Journal of Network Security*, vol. 7, no. 1, pp. 120-129, 2008.

[13] A. A. Kamal, "Cryptanalysis of a polynomial-based key management scheme for secure group communication", *International Journal of Network Security*, vol. 15, no. 1, pp. 68-70, 2013.

[14] C. T. Li and 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.

[15] W. T. Li, C. H. Ling, and M. S. Hwang, "Group rekeying in wireless sensor networks: A survey", *International Journal of Network Security*, vol. 16, no. 6, pp. 401-410, 2014.

[16] J. P. Lin, J. M. Fu, "Authenticated key agreement scheme with privacy-protection in the three-party setting", *International Journal of Network Security*, vol. 15, no. 3, pp. 179-189, 2013.

[17] J. Liu and J. Li, "A better improvement on the integrated Diffie-Hellman-DSA key agreement protocol", *International Journal of Network Security*, vol. 11, no. 2, pp. 114–117, 2010.

[18] J. W. Lo, M. S. Hwang, and C. H. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy", *Information Sciences*, vol. 181, no. 4, pp. 917–925, 2011.

[19] National Institute of Standards and Technology, *Specification for the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication (FIPS) 197, Nov. 26, 2001. (`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`)

[20] H. T. Pan, J. R. Sun, and M. S. Hwang, "Cryptanalysis of Biswas's multi-party keys scheme based on the Diffie-Hellman technique", in *Advances in Engineering Research*, vol. 15, pp. 842–847, Atlantis Press, 2015.

[21] Y. K. Peker, "A new key agreement scheme based on the triple decomposition problem", *International Journal of Network Security*, vol. 16, no. 6, pp. 426–436, 2014.

[22] M. Rajaram and T. D. Suresh, "An interval-based contributory key agreement", *International Journal of Network Security*, vol. 13, no. 2, pp. 92–97, 2011.

[23] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. Chidambaram Kalimuthu, and R. Dharmaraj, "Secure Group Key Management Scheme for Multicast Networks", *International Journal of Network Security*, vol. 11, no. 1, pp. 33–38, 2010.

[24] Y. M. Tseng and T. Y Wu, "Analysis and improvement on a contributory group key exchange protocol based on the Diffie-Hellman technique", *Informatica*, vol. 21, no. 2, pp. 247–258, 2010.

[25] T. Thomas, "Secure two-party protocols for point inclusion problem", *International Journal of Network Security*, vol. 9, no. 1, pp. 1–7, 2009.

[26] L. Wang and C. K. Wu, "Efficient key agreement for large and dynamic multicast groups", *International Journal of Network Security*, vol. 3, no. 1, pp. 8–17, 2006.

[27] F. Wang, C. C. Chang, Y. C. Chou, "Group authentication and group key distribution for ad hoc Networks", *International Journal of Network Security*, vol. 17, no. 2, pp. 199–207, 2015.

[28] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object", *International Journal of Network Security*, vol. 1, no. 2, pp. 81–83, 2005.

Chung-Huei Ling received his M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California , USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and radio frequency identification.

Shih-Ming Chen received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999; the M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2003. He is currently pursuing his PhD degree in Computer Science and Information Engineering from Asia University. His current research interests include information security and Science & Technology of Chinese studies.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. 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 the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Cryptanalysis of a Secure and Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems

Chin-Yu Sun[1], and Ching-Chun Chang[2]
(Corresponding author: Chin-Yu Sun)

Department of Computer Science, National Tsing-Hua University[1]
Hsinchu, Taiwan 30013, R.O.C.
Department of Information Management, National Central University[2]
Taoyuan, Taiwan 32001, R.O.C.
(Email: sun.chin.yu@gmail.com)
(Received Mar. 15, 2014; revised and accepted June 5 & July 25, 2015)

Abstract

In 2012, Yeh and Tsaur proposed an advanced scheme for access control in mobile pay-TV systems based on pairing and elliptic curve, which were inherent in the cryptography of Sun and Leu's scheme. In their paper, they pointed out two weaknesses in Sun and Leu's scheme and tried to overcome these weaknesses. However, we still found that Yeh and Tsaur's scheme was not secure. In this research, we will show that an attacker who obtains an obsolete, previous session key can easily break Yeh and Tsaur's scheme. The analysis shows that Yeh and Tsaur's scheme is not secure for practical applications.

Keywords: Authentication, conditional access system, cryptanalysis, pay-TV services

1 Introduction

With the tremendous breakthroughs in wireless network technologies and electronic commerce, television payment systems (i.e., pay-TV systems) have become one of the most significant modes of payment in multimedia services. Pay-TV systems allow viewers to selectively purchase their favorite programs and control the access of those authorized viewers to paid TV programs. For these reasons, the issue of authorization in pay-TV systems has become important and attracted a lot of attention.

In the early stages of designing pay-TV systems, researchers tried to utilize the properties of conditional access systems (CASs) to obtain more secure and convenient control of users' access. Several CASs based on symmetric cryptosystems have been proposed [2, 3, 8]. Unfortunately, researchers have found that schemes based on symmetric cryptosystems are insecure. For this reason, different types of pay-TV schemes have been proposed. In 2000, Lee [5] designed an authentication protocol based on the digital-signature technique. In Lee's scheme, pay-TV systems can deal effectively with the problems of privacy and non-repudiation. In 2003, Song and Korba [7] proposed an RSA-based authentication protocol for pay-TV systems. In 2009, Sun and Leu [9] proposed an authentication scheme for pay-TV systems using a bilinear pairing technique [1] and elliptic curve cryptography [4, 6]. However, Yeh and Tsaur [10] pointed out that there were two security flaws in Sun and Leu's scheme, i.e., 1) failure in subscriber authentication and 2) unauthorized access. Also, Yeh and Tsaur proposed an advanced scheme to improve these security flaws, but we found that Yeh and Tsaur's scheme still does not have adequate security. Specifically, their scheme cannot resist Type II adverse event (Section 3). This shortcoming will be demonstrated and analyzed in detail in the following section.

2 Yeh and Tsaur's Scheme

In this section, first, we review Yeh and Tsaur's scheme, and, then, we discuss its weakness. Yeh and Tsaur's scheme is divided into four phases: 1) initialization, 2) issue, 3) subscription, and 4) hand-off. Here, we omit descriptions of Phases 3 and 4 because the weakness has no immediate impact in those phases. A more-detailed description of Yeh and Tsaur's scheme are given in [10].

2.1 Initialization Phase

First, the server must choose an elliptic curve E (with order q) and a base point P. Then, the server sets a cyclic additive group G_1 (with order q), multiplicative group G_2 (with order q), and a bilinear map e ($G_1 \times G_1 \rightarrow G_2$). At the same time, the server chooses two

secret numbers x and $k_s \in Z_q^*$ to generate $A_S = x \cdot P$ and $Z_S = k_s \cdot A_S$. Then, the server encodes a service identity number SIN to $GSIN = (x_{SIN}, y_{SIN}) \in G_1$ and encodes its identity ID_S by a one-way hash function $H_1(\cdot)$, which maps $\{0,1\}^* \rightarrow G_1$. After that, the server publishes $Q_S = H_1(ID_S)$, A_S, and $GSIN$.

After self-setting, the server helps the i^{th} user to compute $Q_i = H_1(ID_i)$ and choose one secret key x_i. Then, the server generates an authentication public key $A_i = x_i \cdot P$ and two private keys $P_i = x_i \cdot Q_i$ and $Z_i = x_i \cdot A_S$. Furthermore, the server encodes ID_i to $GID_i = (x_{ID_i}, y_{ID_i}) \in G_1$. Finally, the server sends Q_i, P_i, A_i, Z_i, and GID_i via a secure channel.

2.2 Issue Phase

When the user i wants to access the service, he or she can execute the issue phase. In this phase, first, the user selects one secret key $k_i \in Z_q^*$ to generate the authentication parameters as $a_i = k_i \cdot A_i$, $E_i = k_i \cdot P$, $X_i = k_i \cdot A_S$, $C_i = k_i \cdot P_i + k_i \cdot x_{sk} \cdot Q_S$, $UID_i = GID_i + k_i \cdot y_{sk} \cdot Z_S$, and $USIN_i = GSIN + k_i \cdot (x_{sk} + y_{sk}) \cdot A_S$. After all of the authentication parameters have been generated, the user sends the message $Auth_i = \{a_i,E_i,X_i,C_i,UID_i,USIN_i\}$ to the server to request service.

After the server receives the message $Auth_i$ from the user, the server generates the session key $SK_i = a_i \cdot x = (x_{sk},y_{sk}) \in G_1$. Then, the server can decrypt UID_i and $USIN_i$ to extract GID_i and $GSIN$. After that, the server can decode GID_i and $GSIN$ to ID_i and SIN, respectively. Finally, the server computes and verifies the equation $e(C_i,A_S)? = e(Q_i,SK_i) \cdot e(Q_S,x_{sk} \cdot X_i)$ to verify the identity of the user, where $e(\cdot)$ is a bilinear paring map. After passing the verification, the server can use received parameters to compute $Y_i = Q_i \cdot x$, $Y_G = \sum_{i=1}^{m} Y_i$, $Q_G = \sum_{i=1}^{m} Q_i$, $\lambda_K = H_2(SIN,(Y_G + Z_S))$, and a certification token $CT = e(Y_G,Q_G) \cdot \lambda_K$. Then, the server sends the message $Auth_S = \{Y_G,Q_G,CT\}$ to the user.

Then, after the user receives the message $Auth_S$, he or she can compute and verify the equation $e(Y_G,a_i)? = e(Q_G,SK_i)$ to verify the validity of the server. If the equation holds, the user can generate her or his own individual certification token $CT_i = CT \cdot e(Y_G,(Q_G - Q_i))^{-1}$; otherwise, the user terminates the procedure.

2.3 Security Analysis

Two types of adverse events were pointed out by Yeh and Tsaur in [9], i.e., 1) an attacker can modify the authentication parameters and pass the subscriber authentication and 2) an attacker can use one previous session key to gain access to services. Yeh and Tsaur claimed that their scheme could withstand both of these adverse events. Upon careful assessment of their security analysis, we were able to demonstrate that Yeh and Tsaur's scheme can be defeated by a Type II adverse event. In order to obtain more clear security analyses, we developed a scenario to analyze Yeh and Tsaur's scheme. Here, we assume that there is an attacker, Justin, who obtains the previous round's session key SK_i from his target user i. Then, we can proceed to accomplish the scenario as described below.

First, Justin intercepts the message $Auth_i = \{a_i,E_i,X_i,C_i,UID_i,USIN_i\}$, which was transmitted between the user i and the server. Also, he can use the session key SK_i and the parameters UID_i and $USIN_i$ to extract GID_i and $GSIN$ by computing $GID_i = UID_i - (y_{sk} \cdot SK_i)$ and $GSIN = USIN_i - ((x_{sk} + y_{sk}) \cdot SK_i)$. Second, Justin chooses a random number J to generate one fake session key $SK_i' = a_i x \cdot J = (x'_{sk},y'_{sk})$ and computes the fake parameters as $a_i' = a_i \cdot J$, $E_i' = E_i/cdotJ$, $X_i' = X_i \cdot J \cdot (x'_{sk})^{(-1) \cdot x_{sk}}$, $C_i' = C_i \cdot J$, $UID_i' = GID_i + y'_{sk} \cdot SK_i'$, and $USIN_i' = GSIN + ((x'_{sk} + y'_{sk}) \cdot SK_i')$. After that, he sends the fake message $Auth_i' = \{a_i',E_i',X_i',C_i',UID_i',USIN_i'\}$ to the server.

After receiving the message $Auth_i'$, the server begins to use its secret number x to generate the session key $SK_i' = a_i' \cdot x = (x'_{sk},y'_{sk})$. Then, the server computes $GID_i = UID_i' - (y'_{sk} \cdot SK_i')$ and $GSIN = USIN_i' - ((x'_{sk} + y'_{sk}) \cdot SK_i')$. Furthermore, the server can use extracted parameters GID_i and $GSIN$ to map ID_i and SIN. Finally, the server computes and verifies the equation $e(C_i',A_S)? = e(Q_i,SK_i') \cdot e(Q_S,x'_{sk}X_i')$ to verify the validity of the user. However, the fake parameters that were generated by Justin can still pass the verification. The details of the equation are shown as follows:

$$
\begin{aligned}
& e(C_i', A_S) \\
= \; & e(J \cdot k_i \cdot P_i + J \cdot k_i \cdot x_{sk} \cdot Q_S, A_S) \\
= \; & e(J \cdot k_i \cdot x_i \cdot Q_i, A_S) \cdot e(J \cdot k_i \cdot x_{sk} \cdot Q_S, A_S) \\
= \; & e(Q_i, A_S)^{J \cdot k_i \cdot x_i} \cdot e(Q_S, A_S)^{J \cdot k_i \cdot x_{sk}} \\
= \; & e(Q_i, x \cdot P)^{J \cdot k_i \cdot x_i} \cdot e(Q_S, J \cdot k_i \cdot x_{sk} \cdot A_S) \\
= \; & e(Q_i, J \cdot k_i \cdot x_i \cdot x \cdot P) \cdot e(Q_S, J \cdot k_i \cdot x_{sk} \cdot A_S) \\
= \; & e(Q_i, SK_i') \cdot e(Q_S, x'_{sk}X_i').
\end{aligned}
$$

According to the above derivation, we see that Justin can use the fake parameters to cheat the server successfully. Most importantly, the original session key SK_i that protects the services in the pay-TV system was replaced by the fake session key SK_i'. However, Justin can compute and generate $SK_i' = SK_i \cdot J$, thereby obtaining unauthorized access to the pay-TV system.

3 Conclusions

Although Yeh and Tsaur proposed an advanced scheme for pay-TV systems to overcome the weaknesses in Sun and Leu's scheme, their advanced scheme still has a serious security flaw. In this research, we pointed out Yeh and Tsaur's advanced scheme is insecure. Using a simple and clear attack scenario, we showed that an unauthorized attacker can modify the transmitted message and cheat the server by gaining access easily.

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Proceedings of 21st Annual International Cryptology Conference*, vol. 2139, pp. 213-229, California, USA, 2001.

[2] ETSI, *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection*, Technical Specification ETSI-TS-102-474-V1.2.1, 2009. (`http://www.etsi.org/deliver/etsi_ts/102400_102499/102474/01.02.01_60/ts_102474v010201p.pdf`)

[3] Y. L. Huang, S. P. Shieh, F. S. Ho, and J. C. Wang, "Efficient key distribution schemes for secure media delivery in pay-TV systems", *IEEE Transactions on Multimedia*, vol. 6, no. 5, pp. 760–769, 2004.

[4] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[5] N. Y. Lee, C. C. Chang, C. L. Lin and T. L. Hwang, "Privacy and non-repudiation on pay-TV systems", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 20–27, 2000.

[6] V. S. Miller, "Use of elliptic curves in cryptography", in *Proceedings of Advances in Cryptology (CRYPTO'85)*, vol. 218, pp. 417–426, California, U.S.A., 1985.

[7] R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection", *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 408–413, 2003.

[8] H. M. Sun, C. M. Chen and C. Z. Shieh, "Flexible-Pay-Per-Channel: A new model for content access control in pay-TV broadcasting systems", *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 1109–1120, 2008.

[9] H. M. Sun and M. C. Leu, "An efficient authentication scheme for access control in mobile pay-TV systems", *IEEE Transactions on Multimedia*, vol. 11, no. 5, pp. 947–959, 2009.

[10] L. Y. Yeh and W. J. Tsaur, "A secure and efficient authentication scheme for access control in mobile pay-TV systems", *IEEE Transactions on Multimedia*, vol. 14, no. 6, pp. 1690–1694, 2009.

Chin-Yu Sun received the MS degree in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan in 2013. He is currently pursuing his Ph.D. degree in computer science from National Tsing Hua University, Hsinchu, Taiwan. He current research interests include information security, cryptography, wireless communications, mobile communications, and cloud computing.

Ching-Chun Chang was born in Taiwan. He is presently an undergraduate student of the Department of Information Management, National Central University, Taoyuan, Taiwan. His current research interests include Information Security, Data Communication as well as E-Commerce Applications

.

On the Security of Privacy-preserving Keyword Searching for Cloud Storage Services

Fuh-Gwo Jeng[1], Shu-Yuan Lin[2], Bing-Jian Wang[2], Chih-Hung Wang[2], Tzung-Her Chen[2]
(Corresponding author: Tzung-Her Chen)

Department of Applied Mathematics, National Chiayi University[1]
Department of Computer Science and Information Engineering, National Chiayi University[2]
Chiayi City, Taiwan 60004, R.O.C.
(Email: thchen@mail.ncyu.edu.tw)
(Received Apr. 21, 2014; revised and accepted Jan. 5 & Jan. 16, 2015)

Abstract

While the traditional public-key encryption schemes with keyword search (PEKS) were pointed out suffering the performance problems, some high-performance PEKS recently have drawn more attentions. Unfortunately, these performance-enhanced schemes could encounter the same security attacks as the traditional PEKS met before. In this paper, Liu et al.'s privacy-preserving keyword searching scheme for cloud storage services (SPKS) is pointed out suffering the security attack of confidentiality. Precisely, an outside attacker could perform the test process by collecting the transmitted ciphertexts and trapdoors from senders and receivers, respectively. Thus, the relationship between encrypted data and the trapdoors is disclosed. An improved version is presented to avoid the security attacks and, furthermore, to benefit the advantages of SPKS as well.

Keywords: Designated tester, privacy-preserving keyword searching, public-key encryption schemes with keyword search, searchable encryption

1 Introduction

In order to protect the confidentiality of sensitive data in cloud-computing environments, a reliable searchable encryption mechanism is required to encrypt the sensitive data. When a user issued a keyword search onto those encrypted data, only the server (a designated tester) chosen by a sender is able to perform the test by checking the relationship between a ciphertext and a trapdoor. However, an adversary is not allowed to do so [3, 5, 9, 10].

The public-key encryption scheme with keyword search (PEKS) was first proposed by Boneh et al. [1]. Based on Boneh et al.'s scheme, Hwang and Lee [4] proposed another PEKS for a multi-receiver environment. In 2010, the concept of proxy re-encryption was applied in keyword searching by Shao et al. [8] and by Yau and Phan [11] as well. Recently, Rhee et al. [7] enhanced the trapdoor security to prevent from off-line keyword-guessing attacks.

In order to enhance the performance, Liu et al. [6] proposed a secure privacy-preserving keyword searching scheme for cloud storage services (SPKS), which enabled the cloud service provider (CSP) to participate in the partial decipherment to obtain an intermediate result of the decipherment before returning the search results. In such a way, the communication and computational overhead was reduced greatly in decryption process for the user.

However, Liu et al.'s scheme met a potential security problem. That is, anyone can perform the test process by collecting the transmitted ciphertexts and the corresponding trapdoors. Therefore, any outside attacker can further construct the relationship between the encrypted data and the given trapdoors of known keywords. The confidentiality is not guaranteed any more. Thus, consequently, an improved SPKS scheme is presented to prevent from the attacks mentioned above and at the same time to inherit the advantages of SPKS as well.

2 The Security of Liu et al.'s Keyword Searching for Cloud Storage Services

In this section, Liu et al.'s SPKS scheme is briefly reviewed and the readers may refer to [7] for details. Finally, its security problem will be pointed out in the later.

2.1 Review of Liu et al.'s SPKS Scheme

In the scenario, there are three participants including the user (sender), the server (CSP), and the receiver.

1) *Global setup:* Determine two cyclic groups G_1 and G_2 with prime order p , and their admissible bilinear paring function $\hat{e} : G_1 \times G_2 \rightarrow G_2$. Given a random element $g \epsilon G_1$ and let H_1, H_2, H_3, H_4 and H_5 are random

oracles, where $H_1, H_3 : \{0,1\}^* \rightarrow G_1^*, H_2, H_5 : G_2 \rightarrow \{0,1\}^{log^q}$, and $H_4 : G_2 \rightarrow \{0,1\}^n$. The plaintext space includes $m\epsilon\{0,1\}^n$ for some n and $W\epsilon\{0,1\}^*$. The ciphertext space includes $C_m = G_1^* \times \{0,1\}^n$ and $C_W \epsilon G_2$.

2) *KeyGen:* The server (resp. receiver) generates his private key by randomly choosing $sk_{CSP} = x\epsilon\mathbb{Z}_q$ (resp. $sk_R = y\epsilon\mathbb{Z}_q$) and the corresponding public key by computing $pk_{CSP} = g^x$ (resp. $pk_R = g^y$).

3) *EMBEnc:* To encrypt an email m under a receiver's public key g^y and CSP's public key g^x, the user selects a random element $r, t\epsilon\mathbb{Z}_q$, computes

$$u_1 = g^r, u_2 = t \oplus H_5(\hat{e}(g^y, g^x)^r),$$
$$u_3 = m \oplus H_4(\hat{e}(H_3(t), (g^y)^r)),$$

and sets the ciphertext $C_m = \langle u_1, u_2, u_3 \rangle$.

4) *KWEnc:* To encrypt m's keywords $W_1, ..., W_k (k\epsilon\mathbb{Z}^+)$ under a receiver's public key g^y, the user computes $C_{W_i} = H_2(\hat{e}(g^y, H_1(W_i)^r))$, where $W_i\epsilon\{W_1, ..., W_k\}$, and sends $\langle C_m, C_{W_1}, ..., C_{W_k} \rangle$ to CSP.

5) *TCompute:* To retrieve only the emails containing keyword $W_j (j\epsilon\mathbb{Z}^+)$, the receiver computes the trapdoor $T_{W_j} = H_1(W_j)^y \epsilon G_1$ under a receiver's private key , and sends it to CSP.

6) *KWTest:* To determine whether a given email contains keyword W_j, CSP tests whether the equation $C_{W_i} = H_2(\hat{e}(u_1, T_{W_j}))$ holds.

7) *PDecrypt:* To obtain an intermediate result of the decipherment, CSP calculates $t = u_2 \oplus H_5(\hat{e}(g^y, u_1)^x)$, computes $C_t = \hat{e}(H_3(t), u_1)$, and sends $\langle C_m, C_{W_1}, \cdots, C_{W_k}, C_t \rangle$ to the receiver.

8) *Recovery:* Given the ciphertext $C_m = \langle u_1, u_2, u_3 \rangle$ and C_t, the receiver computes $m = u_3 \oplus H_4((C_t)^y)$ to recover the message m.

2.2 Security Problem

Since an outside attacker may intercept the transmitted ciphertexts from senders and the trapdoors from receivers. Without the key, the outside attacker also can easily check if the equation $C_{W_i} = H_2(\hat{e}(u_1, T_{W_j}))$ holds.

The scheme called secure means that attackers have no feasible way to deduce any information about secret. However, this attack does not need to face the hard problem on which a cryptosystem relies. It's worthwhile to note that the cost of this attack by intercepting and checking the above equation is low. That is, the attack is feasible. Therefore, the relationship between encrypted data and the given trapdoors of known keywords is able to be constructed. That is, the security information of linkage between them is revealed. This is why the designated-tester scheme is essential for searchable encryption schemes.

3 Improvement of Liu et al.'s SPKS Scheme

Inspired by Hu and Liu's scheme [2], the enhanced SPKS scheme consisting of the following processes is proposed.

1) *Global setup:*The first process is the same as that setup in Liu et al.'s.

2) *KeyGen:*CSP generates his private key by randomly choosing $sk_{CSP} = x\epsilon\mathbb{Z}_q$ and the corresponding public key by computing $pk_{CSP} = g^x$. The receiver generates his private key by randomly choosing $sk_R = \langle y, z \rangle \epsilon\mathbb{Z}_q$ and the corresponding public key by computing $pk_R = \langle k_{R1}, k_{R2}, k_{R3}, k_{R4} \rangle = \langle g^y, g^{zy^2}, g^{yz}, (pk_{CPS})^z \rangle$.

3) *EMBEnc:*To encrypt an email m under a receiver's public key $k_{R1} = g^y$ and CSPs public key g^x, the sender selects a random element $r, t\epsilon\mathbb{Z}_q$, and computes
$u_1 = g^r, u_2 = t \oplus H_5(\hat{e}(g^y, g^x)^r)$,
$u_3 = m \oplus H_4(\hat{e}(H_3(t), (g^y)^r))$,
and sends the ciphertext $C_m = \langle u_1, u_2, u_3 \rangle$.

4) *KWEnc:* To encrypt m's keywords $W_1, ..., W_k (k\epsilon\mathbb{Z}^+)$ under the receiver's public key $k_{R2} = g^{zy^2}$ and $k_{R4} = g^{zx}$, the user computes $C_{W_i} = \langle A, B \rangle = \langle (k_{R2}^r), H_2(\hat{e}(k_{R4}, H_1(W_i)^r)) \rangle$, where $W_i\epsilon\{W_1, ..., W_k\}$, and sends $\langle C_m, C_{W_1}, ..., C_{W_k} \rangle$ to CSP.

5) *TCompute:* To retrieve the emails containing keyword $W_j (j\epsilon\mathbb{Z}^+)$, the receiver computes the trapdoor $T_{W_j} = \langle T_1, T_2 \rangle = \langle (pk_{CSP})^{r'}, H_1(W_j)^{1/y^2} \cdot g^{r'} \rangle$ where $r'\epsilon\mathbb{Z}_q$ is randomly chosen by the receiver, and sends it to CSP.

6) *KWTest:* To determine whether a given email contains keyword W_j, CSP should compute $T_3 = (T_2)^x / T_1 = H_1(W_j)^{x/y^2}$ with the private key x, and then check if $H_2(\hat{e}(A, T_3))$ is equal to B.

7) *PDecrypt:* To obtain an intermediate result of the decipherment, CSP calculates $t = u_2 \oplus H_5(\hat{e}(g^y, u_1)^x)$ and $C_t = \hat{e}(H_3(t), u_1)$, and sends $\langle C_m, C_{W_1}, \cdots, C_{W_k}, C_t \rangle$ to the user.

8) *Recovery:* Given the ciphertext $C_m = \langle u_1, u_2, u_3 \rangle$ and C_t, the receiver computes $m = u_3 \oplus H_4((C_t)^y)$ to recover the message m.

4 Discussions

4.1 Correctness

The correctness of searchable encryption, i.e. *KWTest*, is described as follows.

$$\begin{aligned} B &= H_2(\hat{e}(k_{R4}, H_1(W_i)^r)) \\ &= H_2(\hat{e}(g^{xz}, H_1(W_i)^r)) \\ &= H_2(\hat{e}(g, H_1(W_i))^{xzr}) \\ &= H_2(\hat{e}(g^{y^2zr}, H_1(W_i)^{x/y^2})) \\ &= H_2(\hat{e}(A, T_3)). \end{aligned}$$

If $W_i = W_j, H_1(W_i)^{x/y^2} = H_1(W_j)^{x/y^2} = T_3$. Hence, $B = H_2(\hat{e}(A, H_1(W_i)^{x/y^2})) = H_2(\hat{e}(A, T_3))$.

4.2 Security

Since the outside attacker doesn't have CSP's private key sk_{CSP} to compute $T_3 = (T_2)^x/T_1 = H_1(W_j)^{x/y^2}$,even if an outside attacker obtains the ciphertext C_m and the trapdoor T_{W_j}, (s)he still cannot perform the test process. Suppose *Alice* is an attacker. Assume that $T_w = \langle T_1, T_2 \rangle$ is a trapdoor. To retrieve a correct keyword w from the given T_w, it should be possible if *Alice* obtains $H_1(w)^{1/y^2}$ or $H_1(w)$ from T_w.

Because a discrete logarithm problem is hard, *Alice* has no feasible way to obtain the unknown r' or $x \epsilon \mathbb{Z}_q$ from $T_1 = (pk_{CSP})^{r'}$ where $pk_{CSP} = g^x$.

Furthermore, even though *Alice* can compute

$$\begin{aligned} & e(pk_{CSP}, T_2)/e(g, T_1) \\ = \; & e(g^x, H_1(w)^{1/y^2} \cdot g^{r'})/e(g, (g^x)^{r'}) \\ = \; & e(g^x, H_1(w)^{1/y^2}). \end{aligned}$$

Alice has no feasible way to guess keyword w by computing $e(pk_{CSP}, H_1(w)^{1/y^2})$ without knowing receiver's secret key y or CSP's secret key x.

Even CSP can obtain $g^{r'}$ from T_1 using its secret key $pk_{CSP} = x$, CSP cannot successfully guess the keyword by checking if $e(k_{R4}, T_2) = e(k_{R4}, g^{r'})e(g, H_1(w'))$.

5 Conclusions

In this paper, the security weakness in Liu et al.s scheme is pointed out. To benefit from Liu et al.'s scheme, i.e., efficiency, an improved version is proposed to solve their weakness and to keep the advantages of Liu et al.'s scheme as well.

Acknowledgments

This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC 102-2221-E-415-014- and NSC 102-2221-E-415-007-.

References

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, "Public-key encryption with keyword search," in *Proceedings of EUROCRYPT'04*, LNCS 3027, pp. 506-522, 2004.

[2] C. Hu, P. Liu, "A secure searchable public key encryption scheme with a designated tester against keyword guessing attacks and its extension," in *Communications in Computer and Information Science*, vol. 215, pp. 131-136, 2011.

[3] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search," *International Journal of Network Security*, vol. 15, no. 2, pp. 71–79, 2013.

[4] Y. H. Hwang, P. J. Lee, "Public-key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proceedings of Pairing'07*, LNCS 4575, pp. 2-22, 2007.

[5] C. C. Lee, S. T. Hsu, and M. S. Hwang, "A study of conjunctive keyword searchable schemes," *International Journal of Network Security*, vol. 15, no. 5, pp. 321–330, 2013.

[6] Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 927–933, 2012.

[7] H. S. Rhee, J. H. Park, W. Susilo, D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," *Journal of Systems and Software*, vol. 83, no. 5, pp. 763-771, 2010.

[8] J. Shao, Z. F. Cao, X. H. Liang, H. Lin, "Proxy reencryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576-2587, 2010.

[9] J. Wang, X. Yu, and M. Zhao, "Fault-tolerant verifiable keyword symmetric searchable encryption in hybrid cloud ," *International Journal of Network Security*, vol. 17, no. 4, pp. 471–483, 2015.

[10] Y. Wang, W. Bao, Y. Zhao, H. Xiong, and Z. Qin, "An ElGamal encryption with fuzzy keyword search on cloud environment," *International Journal of Network Security*, vol. 18, no. 3, pp. 481–486, 2016.

[11] W. C. Yau, R. C. W. Phan, S. H. Heng, B. M. Goi, "Proxy re-encryption with keyword search: new definitions and algorithms," *Communications in Computer and Information Science*, vol. 122, pp. 149-160, 2010.

Fuh-Gwo Jeng received his M.S. in computer and information science from National Chiao Tung University and Ph.D. degree at the Institute of Computer Science, National Chung Hsing University, Taiwan. He is presently an associated professor of Department of Applied Mathematics, National Chiayi University. His research interests include information security and computer graphics.

Shu-Yuan Lin received her M.S. in Department of Computer Science and Information Engineering from

National Chiayi University in 2013. Her research interest is multimedia security.

Bing-Jian Wang received his M.S. in Department of Computer Science and Information Engineering from National Chiayi University in 2012. His research interest is visual crypotography and information security.

Chih-Hung Wang was born in Kaohsiung Taiwan, in 1968. He received his BS degree in information science from Tunghi University and MS degree in information engineering from National Chung-Cheng University, Taiwan, R.O.C., in 1991 and 1993, respectively. He received the PhD degree in information engineering from National Cheng Kung University, Taiwan, R.O.C. in 1998. He is presently an associated professor of Department of Computer and Information Engineering, Nation Chiayi University, Taiwan, R.O.C. His research interests include cryptography, and information security.

Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the B.S. degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the M.S. degree in Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his Ph.D. degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as Professor since August 2011. His research interests include information hiding, multimedia security, digital rights management, network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

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.