IJNS
International Journal of Network Security

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

Vol. 24, No. 3 (May 2022)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

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

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

PUBLISHER: Candy C. H. Lin

Volume: 24, No: 3 (May 1, 2022)

International Journal of Network Security

Attack Chains Construction Method Based on Vulnerabilities Combination

Jing Zhao[1], Hao Sun[1], and Yang Cheng[2]
(Corresponding author: Jing Zhao)
College of Software, Dalian University of Technology[1]
321 TuqiangStreet, Dalian 116620, China
Email: zhaoj9988@dlut.edu.cn
College of Computer Science and Technology, Harbin Engineering University[2]
145 NantongStreet, Harbin 150001, China
(Received May 23, 2021; Revised and Accepted Mar. 28, 2022; First Online Apr. 7, 2022)

Abstract

In computer networks, vulnerabilities exist in all aspects of system design and operation management, and vulnerabilities cannot be eliminated. Therefore, the attacker will use a series of vulnerabilities in the target system to achieve the purpose of the attack. Generally, a multi-stage vulnerabilities combination attack form has a higher success rate and destructiveness. To accurately reflect the security risks brought by the multi-stage vulnerabilities combination attack to the target system, this paper proposes a method of constructing attack chains based on the vulnerabilities combination. First, perform generalized clustering of the vulnerabilities and then use the idea of combined testing to combine the vulnerabilities and build attack chains. At the same time, this paper also proposes using answer set programming to remove redundant and meaningless combinations of vulnerabilities further. Finally, in the experimental environment designed in this paper, the attack experiment is carried out according to the attack chain. The experiment verifies the effectiveness of the attack chain construction method based on the vulnerabilities combination and improves the efficiency of network security analysis.

Keywords: Answer Set Programming (ASP); Attack Chain; Clustering; Vulnerability Combination

1 Introduction

With the continuous development of information technology, the penetration rate of the Internet is getting higher and higher, almost involving most countries and regions in the world. But while enjoying the convenience of the Internet, people often ignore the dangers behind it. With the continuous expansion of the network scale and the increasing complexity of the network structure, there are more and more security issues in the network. Due to the lack of security awareness and protection methods, cyber espionage activities, privacy, and security issues are becoming more frequent, complex, continuous, and difficult to intercept [23]. Among them, targeted network intrusions are also called Advanced Persistent Threats (APT). Attackers will comprehensively consider the vulnerabilities in the network system before APT attacks, and then use a combination of multi-stage vulnerabilities to slowly sneak into the network system to achieve their goals, usually stealing network resources or even network extortion [1, 12]. Attacks launched using combined vulnerabilities are often more subtle and difficult to detect, and are more likely to cause persistent and serious threats to the network. For example, the Russian threat organization APT28 used two 0day vulnerabilities to invade a multinational government agency. The two 0day vulnerabilities are CVE-2015-3043 of Adobe Flash and CVE-2015-1701 of Microsoft Windows. When a user visits a malicious website, Flash triggers the CVE-2015-3043 vulnerability, executes the shellcode to download the payload, and finally triggers CVE-2015-1701 to steal the system token. Egyptian security researcher Yasser discovered three high-risk vulnerabilities on the PayPal website, namely CSRF (cross-site request forgery) vulnerabilities, authentication token bypass vulnerabilities, and security authentication reset vulnerabilities. Yasser used the combination of these three vulnerabilities to reset the answers to the PayPal user's security verification questions, and finally took control of the victim's PayPal account.

Multi-stage vulnerabilities combined attacks can attack targets with high efficiency and high concealment while being strategic and intelligent to avoid detection. Even with the most advanced protection strategies, it is still difficult to avoid this new type of attack [2,20]. Therefore, the vulnerability must be analyzed from the overall network system. Proposing an effective security analysis strategy for the target network system is particularly critical to realize the predictability and visualization of net-

work attacks. At present, many scholars have proposed different analysis methods. For example, [16, 17, 21] proposed a method that can analyze the attack path of the attacker from the perspective of the bottom layer of the operating system. This method believes that the attacker will use some commands to achieve the goal when entering the network system, and the invocation process of these commands will be recorded in the log by the system's monitoring tool or command audit tool, to analyze the causality of the attack. However, this method needs to collect a large number of log records for a specific network, and it is not an easy task to extract effective attack information from a large amount of data. And because of the diversity of logs, it is difficult to analyze the dependency of attacks [14]. As early as 1998, Phillips *et al.* proposed the concept of constructing an attack graph to analyze the vulnerability of the overall network system [22]. Analyze the possible attack path from the attack graph. However, because the attack graph enumerates all possible attack paths in the network system, the complexity and computational cost of constructing the attack graph will increase as the system scales up.

To solve the difficulty of analyzing attack information from log records, we hope to analyze the attack path from the vulnerabilities in the system. In this way, it is possible to analyze the correlation in the attack process more intuitively. Given the high complexity and high cost of the attack graph, we found that during the construction of the attack graph, the exploitation of vulnerabilities in certain attack stages is similar. The similarities mentioned here will be explained in detail later. To reduce the risk of being discovered, the attacker usually chooses a simple and efficient attack path to achieve the goal. Similar vulnerabilities bring similar results to attackers, so attackers usually do not reuse similar vulnerabilities. The attack chain construction technology based on vulnerability clustering-combination can effectively solve the problem of attack graphs. It is worth mentioning that vulnerabilities are widespread in network systems and will always exist [24, 25]. Even if the maintenance personnel make timely patches and updates when they detect vulnerabilities in the system, they cannot guarantee that the vulnerabilities no longer exist and whether new vulnerabilities are introduced. Moreover, in some cases, it is very expensive to repair vulnerabilities, especially in the field of industrial control. It is difficult to repair vulnerabilities. Therefore, it is necessary to combine the vulnerabilities in the known network system, construct the attack chain, and analyze the security of the network system.

The main contributions of this paper are as follows:

1) According to the characteristics of vulnerabilities, this paper designs a formal description method.

2) According to the similarity of vulnerabilities, this paper designs a method of vulnerabilities clustering, which divides vulnerabilities into limited categories.

3) This paper designs two methods to combine vulnerabilities. First, based on the idea of t-way combination, we use the IPOG algorithm to perform a 2-way combination of vulnerabilities. Second, we consider using an answer set programming program to combine vulnerabilities to remove redundant and meaningless combinations of vulnerabilities.

4) Finally, we designed an experimental environment. Then use the attack chain to attack the target system. The experiment proves the effectiveness of our method.

The rest of this paper is organized as follows. In the second section, we reviewed more related work. In the third section, the description method of the vulnerability and the architecture of the attack chain are introduced. Then, in the fourth section, we will introduce the algorithm process of vulnerability clustering and combination in detail. In the fifth section, we conducted an experimental analysis. Finally, summarize the paper.

2 Related Works

Common network security defense methods are passive. For example, virus detection, intrusion detection, firewall, etc. are all passive defense methods. Most of these security defense methods can only be deployed and defended on one node, so the vulnerability of the system cannot be considered from the overall network system. The combined use of vulnerabilities can often bypass these defense methods. Therefore, with increasing vulnerabilities and diversification of attack methods, traditional security defenses cannot meet the needs of network security. Many outstanding scholars are studying the method of vulnerability combination. From the combination of vulnerabilities to analyze the vulnerability of the system, attack graphs are the main research method.

The construction of attack graphs is usually divided into two categories: the first is to represent the network status from the perspective of known vulnerabilities as a whole and enumerate state transitions through model checking [26]. The second is to combine and code individual vulnerabilities by identifying individual causality [9]. The first form suffers from the state explosion problem due to the increase in the number of vulnerabilities, so the second form is more and more popular because of its better scalability.

Attack graphs are also used for offline and online network security analysis. In offline situations, it can be used to determine the best location of firewalls and intrusion detection/defense systems without intervening in the current operation of the target network [6], calculate network security evaluation indicators [13], and perform network security risk analysis [3].

However, the attack graph is mainly constructed from the perspective of system attributes and status. Although it can reflect the combination and utilization of vulnerabilities in the network to a certain extent, it is still not

intuitive enough. To analyze the attacker's behavior pattern and combination of system vulnerabilities, this paper proposes a method to efficiently construct an attack chain based on the current vulnerabilities of the system. At present, academia and industry have two general models for the concept and classification of cyberattacks, namely "Cyber Kill Chain" and "ATT&CK" cyber-attack techniques and tactics. Cyber Kill Chain is an attack model proposed by Lockheed Martin, which is essentially targeted, staged attack. The attacker's attack process is usually planned, and each step has a clear goal. Lockheed Martin divides the attacker's planned steps into seven stages, namely reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective [27]. The Cyber Kill Chain model reflects that the attacker's penetration process is a combination of various attack methods and a combination of vulnerabilities. MITRE launched the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model in 2013 [18]. The ATT&CK model describes and categorizes the technologies and tactics used in the attack process based on network attack events that occur in the real world. ATT&CK not only classified and summarized the tactics and techniques that attackers may use, but also collected some information about penetration testing teams and hacker organizations, including the techniques and tactics they used, attack weapons, and other information. At present, the ATT&CK model is still being continuously updated, and with the continuous development of the actual attack methods, the techniques and tactics are continuously refined. Using the general classification of attacker behavior in ATT&CK can help security teams such as cyber incident response teams, security operations centers, red and blue teams, threat hunters, and IT departments to better test their detection and response mechanisms against cyber attacks. This paper will build attack chains with the help of the seven stages of the Cyber Kill Chain and the techniques and tactics in the ATT&CK model.

3 The Architecture of The Attack Chain

3.1 Formal Description of Vulnerability

Since CVE and CNNVD describe vulnerabilities in the form of text, this paper uses an automated framework proposed by Joshi *et al.* [7], which can extract entities, concepts, and relationships related to network security from text sources describing vulnerabilities. To enable vulnerabilities to be easily clustered and combined, and to express the prerequisites and consequences of exploiting vulnerabilities, we designed a description method for vulnerabilities and atomic attacks, and the form is as in Equation (1).

$$V_t = (e_t^{Pre}, \lambda, \delta, \sigma, e_t^{Post}) \tag{1}$$

V_t means vulnerability. The vulnerability V_t requires the implementation of λ tactics under e_t^{Pre} conditions, use δ tools to attack σ targets, and the follow-up result can be e_t^{Post}, as in Equation (2).

$$e_t^{Pre} \times \{\lambda, \delta, \sigma\} \rightarrow e_t^{Post} \tag{2}$$

Among them, each attribute value has the following characteristics:

$\lambda \in Tech$, $Tech$ is the collection of network attack techniques and tactics in the ATT&CK framework, which is used to launch attacks by exploiting the vulnerability.

$\delta \in Tool$, $Tool$ represents the set of penetration testing tools or network attack weapon library that an attacker may use.

$\sigma \in Target$, $Target$ represents a collection in the system that can be used as an attack target. It can be a host in the target network, or the operating system, software, or running service on the host.

$e_t^{Pre} = \{c_1, c_2, ..., c_n\}$, $e_t^{Post} = \{c_1, c_2, ..., c_n\}$, $c \in \Sigma$ and Σ represent the collection of target system assets and all available resources or permissions of the system, such as user rights, administrator permissions, system data, etc.

Such a description can describe not only vulnerabilities but also atomic attacks, such as detection and scanning mentioned above. These attacks are indispensable in the process of constructing the attack chain.

3.2 Attack Chain Construction Based on Vulnerability Combination

As shown in Figure 1, this paper is divided into three processes when constructing the attack chain, which are the construction of a vulnerability database, the clustering of vulnerabilities, and the combination of vulnerabilities to form the attack chain.

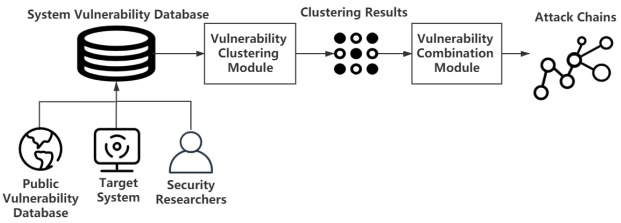


Figure 1: Attack chain construction process

Vulnerability database construction. For a given network system, security analysts use vulnerability scanning tool Nmap to perform host detection, port scanning and vulnerability detection on network systems. Security analysts will count the information of all nodes in the entire network system. The nodes here include PCs, servers, switches, and routers. Security analysts mainly count the operating system version, installed software version, which services are running, and what vulnerabilities exist on the node. Security analysts can easily find the corresponding vulnerability and atomic attack information

from the vulnerability database disclosed by CVE and CNNVD. Then use an automated framework proposed by Joshi *et al.* to extract entities, concepts, and relationships related to network security in the text source of the vulnerability. According to the formal description method of the above vulnerabilities, all vulnerabilities and atomic attacks are formalized and stored in the vulnerability database in the form of entries. At the same time, the $Tech$, $Tool$, $Target$, and Σ generalization hierarchies are constructed through the formal description of vulnerabilities and atomic attacks, and these generalization hierarchies will be used in subsequent cluster analysis.

Vulnerability clustering. This paper will cluster vulnerabilities based on the clustering algorithm of generalized hierarchical structure. For the target network system, if the scale is large, the vulnerability database of the target system will be very large and complex. Assuming that the size of the vulnerability is N, it is known that there are a variety of algorithms that can find the path from one point to the rest. Among them, the most classic way to find the single source shortest path is Dijkstra, and its time complexity is $O(N^2)$. To traverse all attack paths, the time complexity will reach $O(N^3)$. Although this time scale can be solved in polynomial time, the expansion of the scale has reached the cubic level. So when faced with large-scale vulnerabilities, it is very inefficient to use this method to solve all attack chains. Moreover, a large number of offensive and defensive practices have shown that there are certain similarities between many vulnerabilities. Attackers use similar vulnerabilities to achieve the same effect. To reduce the possibility of exposure in network systems, attackers usually do not reuse similar vulnerabilities. Here we may as well assume that there are M groups of vulnerabilities after clustering, and the vulnerabilities between the same groups are not reachable. Then when the single-source shortest path calculation is performed, the time complexity will become $O(M^2)$. Similarly, when traversing all attack paths, the time complexity is $O(M^3)$. Although the order of magnitude is still cubic, the size of M will not increase significantly as the size of the vulnerability increases. It can even be considered to a certain extent that the size of M is fixed, then $O(M^3)$ will be reduced to a constant level. Therefore, the clustering of vulnerabilities is very necessary, but the similarity of vulnerabilities is difficult to define. We will introduce in detail how to cluster vulnerabilities in the fourth section of the vulnerability clustering algorithm.

Vulnerability combination. For vulnerabilities after clustering, we consider using the idea of combined testing [5] to generate a sequence of vulnerability combinations as test cases for further analysis. The number of combinations of vulnerabilities happens to limit the length of the attack path, so we don't have to worry about those ultra-long attack paths. In each group of combinations, there may be vulnerabilities that are related to each other. In the t-way coverage combination test, 2-way coverage can achieve pairwise combinations of all parameters, and the overall number of test cases is much smaller than the combination of all parameters. At the same time, 2-way coverage can ensure that the generated combination contains an attack chain with a length of at least 2. Then we use answer set programming to further filter and merge to get a collection of attack chains. Therefore, the method of combining vulnerabilities and constructing an attack chain using the idea of combined testing can achieve the optimization of the attack chain construction process to a certain extent.

4 Vulnerability Clustering and Combination

4.1 Vulnerability Clustering Algorithm

Julisch *et al.* proposed an algorithm for clustering alarms [8]. The motivation for proposing this algorithm stems from the observation that the alarms of a given root cause are usually similar, but a large number of alarms affects the efficiency of the operation and maintenance personnel to maintain the system. Therefore, the alarms can be clustered, and the alarms with the same root cause can be summarized into a generalized structure that can cover the content of the alarm, and finally, an alarm summary with only a few generalized structures can be formed. We noticed that the vulnerability description method used in this paper is similar to the alarm structure input by the clustering algorithm. Julisch uses a row of attributes with multiple values to represent an alarm. Similar to the way we use five-tuples for vulnerability descriptions, we also use a row of attributes with multiple values. But the difference is that in our vulnerability description method, e_t^{Pre} and e_t^{Post} are not attributes of a single value. And when the attribute value has multiple parent nodes, the original algorithm cannot generalize the vulnerability attribute. Meanwhile, some vulnerabilities may be too unique to be clustered into a group with other vulnerabilities. If a uniform minimum coverage index is adopted, it may lead to over generalization and make clustering meaningless.

Given these three points, we have made the following improvements:

1) When generalizing e_t^{Pre} and e_t^{Post}, each attribute value of them is replaced by a parent node. If any node is generalized as the descendant node of other nodes, these attributes are deleted and only the attribute value with the best generality is retained. After generalizing different vulnerabilities, comparing whether a or B is equal requires comparing whether each value in the set is equal;

2) When a node has more than one parent node to select for generalization, one parent node is randomly selected for generalization;

3) Set the parameter minimum coverage ratio p, which means that all classes don't need to reach the minimum coverage to finish clustering. As long as the

Algorithm 1 Vulnerability Clustering Algorithm

Input: L: A list of vulnerabilities;
Input: G_0: Generalization hierarchy of Σ;
Input: G_1: Generalization hierarchy of $Tech$;
Input: G_2: Generalization hierarchy of $Tool$;
Input: G_3: Generalization hierarchy of $Target$;
Input: min_size: Minimum coverage;
Input: p: Minimum coverage ratio;
Output: A solustion for$(L, G_0, G_1, G_2, G_3, min_size, p)$;

$T := L$;
for all vulnerabilities v in T **do**
  $v[count] := 1$;
end for
while count$(v[count] > min_size)$/**sizeof**$(T) < p$ **do**
  Use heuristics to select an attribute A_i, $i \in \{0, 1, 2, 3\}$;
  for all vulnerabilities v **in** T **do**
    $v[A_i]$ **:= a random father of** $v[A_i]$ **in** G_i
    while identical v, v' **exist do**
      Set $v[count]$ **:=** $v[count] + v'[count]$ **and delete** v' **from** T;
    end while
  end for
end while
return all generalized vulnerabilities $v \in T$ **with** p **of** $v[count] > min\_size$;

number of vulnerabilities in some classes reaches the index, clustering can be stopped.

Our improved algorithm is shown in Algorithm 1.The heuristic functions used in the algorithm are as in Equations (3) and (4).

$$f_i(a) = \mathbf{sum}\{v\,[count]\,|A_i = a\} \quad (3)$$

$$F_i = \mathbf{max}\{f_i(a)|a \in \mathbf{Dom}(A_i)\} \quad (4)$$

Since the value of the same attribute A_i is different, the corresponding number of vulnerabilities is different. The function of f_i is to count the number of vulnerabilities whose attribute A_i corresponds to different values among all vulnerabilities. F_i is to count the largest number of vulnerabilities in different attribute values. The heuristic function guides which attribute should be selected for generalization in each iteration. Through this heuristic function, as many vulnerabilities as possible can be classified into the same category at each step. During the execution of the algorithm, we hope to save the classification results of vulnerabilities with a collection *coverlist*. The actual operation steps of the algorithm are as follows:

1) Because the generalization hierarchy G_i may not be a tree structure, a node may have multiple parent nodes, so the algorithm randomly selects a parent node for generalization.

2) Each vulnerability object will save a collection *coverlist*. When the *coverlist* is initialized, there is only a reference to the vulnerability itself. The meaning is that each vulnerability is in its category at the beginning, and other categories will be added during clustering.

3) Use heuristic function to select one of e_t^{Pre},λ, δ, σ, e_t^{Post} as A_i, and the A_i value of all vulnerabilities in T is replaced by the parent value of A_i in its generalized hierarchy G_i. If A_i is e_t^{Pre} or e_t^{Post} , each attribute value in the selected set is generalized, and each step determines whether the attribute in the set has an inclusion relationship. If so, the two attributes are merged.

4) Scan all vulnerabilities at this time. If the attributes of any vulnerability are identical, add the *coverlist* of the second vulnerability to the *coverlist* of the first vulnerability, and delete the second vulnerability from the vulnerability formal description table.

5) Continue the operation of Steps (3) (4). Because some vulnerabilities may vary greatly, they will not be covered unless they are generalized to the root node. Excessive generalization is meaningless, so when the percentage of vulnerabilities whose *coverlist* size is greater than min_size in all vulnerabilities reaches p, clustering stops.

6) Output the remaining vulnerabilities in Step (5). The *coverlist* of each vulnerability is all the vulnerabilities of this class.

4.2 Vulnerability Combination Algorithm

4.2.1 Vulnerability Combination Based on ACTS

This paper chooses to use ACTS [19] tool to generate vulnerability combinations. ACTS is a test case generation tool for constructing t-way coverage combination, which is widely used in system combination testing [4]. Due to its good performance, this paper chooses to use it to generate a 2-way coverage combination of vulnerabilities. ACTS supports the use of multiple algorithms to generate t-way coverage combinations, these algorithms include IPOG, IPOG-D, IPOG-F, and IPOG-F2, etc. [10, 11].

The strategy of the IPOG algorithm for constructing the t-way combination is expansion-based. In each iteration, horizontal expansion and vertical expansion are performed until the generated test cases can cover all t-way combinations. The strategy framework is described as follows: First, the categories are sorted non-increasingly according to the number of parameters in each category. Then select the first t classes to form all the combinations of the parameters in these classes, and expand the combination level to the t+1 parameter. If the horizontal expansion cannot guarantee to cover the t-way combination of the first t+1 parameters, then the vertical expansion is performed until it is satisfied. And so on, until all the t-way combinations of parameters can be covered.

Among them, horizontal expansion refers to the expansion of each existing combination by adding a value for the new parameter. Vertical growth refers to adding new combinations to the test set generated by horizontal expansion when necessary.

Algorithm 2 describes the test generation algorithm that implements this strategy, named IPOG-Test. The input of the algorithm is two parameters: an integer t that specifies the coverage strength, and a parameter set PS that contains the input parameters and their values. The output of the algorithm is the t-way test set of the parameters in PS. Assume that the number of parameters in the set PS is greater than or equal to t. Figure 2 shows the application of the IPOG-Test algorithm in an example 3-way test system. This example system consists of four parameters, P1, P2, P3, P4, where P1, P2, P3 have two values 0 and 1, and P4 has three values 0, 1, and 2. The algorithm first generates all the combinations between the three parameters P1, P2, and P3, that is, 2^3 combinations. Then, expand horizontally based on the original 8 combinations, and introduce the three parameters of P4 into the combination. However, after introducing the three parameters of P4, the combination of P4 and any three parameters before P1, P2, and P3 cannot be covered. Therefore, vertical expansion is required until the final combination can cover any combination of three parameters among these four parameters.

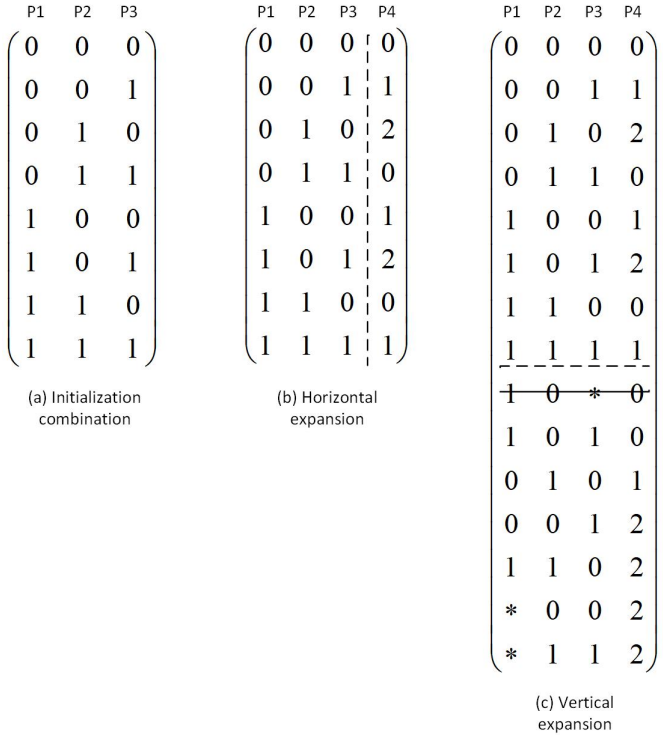


Figure 2: Schematic diagram of IPOG algorithm

Algorithm 2 IPOG Algorithm

Input: t: the strength of Combnation
Input: PS: the parameter set
Output: TS:Numerical test cases set

```
initialize test set TS to be an empty set
sort the parameters in set PS in a non-increasing order of their domain sizes, and denote them as P1, P2,...,Pk
add into TS a test for each combination of values of the first t parameters
for t+1 ≤ i ≤ k do
    let π be the set of all t-way combinations of values involving parameter P_i and any group of t−1 parameters among the first i−1 parameters
    // horizontal extension for parameter P_i
    for each test (o=v_1, v_2, ..., v_{i−1}) in TS do
        choose a value v_i of P_i and replace o with o'={v_1, v_2, ..., v_{i−1}, v_i} so that o' covers the most number of k-way of values in π
        remove from π the combinations of values covered by o'
    end for
    // vertical extension for parameter P_i
    for each combination σ in set π do
        if there exists o in TS such that it can be changed to cover σ then
            change test o to cover σ
        else
            add a new test to cover σ
        end if
    end for
end for
return TS
```

4.2.2 Vulnerability Combination Based on Answer Set Programming

Although the number of combinations generated by 2-way coverage is much smaller than the number of combinations of all vulnerabilities, it is still possible to generate many redundant and meaningless combinations of vulnerabilities. Since there are constraints between vulnerabilities and vulnerabilities, that is, some vulnerabilities are the prerequisites for other vulnerabilities, these constraints can be found first to assist in solving the vulnerability combinations, and this method can further reduce the number of generated combinations. Considering this feature, we can use answer set programming to solve the vulnerability combination.

Answer set programming [15] is a declarative programming method and language, mainly used to solve complex search problems, and can solve combined problems well. The main focus of programming with answer sets is the model of the problem, not the solution of the problem, which is very different from languages such as Java and python. When the problem is modeled using the syntax of answer set programming, the solution of the problem can

be obtained by running the answer set solver. For answer set programming, the University of Potsdam has developed an assembly Potassco (Potsdam Answer Set Solving Collection). Among them, clingo can be used to run ASP code. Therefore, for a problem that builds an attack chain based on a combination of vulnerabilities, we can use the answer set programming method to describe the vulnerability combination problem as an answer set programming logic program, and then use clingo to solve it. Finally, get the vulnerability combination. The main special symbols of answer set programming are shown in Table 1.

Table 1: ASP Special Symbol

Symbol	Function
%	Represents the start of code comments.
.	Represents the end of statement.
:-	Represents a constraint.
,	Represents "AND".
;	Represents "OR".
#show	Represents the output.

According to the vulnerability constraints, we can design programs to complete the modeling of automatic implementation problems. It mainly consists of four parts:

1) All possibilities of vulnerability combination. Assuming that four classes are obtained by clustering, four-parameter predicates need to be constructed. The values of parameters in each class are separated by ";".

2) Vulnerability constraints. The basic requirement of the attack chain is that the result of the previous exploit can be the precondition of the next atomic attack.

3) Constraints of problem modeling. These constraints are mainly used to eliminate the vulnerability combinations that do not contain the constraints between vulnerabilities in (1), and a group of combinations needs to contain more than one directed edge. When designing an answer set programming program, we can set the number of constraints at least contained in each group.

4) The final output is based on the result of the vulnerability combination attack chain construction.

5 Experiments and analysis

5.1 Experimental Environment Design

We designed an experimental environment, as shown in the Figure 3. The experimental environment is mainly composed of the attacker and target system. Attackers

Table 2: ASP special symbol

Machine	IP
Attacker	10.10.10.128
Web Server (OWASPBWA)	10.10.10.129
Back-end Server (Win2k3 Metasploitable)	10.10.10.130
Gateway	10.10.10.254 192.168.10.254
Intranet Client (WinXP Metasploitable)	192.168.10.128

are mainly computers with pre-installed penetration testing tools, such as Kali Linux or BackTrace. The target system is mainly composed of 4 machines, which are website server (OWASPBWA), back-end server (Win2k3 Metasploitable), gateway server (Linux Metasploitable), and intranet client (WinXP Metasploitable).

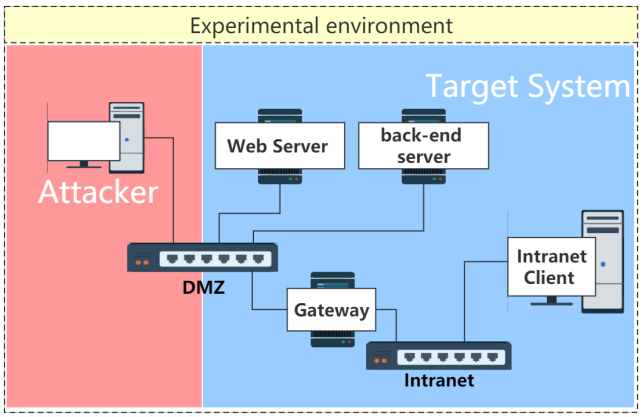


Figure 3: Experimental environment

OWASP BWA brings together a large number of training experimental environments and real web applications with known security vulnerabilities. There are various pre-set web applications with vulnerabilities, which are divided according to the security level, and the defect code programs at each security level are given. Win2k3 Metasploitable, Linux Metasploitable, WinXP Metasploitable, etc. are a series of virtual target machine images, these virtual machines contain a large number of unfixed security vulnerabilities.

Set two network segments through VMware's virtual network setting function, and distinguish the internal network and external network of the target system through the gateway. Intranet clients can access the internal network through the gateway, but the attacker cannot directly access intranet clients. The IP address of each machine is set as Table 2.

The virtual machine of the target system is specially selected by us. These virtual machines have some classic

vulnerabilities. According to our collation and continuous experiments, we mainly used 37 vulnerabilities in our experiment.

5.2 Experimental Data

The input required for the attack chain construction technology based on the vulnerability combination is the vulnerability list, the technical and tactical generalization hierarchy, the attack weapon generalization hierarchy, the target system asset generalization hierarchy, and the attack target generalization hierarchy. The construction of these inputs has been introduced in Section 3. To facilitate the operation of the program, the data is stored in XML format. Due to space limitations, this section mainly shows the vulnerability list and technical and tactical generalization hierarchy.

List of vulnerabilities/atomic attacks. The XML document of the attack list stores all the vulnerabilities/atomic attacks of the system. After scanning the target system with tools such as Nmap, W3AF, and Metasploit, there is no hierarchical division of atomic attacks generated by combining manual operations, and they are unified under the root node. The assets used by each atomic attack are stored in the "Conditions" node, the techniques and tactics used are stored in the "tech" node, the attack tools are stored in the "tool" node, the targets are stored in the "target" node, and the results generated are stored in the "results" node. For example, CVE-2009-1979 on the back-end server, its manifestation is shown in the Figure 4.

```
<bug id="11" type="Back-end_CVE-2009-1979">
  <Conditions>10.10.10.130:1521_oracle-tns</Conditions>
  <Conditions>10.10.10.130_Oracle_10.2.0.1.0</Conditions>
  <tech>Thread_Local_Storage</tech>
  <tool>msf_exploit_oracle_tns_auth_sesskey</tool>
  <target>10.10.10.130_Oracle_10.2.0.1.0</target>
  <Results>10.10.10.130_admin</Results>
</bug>
<bug id="12" type="Back-end_CVE-2011-0406">
...
</bug>
<bug id="13" type="Back-end_MS08-067">
...
</bug>
```

Figure 4: Vulnerability list

Technical and tactical generalization hierarchy. We designed a crawler script to crawl the data in https://attack.mitre.org/beta/ and build a generalized hierarchy of attack techniques and tactics based on the hierarchical structure of the ATT&CK matrix. Part of the manifestation of this hierarchical structure is shown in the Figure 5.

5.3 Vulnerability Clustering Experiment

This experiment uses the vulnerability clustering algorithm described in Section 4.1 to cluster vulnerabilities. According to different parameter settings, different clustering results can be obtained. The main parameters to

```
<Level_1>
  att&ck
  <Level_2>
    Initial_Access
    <Level_3>Drive-by_Compromise</Level_3>
    <Level_3>Exploit_Public-Facing_Application</Level_3>
    <Level_3>External_Remote_Services</Level_3>
    <Level_3>Hardware_Additions</Level_3>
    <Level_3>
      Phishing
      <Level_4>Spearphishing_Attachment</Level_4>
      <Level_4>Spearphishing_Link</Level_4>
      <Level_4>Spearphishing_via_Service</Level_4>
    </Level_3>
    <Level_3>Replication_Through_Removable_Media</Level_3>
    <Level_3>
    ...
```

Figure 5: ATT&CK generalization hierarchy

be set are *min_size* and p, which are the minimum coverage and the minimum coverage ratio. When *min_size* is set to 1, it means that there is only one vulnerability in each class. At this time, clustering is meaningless, so the value of *min_size* must be greater than 1. We tested multiple sets of use cases through dichotomy, and finally determined *min_size* and p. Take two of them as examples.

In the first group of clustering experiments, the parameters we adopted were $min\_size = 2$, $p = 1$. The experiment finally divided vulnerabilities into 2 classes. The vulnerabilities of each class are shown in Table 3, and the numbers represent different vulnerabilities. It can be seen that at this time, it has been over-generalized, and only divided into two groups is useless for vulnerability combinations.

Table 3: Clustering Result 1

Class	Vulnerabilities
1	1,8,2,9,4,5,3,6,24,7,21
2	10,11,35,17,18,34,12,14,16, 25,26,28,30,32,13,15,27,31, 29,33,19,20,36,37,22,23

In the second group of clustering experiments, the parameters we adopted were min_size=2, p=0.25. The experiment finally divided atomic attacks into 11 categories. The specific atomic attacks of each category are shown in Table 4. In this set of experiments, the number of categories 1, 4, 5, 6, and 10 exceeded *min_size*. However, there is only one vulnerability in the 2, 3, 7, 8, 9, and 11 categories. Among them, the fourth category contains 13 vulnerabilities. By analyzing the list of vulnerabilities, it can be known that the main target of these vulnerabilities is 10.10.10.130 and 10.10.10.254, which can achieve control of the target, but use different software vulnerabilities, different services have been attacked, different techniques and tactics have been used, and the use conditions and consequences are also different. The remaining vulnerabilities in categories 1, 5, 6, and 10 also achieved the goal of clustering "similar" vulnerabilities. This set of

Table 4: Clustering Result 2

Class	Vulnerabilities
1	1,8,2,9,4,5,3,6,24
2	7
3	10
4	11,35,17,18,34,12,14, 16,25,26,28,30,32
5	13,15,27,31
6	19,20,36
7	21
8	22
9	23
10	29,33
11	37

clustering results is relatively good, and the experiment in the vulnerability combination stage will adopt this set of clustering results.

5.4 Vulnerability Combination Experiment

We have designed two methods for vulnerability combination, which are mainly based on the combination test tool ACTS's vulnerability combination and the further screening of the vulnerability combination based on answer set programming.

This experiment uses the vulnerability combination method described in Section 4.2 and invokes the interfaces of the ACTS tool, and selects the vulnerabilities from each class of the clustering results for combination. Since 2-way coverage has been able to find pairwise combinations of vulnerabilities between different classes, it can find all effective attack paths with a length of at least 2. Therefore, 2-way coverage is used for vulnerability combination. Part of the result is shown in Figure 6.

```
# ACTS Test Suite Generation: Tue May 26 02:48:36 PDT 2020
#  * represents don't care value

# Degree of interaction coverage: 2
# Number of parameters: 11
# Maximum number of values per parameter: 13
# Number of configurations: 2808
# ************************************************
0,1,2,3,4,5,6,7,8,9,10
1,7,10,11,13,19,21,22,23,29,37
1,7,10,11,13,19,21,22,23,33,37
1,7,10,11,13,20,21,22,23,29,37
1,7,10,11,13,20,21,22,23,33,37
```

Figure 6: Combination result

Each row of the result represents a combination of vulnerabilities. A total of 2808 2-way combinations were generated. From these combinations, attack chains can be obtained, and each attack chain appears differently. However, the vulnerabilities combined in this way have overlapping parts and can be further merged. According to the vulnerability combination method based on answer set programming mentioned in Section 4.2.2, we designed the ASP program and used clingo to solve it. In this way, the relationship between the 2-way combinations of vulnerabilities is no longer considered, but only whether the number of constraints in a set of combinations meets the requirements. We set each group needs to contain at least 4 constraints. The results are shown in Table 5. In Table 5, F represents the frequency of each attack chain. Each number in the attack chain represents a vulnerability. It can be seen from Table 5 that some attack chains overlap, so attack chains can be further merged.

Table 5: Attack Chain Statistics 2

Index	F	Attack Chain	Index	F	Attack Chain
1	1102	7→21	30	312	6→7→21
2	1102	7→22	31	312	6→7→22
3	1102	7→23	32	312	6→7→23
4	312	6→7	33	156	29→6→7→22
5	216	10→17	34	156	29→6→7→23
6	216	35→37	35	156	29→6→7→21
7	156	29→6	36	78	31→6→7→22
8	108	33→17	37	78	27→6→7→22
9	78	5→27	38	78	31→6→7→21
10	78	31→6	39	78	27→6→7→23
11	78	27→6	40	78	31→6→7→23
12	78	4→13	41	78	27→6→7→21
13	78	4→15	42	72	10→17→19
14	72	17→19	43	72	10→17→20
15	72	17→20	44	36	33→17→19
16	72	18→19	45	36	33→17→20
17	72	35→36	46	24	24→35→37
18	72	18→20	47	24	32→6→7→23
19	24	30→6	48	24	28→6→7→21
20	24	4→12	49	24	30→6→7→23
21	24	24→35	50	24	32→6→7→22
22	24	32→6	51	24	30→6→7→22
23	24	8→18	52	24	28→6→7→22
24	24	8→25	53	24	32→6→7→21
25	24	8→26	54	24	30→6→7→21
26	24	4→11	55	24	28→6→7→23
27	24	4→14	56	8	8→18→20
28	24	28→6	57	8	24→35→36
29	8	8→18→19			

It can be seen that the vulnerability combination method based on answer set programming is the same as the attack chain generated by the ACTS-based vulnerability combination method, but the total number generated by the vulnerability combination method based on answer set programming is small, which reduces the sample space while achieving the same effect.

To further analyze the attack chains that exist on the experimental target system, the generated attack chains need to be merged. The final result is shown in Figure 7. Attack chain merge result graph, each node represents a vulnerability. We will use the attack chain to test in the experimental environment.

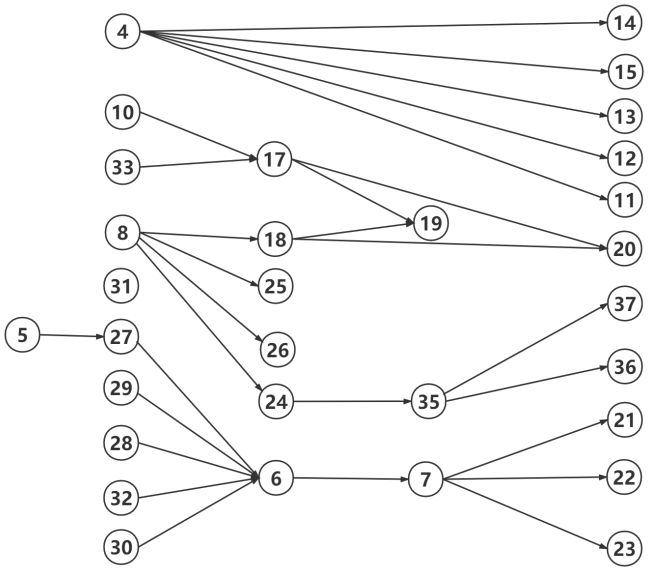


Figure 7: Attack chains

5.5 Attack Chain Implementation Experiment

In response to the 37 vulnerabilities of this experimental platform, we have compiled a manual for their utilization methods. The attack can be easily realized with the help of the manual. This section does not enumerate all the processes of the attack chain. We choose the longest attack chain {5,27,6,7,21} for illustration, and the most difficult attack chain is used to illustrate the effectiveness of the attack process. The attack process is as follows:

1 Vulnerability No.5: Obtain the services running on each port of the gateway server. Use Nmap to use the "-sT -PN -spoof-mac 0" option to detect 10.10.10.254, then we can get the result of the port service of the gateway.

2 Vulnerability No.27: Exploit CVE-2007-2447 and obtain the root of the gateway server. According to the results of the previous step, it can be seen that the gateway has opened port 139 to the outside world. Usually, samba runs on this port. Some versions of the samba service have the CVE-2007-2447 vulnerability. Use Metasploit's payload to attack the gateway. The gateway does have a vulnerability, so the control of the gateway is obtained.

3 Vulnerability No.6: Obtain the IP of the host that has communicated with the gateway. Since the attacker cannot directly scan the intranet, we can find the IP of the intranet client through the "arp" command of the gateway.

4 Vulnerability No.7: Scan the port of 192.168.10.128. After obtaining the IP of the intranet client, we can use Nmap to scan the client.

5 Vulnerability No.21: Exploit MS08-067(CVE-2008-4250) and get control of the intranet client. After scanning the client in the previous step, it is known that the internal network client machine opens port 445. This port is an SMB channel. The SMB channel may have the MS08-067 vulnerability. Then we can use Metasploit's payload to attack the intranet client. It is found that the attack is successful and the client control is obtained. The attack result is shown in the Figure 8.

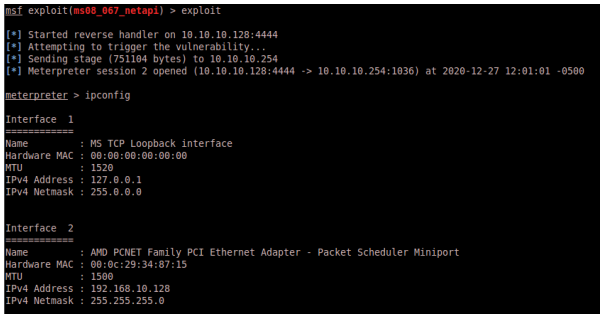


Figure 8: Result: Penetration into the intranet

Through the experimental process, the attack chain realized the penetration of the target system from the outside to the inside, and finally gained control of the intranet client. This attack chain realizes step-by-step penetration from the external network into the internal network and gains the control authority of the internal network machine, which has a strong threat. We carry out experiments according to the attack chain screened in Figure **??**, and all of them can achieve the purpose of the attack. To verify the effectiveness of our attack chain method for the target network construction, we analyze the different vulnerable attack paths in the target network as a whole, which provides a basis for the subsequent network defense process.

6 Conclusion

To achieve high efficiency and visualization of target network security analysis, this paper proposes an attack chain construction method based on the combination of vulnerabilities based on the research status of vulnerabilities and attack models. This paper uses the 5-tuple field to formally describe the vulnerabilities, using this method to build a vulnerability library for the target network. At the same time, we build a generalization hierarchy for each attribute on the 5-tuple, which makes the vulnerabilities can be clustered. Then we combined the generalized hierarchy of each attribute in the vulnerability, and we proposed a clustering algorithm to group "similar" vulnerabilities into one category, so the vulnerabilities are grouped into a limited number of categories.

We use the combination test tool ACTS for 2-way vulnerabilities combination, which guarantees a way to find

all the two-way combinations of vulnerabilities. Further use answer set programming to solve vulnerabilities combinations to remove redundant and meaningless combinations. Finally, an experimental simulation environment was built, and the attack chain constructed by the vulnerability combination was used to conduct attack experiments. The experiment shows the effectiveness of the attack chain construction method and provides a basis for the subsequent network system defense. Due to the limitation of the experimental environment, the target network designed in this paper is not complex enough. In the future, we will build a larger network attack and defense environment, and introduce industrial control systems, rail transit systems, and other simulation scenarios that are closely related to the construction of network security and national defense. In the complex network environment, the validity and practicability of the attack chain construction technology based on the combination of vulnerabilities are further verified.

References

[1] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[2] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, I. Ghafir, S. Lambotharan, and J. A. Chambers, "Multi-stage attack detection using contextual information," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 1–9.

[3] K. Beckers, M. Heisel, L. Krautsevich, F. Martinelli, R. Meis, and A. Yautsiukhin, "Determining the probability of smart grid attacks by combining attack tree and attack graph analysis," in *International Workshop on Smart Grid Security*. Springer, 2014, pp. 30–47.

[4] M. N. Borazjany, L. Yu, Y. Lei, R. Kacker, and R. Kuhn, "Combinatorial testing of acts: A case study," in *2012 IEEE Fifth International Conference on Software Testing, Verification and Validation*. IEEE, 2012, pp. 591–600.

[5] M. Grindal, J. Offutt, and S. F. Andler, "Combination testing strategies: a survey," *Software Testing, Verification and Reliability*, vol. 15, no. 3, pp. 167–199, 2005.

[6] S. Jajodia and S. Noel, "Topological vulnerability analysis," in *Cyber situational awareness*. Springer, 2010, pp. 139–154.

[7] A. Joshi, R. Lal, T. Finin, and A. Joshi, "Extracting cybersecurity related linked data from text," in *2013 IEEE Seventh International Conference on Semantic Computing*. IEEE, 2013, pp. 252–259.

[8] K. Julisch, "Clustering intrusion detection alarms to support root cause analysis," *ACM transactions on information and system security (TISSEC)*, vol. 6, no. 4, pp. 443–471, 2003.

[9] M. Khouzani, Z. Liu, and P. Malacaria, "Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs," *European Journal of Operational Research*, vol. 278, no. 3, pp. 894–903, 2019.

[10] Y. Lei, R. Kacker, D. R. Kuhn, V. Okun, and J. Lawrence, "IPOG: A general strategy for t-way software testing," in *14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07)*. IEEE, 2007, pp. 549–556.

[11] Y. Lei, R. Kacker, D. R. Kuhn, V. Okun, J. Lawrence, "IPOG-IPOG-D: Efficient test generation for multi-way combinatorial testing," *Software Testing, Verification and Reliability*, vol. 18, no. 3, pp. 125–148, 2008.

[12] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26–59, 2018.

[13] E. Lemay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W. H. Sanders, "Adversary-driven state-based system security evaluation," in *Proceedings of the 6th International Workshop on Security Measurements and Metrics*, 2010, pp. 1–9.

[14] T. Li, J. Ma, Q. Pei, Y. Shen, C. Lin, S. Ma, and M. S. Obaidat, "Aclog: attack chain construction based on log correlation," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[15] V. Lifschitz, *Answer set programming*. Springer Berlin, 2019.

[16] Y. Liu, M. Zhang, D. Li, K. Jee, Z. Li, Z. Wu, J. Rhee, and P. Mittal, "Towards a timely causality analysis for enterprise security." in *NDSS*, 2018.

[17] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, and V. Venkatakrishnan, "Holmes: real-time apt detection through correlation of suspicious information flows," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1137–1152.

[18] MITRE ATT&CK, *ATT&CK*, Feb. 19, 2022. (https://attack.mitre.org/)

[19] NIST, *Website for the NIST Automated Combintorial Testing (ACTs) Project*, Feb. 19, 2022. (https://www.nist.gov/programs-projects/automated-combinatorial-testing-software-acts)

[20] J. P. P. M. Orvalho and R. M. S. Silva, "Flexible approach to multi-stage network attack recognition," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 8, 2019.

[21] T. Pasquier, X. Han, T. Moyer, A. Bates, O. Hermant, D. Eyers, J. Bacon, and M. Seltzer, "Runtime analysis of whole-system provenance," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1601–1616.

[22] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 workshop on New security paradigms*, 1998, pp. 71–79.

[23] S. Smarter and S. Malware, "Security threat report 2014."

[24] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," in *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*. IEEE, 2016, pp. 1–5.

[25] V. Subrahmanian, M. Ovelgonne, T. Dumitras, and B. A. Prakash, "The global cyber-vulnerability report," 2015.

[26] L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-attack graph generation tool," in *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01*, vol. 2. IEEE, 2001, pp. 307–321.

[27] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 438–452.

Biography

Jing Zhao received the Ph.D. degree in computer science and technology from the Harbin Institute of Technology of China in 2006. In 2010, she was with the Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina, working as a postdoctoral researcher under the supervision of Dr. Kishor Trivedi. From 2006 to 2018, she was a professor at the School of Computer Science and Technology, Harbin Engineering University, China. She is currently a professor at the School of Software Technology, Dalian University of Technology, China. Her research interests include cyber security and Internet of vehicles security.

Hao Sun is currently a master of Software Engineering, Dalian University of Technology. He received a bachelor's degree from Harbin Engineering University in 2019. His research interests include network security and Internet of Things security.

Yang Cheng received a master's degree in computer science and technology from Harbin Engineering University in 2021. He received a bachelor's degree from Harbin Engineering University in 2018. His research direction is mainly network security.

A Feature Selection Method of CERT for Abnormal Network Traffic Detection

Yongxin Feng[1], Wenxin Li[1], Yuntao Zhao[1], Shengnan Geng[2], Bo Yu[3], and Junxing Jia[1]
(Corresponding author: Yuntao Zhao)

School of Information Science and Engineering, Shenyang Ligong University[1]
Shenyang 110159, China
Email: fengyongxin@263.net; 1072785916@qq.com
Beijing Institute of Astronautical System Engineering[2]
Beijing 100076, China
Email: shengnan01@126.com
China Telecom Corporation Huludao Branch[3]
Huludao 100000, China
Email: zhaoyuntao2014@163.com
(Received Mar. 25, 2021; Revised and Accepted Mar. 17, 2022; First Online Apr. 16, 2022)

Abstract

To avoid the curse of dimensionality, many feature reduction or feature selection methods, which can reduce the time complexity and reconstruct the appropriate feature space, have been studied in the field of security. This paper proposes a method of the chi-square highly randomized trees (CERT) feature selection against abnormal behaviors. The method builds the relationship between features and labels through relevance and feature importance, innovatively combining the extremely randomized trees and chi-square test algorithms. With the KDD CUP99, NSL-KDD, NUSW-NB15 datasets, we compare our method's accuracy and recall with those of LightGBM, AdaBoost, and XGBoost ensemble learning algorithms. The experimental results show that the feature Selection Method of CERT proposed in the paper can effectively realize feature reduction, whose detection accuracy is above 94%, and the recall rate is 95%.

Keywords: Abnormal Network Traffic Detection; Ensemble Learning; Feature Selection

1 Introduction

Network abnormal traffic detection technology is an important method to detect attack behavior in the field of network security [31]. There are many characteristics and attributes of network traffic data, but the detection technology of abnormal network traffic usually depends on some of all characteristics.Therefore, an appropriate feature selection method can eliminate the features that have negative effects on classification and retain the features that have positive effects on classification, which will greatly improve the efficiency of traffic detection [20]. Besides, the single classification methods in machine learning are prone to instability and over-fitting in the detection of network traffic attack behavior. Applying the feature selection method to the data and combining the advantages and characteristics of ensemble learning algorithm can effectively enhance the detection stability and solve the over-fitting phenomenon, while reducing the complexity of time and space, and further improve the detection performance.

The main contributions of the paper are as follows: Combining the chi-square test method which judges correlation between features and labels by calculating chi-square value and the extremely randomized trees algorithm which measures feature importance,this paper presents an innovative feature selection method based on CERT, which can measure both relevance and feature importance.

In Section 2, we review the previous work in feature selection. In Section 3, we introduce the mathematical principle of chi-square test and extremely randomized trees, besides, the running process of feature selection method based on CERT is introduced. In Section 4, KDD CUP99, NSL-KDD and NUSW-NB15 data sets were tested by unused feature selection, chi-square feature selection and CERT feature selection methods.

2 Related Research

Feature selection is an important research area in traffic detection technology, and researchers have proposed many feature selection methods [25]. Literature [19] proposed a heuristic feature selection method based on

ReliefF-MFO. This method uses the ReliefF algorithm to select relevant features and uses the MFO heuristic algorithm to optimize the feature subset. Literature [18] proposed an intrusion detection method based on a mixture of the artificial bee colony and AdaBoost algorithm. This method uses artificial bee colony algorithm for feature selection and uses AdaBoost to evaluate and classify features, but the artificial bee colony algorithm is prone to fall into a locally optimal solution.

Literature [22] proposed a feature selection method with a mixture of rough set theory and Bayes 'theorem. This method uses rough set theory to distinguish the features in the dataset and solves it through Bayes' theorem to obtain the best feature subset. However, this method has the disadvantage of too long calculation time when facing large-scale datasets. Literature [2] proposed an intrusion detection model based on the intelligent water drop (IWD) feature selection algorithm. This model uses the natural heuristic IWD optimization algorithm to select the features of the dataset and SVM as a classifier to evaluate the selected features. However, the classification effect for multi-class datasets is not very obvious.

Literature [4] proposed a hybrid feature selection method based on a binary gravity search algorithm (BGSA) and mutual information (MI). This method uses MI to calculate the feature-feature and feature-class mutual information and uses the detection rate and false-positive rate as the fitness function for the global search of the BGSA algorithm, so as to select the feature with the least redundancy and the strongest class correlation. However, this method has a high computational complexity. For the above feature selection methods, although different algorithms are used to evaluate features, they all follow the same principle, which is to reduce the data dimension while improving the accuracy and detection efficiency of the final classification model [14, 21].

3 Feature Selection Method Based on CERT

In order to more effectively identify malicious attacks in the network, based on the research of existing feature selection methods, this paper proposes a feature selection method based on the CERT. The feature selection method is to select features in-depth from two aspects of correlation and feature importance, so as to select the most valuable features for classification.

3.1 Chi-Square Test

Chi-square test is a widely used hypothesis testing method with good performance. The relationship between the attributes is measured by the degree of deviation between the actual frequency and the theoretical frequency of the statistical data samples [12]. Therefore, the correlation between features can be judged by calculating the degree of deviation between features and labels. In the chi-square test, the chi-square value larger between features and labels, the correlation greater between features and labels, and the feature is more favorable for classification. On the contrary, the correlation smaller between features and labels, and the effect smaller on classification [5].

The basic formula of the chi-square test is shown in formula 1.

$$\chi^2 = \sum \frac{(A-T)^2}{T} \tag{1}$$

Where A is the actual frequency of the data sample, T is the theoretical frequency of the data sample [16].

The theoretical frequency [7] of the data sample x in the first feature column and the labels is shown in formula 2.

$$T_{L(m),F_1(x)} = \frac{A_{L(m)}, F_1(x)}{N} \times N_{L(m)} \tag{2}$$

Where N is the total number of data samples, is the actual frequency of the label and the data sample x in the first feature column, and is the total number of data samples for labels.

3.2 Extremely Randomized Trees

Extremely randomized trees algorithm is similar to random forest algorithm, and it is also composed of decision trees [27]. Compared with the randomness in the random forest algorithm, the randomness in the extremely randomized trees refers to feature randomness and split randomness. Extremely randomized trees algorithm is more random than random forest algorithm [9, 32].

This paper uses the CART decision tree as the basic tree model of the extremely randomized trees algorithm. The CART decision tree uses the Gini coefficient as the evaluation criterion. Suppose there are n categories, represents the probability of n category, and the Gini coefficient on the probability distribution is shown in formula 3.

$$\text{Gini}(p) = \sum_{n=1}^{N} p_n (1-p_n) = 1 - \sum_{n=1}^{N} p_n^2 \tag{3}$$

Suppose there are dataset, the feature F can divide the dataset D into two parts D_1 and D_2 [3]. Under the condition of the feature F, the dataset Gini coefficient is shown in formula 4.

$$\text{Gini}(D,F) = \frac{|D_1|}{|D|}\text{Gini}(D_1) + \frac{|D_2|}{|D|}\text{Gini}(D_2) \tag{4}$$

The relationship is measured using feature importance between features and labels in extremely randomized trees algorithm [13]. The normalized value of the Gini coefficient reduction is used to represent the feature importance. The calculation formula of feature importance [11] is shown in formula 5.

$$\begin{aligned} I(F) = &\frac{N_t}{N} \times \left(\text{Gini}(D,F) - \frac{N_{tR}}{N_t} \times R\_ \text{ Gini}(D,F \right. \\ &\left. - \frac{N_{tL}}{N_t} \times L\_ \text{ Gini}(D,F) \right) \end{aligned} \tag{5}$$

Where N is the total number of samples, N_t is the number of current node samples, N_{tR} is the number of samples on the right subtree, N_{tL} is the number of samples on the left subtree, $R_Gini(D,F)$ is the Gini coefficient of right subtree, $L_Gini(D,F)$ is the Gini coefficient of left the subtree.

the number of samples on the right subtree, N_{tL} is the number of samples on the left subtree, $R\_$ Gini (D,F) is the Gini coefficient of right subtree, $L\_$ Gini (D,F) is the Gini coefficient of left the subtree [8,26].

3.3 CERT Feature Selection Method's Operation Process

In the above chapters, the theoretical knowledge and implementation details of the feature selection method based on the CERT are comprehensively introduced. The pseudo-code of this method is given in Algorithm 1.

Algorithm 1 Feature selection method based on CERT

Input: dataset D, chi-square threshold χ^2- th, extremely randomized trees threshold ERT_th

Output: dataset $D_{\chi^2-\mathrm{ERT}}$

N=Statistics Line_(D), K=Statistics Column_(D), $N_{L(m)} = Statistics\_L(m)\_(D)$, $A_{L(m),F_1(x)} = Statistics\_L(m)\_F_1(x)\_(D)$;
$T_{L(m),F_1(x)} \leftarrow \left(N, N_{L(m)}, A_{L(m),F_1(x)}\right)$;
$\chi^2\left(L(m),F_1(x)\right) \leftarrow \left(A_{L(m),F_1(x)}, T_{L(m),F_1(x)}\right)$;
for $(k=1; k<=K; k++)$
  for m to M do
    for x to X do
      $\chi^2\left(L(m),F_1\right) \leftarrow \sum_x^X \left(A_{L(m)F_1(x)'}, T_{L(m),F_{(x)}}\right)$;
    end for
    return $\chi^2\left(L,F_1\right)$;
    $\chi^2\left(L,F_1\right) \leftarrow \sum_m^M \left(A_{L(m),F_1}, T_{L(m),F_1}\right)$;
  end for
  return $\chi^2\left(L,F_1\right)$;
  $\chi^2\left(L,F_k\right) \leftarrow \left(A_{L(m),F_k}, T_{L(m),F_k}\right)$;
  if $\chi^2\left(L,F_k\right) > \chi^2 - th$
  return F_k;
end for
$D_{\chi^2} = [F_k]$
Gini $\left(D_{\chi^2}, F_k\right) \leftarrow \left(D_{\chi^2-1'} D_{\chi^2-2}\right)$
$I(F_k) \leftarrow (\frac{N_t}{N}, \frac{N_{tR}}{N_t}, \frac{N_{tL}}{N_t}, R\_\,\mathrm{Gini}(D_{\chi^2}, F_k), L\_\,\mathrm{Gini}(D_{x^2}, F_k), \mathrm{Gini}(D_{x^2}, F_k))$
$I\left(F_k\right) \leftarrow \mathrm{vote}\left(F_k, F_k, \cdots, F_k\right)$ IF $I\left(F_k\right) >$ ERT_th
return F_k;
$D_{\chi^2-\mathrm{ERT}} = [F_k]$
end

Firstly, statistics the total number of data samples N, the number of feature columns K, the total number of data samples $N_{L(m)}$ for labels $L(m)$, the actual frequency $A_{L(m),F_1(x)}$ of label $L(m)$ and feature sample x in the first column. Secondly, calculate the chi-square values between each column of features and labels. The features are sorted in descending order according to the chi-square value, and select features to compose dataset D_{x^2} whose chi-square value is greater than the chi-square threshold. And then, calculate the feature importance of dataset D_{χ^2}. The features are sorted in descending order according to the feature importance, and the features less than the feature importance threshold are eliminated. Finally, the features selected by the CERT method constitute the dataset D_{χ^2}. The features are sorted in descending order according to the feature importance, and the features less than the feature importance threshold are eliminated. Finally, the features selected by the CERT method constitute the dataset $D_{\chi^2-\mathrm{ERT}}$.

4 Experimental Simulation and Analysis

4.1 Experimental Data

To verify the feasibility and superiority of the CERT feature selection method in abnormal network traffic detection [23, 28], this paper uses the authoritative KDD CUP99 [30], NSL-KDD, NUSW-NB15 datasets for abnormal network traffic detection to verification [24]. The KDD CUP99 dataset is a network data collected by the Lincoln Laboratory simulating the US Air Force LAN, covering common network attack behaviors. The NSL-KDD [10] dataset removes the redundancy of the KDD CUP99 dataset and adjusts the ratio of normal data and abnormal data to make the test data and training data more reasonable. The NUSW-NB15 [15, 17] dataset is a hybrid dataset based on real normal behavior and modern attacks generated by the Australian Cyber Security Centre in 2015 using the LXIA Perfect Storm tool, which can better reflect the true status of current network traffic.

Table 1 is the sample distribution of the training set and test set of the KDD CUP99, NSL-KDD, and NUSW-NB15 datasets.

Table 1: Dataset distribution

Dataset	Quantity (items)	
	Training set	Testing set
KDD CUP99	404921	311029
NSL-KDD	125973	22544
NUSW-NB15	175341	82332

4.2 Experimental Results and Analysis

In this paper, experiments are performed on KDD CUP99, NSL-KDD, NUSW-NB15 datasets using unselected feature selection, chi-square feature selection, and CERT feature selection methods. The LightGBM, AdaBoost, and XGBoost [1,29] ensemble learning algorithms are used to classify and detect three different feature sets, and the performance of the feature selection algorithm is

compared and analyzed through two indicators, accuracy and recall.

1) KDD CUP99 dataset. The KDD CUP99 dataset has 41 -dimensional feature attributes, represented by fk(k = $1, 2, 3, \ldots, 41$), including f1 = duration, f2 = protocol type, f3 = service , . . . , f41 = dst host srv rerror rate, *etc.* [6]. The chi-square test method was used to calculate the chi-square value for the KDD CUP99 dataset, and the chi-square threshold was set to 12000. The features of f5, f6, ...f4 with a total of 30 dimensions larger than the chi-square threshold are selected. These 30 -dimensional features are the chi-square feature selection dataset, as shown in Table 2

   Use the extremely randomized trees algorithm to calculate the importance of the remaining 30-dimensional features, and set the threshold of feature importance to 0.0025. Remove features with a total of 7 dimensions smaller than the feature importance threshold in $f16$, $f17$, $f14$, $f11$, $f1$, $f22$, and $f6$. The remaining 23-dimensional features are the CERT feature selection dataset, as shown in Table 3.

   From Table 3 feature importance, we can know that $f12$ = logged_in, $f23$ = count, $f24$ = srv_count, $f2$ = protocol_type, $f32$ = dst_host_count, $f36$ = dst_host_same_src_port_rate, $f33$ = dst_host_srv_count, $f26$ = srv_serror_rate, $f4$ = flag, $f39$ = dst_host_srv_serror_rate, $f38$ = dst_host_serror_rate, $f25$ = serror_rate, $f3$ = service, $f35$ = dst_host_diff_srv_rate, $f40$ = dst_host_rerror_rate, $f31$ = srv_diff_host_rate, $f30$ = diff_srv_rate, $f41$ = dst_host_srv_rerror_rate, $f27$ = rerror_rate, $f28$ = srv_rerror_rate, $f37$ = dst_host_srv_diff_host_rate, $f5$ = src_bytes, $f10$ = hot, a total of 23 dimensions are the features obtained after the CERT feature selection. Table 4 is the detection results of the KDD CUP99 dataset without using feature selection, using the chi-square feature selection method and using the CERT feature selection method.

2) NSL-KDD dataset. The NSL-KDD dataset also contains 41-dimensional feature attributes, which are represented by vk ($k = 1, 2, \cdots, 41$), including $v1$=duration, $v2$=protocol_type, $v3$=service, $\cdots$, $v41$=dst_host_srv_rerror_rate, *etc.* The chi-square test method was used to calculate the chi-square value for the NS-KDD dataset, and the chi-square threshold was set to 4000. The features of $v5, v6, \cdots, v8$ with a total of 32 dimensions larger than the chi-square threshold are selected. These 32-dimensional features are the chi-square feature selection dataset, as shown in Table 5.

   Use the extremely randomized trees algorithm to calculate the importance of the remaining 32-dimensional features, and set the threshold of feature importance to 0.015. Remove features with a total of 12 dimensions less than the feature importance threshold in v16, v14, v22, v13, v1, v10, v6, v5, v8, v3, v31, v24. The remaining 20-dimensional features are the CERT feature selection dataset, as shown in Table 6

   From Table 6 feature importance, we can know that $v29$ = same_srv_rate, $v26$ = srv_serror_rate, $v39$ = dst_host_srv_serror_rate, $v38$ = dst_host_serror_rate, $v25$ = serror_rate, $v12$ = logged_in, $v4$ = flag, $v34$ = dst_host_same_srv_rate, $v33$ = dst_host_srv_count, $v36$ = dst_host_same_src_port_rate, $v2$ = protocol_type, $v23$ = count, $v35$ = dst_host_diff_srv_rate, $v30$ = diff_srv_rate, $v40$ = dst_host_rerror_rate, $v41$ = dst_host_srv_rerror_rate, $v28$ = srv_rerror_rate, $v27$ = rerror_rate, $v32$ = dst_host_count, $v37$ = dst_host_srv_diff_host_rate, a total of 20 dimensions are the features obtained after the CERT feature selection. Table 7 is the detection results of the NSL-KDD dataset without using feature selection, using the chi-square feature selection method and using the CERT feature selection method.

3) NUSW-NB15 dataset. The NUSW-NB15 dataset contains 42-dimensional feature attributes, which are represented by zk ($k = 1, 2, \cdots, 42$), including z1 = duration, z2 = protocol, z3 = service,..., z42 = is_sm_ips_ports, etc. The chi-square test method was used to calculate the chi-square value for the NUSW-NB15 dataset, and the chi-square threshold was set to 5000. The features of z22, z21, z32 with a total of 32 dimensions larger than the chi-square threshold are selected. These 31-dimensional features are the chi-square feature selection dataset, as shown in Table 8.

Use the extremely randomized trees algorithm to calculate the importance of the remaining 3 1-dimensional features, and set the threshold of feature importance to 0.01. Remove features with a total of 13 dimensions less than the feature importance threshold in $z30, z19, z8, z15, z17, z18$ z5, z6, z7, z12, z33, z16, z40. The remaining 18 -dimensional features are the CERT feature selection dataset, as shown in Table 9.

From Table 9 feature importance, we can know that $z10$ = stt1, z32 = ct state tt1, z11 = dttl, z20 = swin z23 = dwin, z35 = ct dst sport ltm, z3 = service , z9 =rate , z13 = dload , z41 = ct srv dst, z36 = ct dst sre ltm z21 = stcpb, z34 = ct src dport 1tm, z22 = dtcpb, z2 = a total of 18 dimensions are the features obtained after the CERT feature selection. Table 10 is the detection results of the NUSW-NB15 dataset without using feature selection using the chi-square feature selection method and using the CERT feature selection method.

Figure 1 shows the detection accuracy of the LightGBM, AdaBoost, and XGBoost ensemble learning algorithms under the KDD CUP99, NSL-KDD, and NUSW-NB15 datasets.

Table 2: Chi-square values of the KDD CUP99 dataset

Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square Value
f5	6.5*1010	f6	7.6*109	f1	9.9*107	f23	4*107
f24	3.5*107	f32	3.9*106	f10	1.7*106	f33	6.3*105
f12	2.7*105	f14	1.2*105	f3	1.1*105	f2	9.9*104
f22	6.3*104	f31	5.2*104	f35	4.5*104	f36	4.4*104
f17	3.2*104	f30	2.9*104	f37	2.8*104	f16	2.5*104
f39	2.1*104	f25	2.1*104	f26	2.1*104	f38	2.1*104
f27	1.8*104	f41	1.8*104	f28	1.8*104	f11	1.8*104
f40	1.7*104	f4	1.2*104				

Table 3: Feature importance of the KDD CUP99 dataset

Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Importance
12	0.154	f23	0.144	f24	0.108	f2	0.079
f32	0.075	f36	0.067	f33	0.039	f26	0.027
f4	0.026	f39	0.025	f38	0.025	f25	0.022
f3	0.017	f35	0.014	f40	0.013	f31	0.013
f30	0.011	f41	0.01	f27	0.01	f28	0.009
f37	0.005	f5	0.004	f10	0.003		

Table 4: Detection results of the KDD CUP99 dataset

Method	Accuracy (%)			Recall (%)		
	Unused Feature Selection	Chi-Square	CERT	Unused feature selection	Chi-Square	CERT
LightGBM	92.623	93.871	96.198	92.706	92.593	95.263
AdaBoost	92.338	93.915	96.184	90.613	92.492	95.064
XGBoost	92.641	93.794	95.99	90.987	92.593	95.027

Table 5: Chi-square values of the NSL-KDD dataset

Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square Value
v5	3.5*1010	v6	1.7*1010	v1	1.5*108	v23	8*106
v33	7*106	v32	1.6*106	v10	3.3*105	v24	1.8*105
v3	1.3*105	v4	5.8*104	v39	5.6*104	v26	5.5*104
v25	5.5*104	v38	5.5*104	v12	3.8*104	v16	3.3*104
v13	2.7*104	v34	2.5*104	v29	2.5*104	v36	2.5*104
v2	1.9*104	v35	1.6*104	v28	1.4*104	v41	1.4*104
v27	1.3*104	v40	1.1*104	v22	1*104	v37	1*104
v14	9.7*103	v31	9.6*103	v30	8.2*103	v8	4.9*103

Table 6: Feature importance of the NSL-KDD dataset

Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Importance
v29	0.118	v26	0.089	v39	0.088	v38	0.087
v25	0.075	v12	0.061	v4	0.055	v34	0.053
v33	0.045	v36	0.038	v2	0.037	v23	0.032
v35	0.032	v30	0.025	v40	0.021	v41	0.02
v28	0.02	v27	0.019	v32	0.017	v37	0.016

Table 7: Detection results of the NSL-KDD dataset

Method	Accuracy (%)			Recall (%)		
	Unused Feature Selection	Chi-Square	CERT	Unused Feature Selection	Chi-Square	CERT
LightGBM	90.738	91.408	94.499	92.915	94.075	97.121
AdaBoost	87.468	88.098	92.809	89.136	90.628	93.128
XGBoost	90.817	91.776	93.679	91.939	93.792	96.69

Table 8: Chi-square values of the NUSW-NB15 dataset

Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square	Feature	Chi-Square Value
z22	1.2*1013	z21	1.2*1013	z12	6.4*1011	z13	5.9*1010
z9	2.4*109	z8	1.5*108	z7	1.3*108	z16	6.1*107
z18	3.1*107	z30	2*107	z28	1.9*106	z20	1.7*106
z17	1.6*106	z19	1.5*106	z23	1.4*106	z10	1.2*106
z2	2.6*105	z6	2.4*105	z34	1.4*105	z35	1.2*106
z11	1.1*105	z36	1.1*105	z27	9.6*104	z41	9.5*104
z31	8.9*104	z15	8*104	z40	7.1*104	z33	6.8*104
z5	6.1*104	z3	3.3*104	z32	6.9*103		

Table 9: Feature importance of the NUSW-NB15 dataset

Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Import.	Feature	Feature Importance
z10	0.176	z32	0.111	z11	0.103	z20	0.097
z23	0.056	z35	0.049	z3	0.042	z9	0.038
z13	0.033	z41	0.022	z36	0.021	z21	0.021
z34	0.02	z22	0.018	z2	0.017	z31	0.016
z28	0.016	z27	0.011				

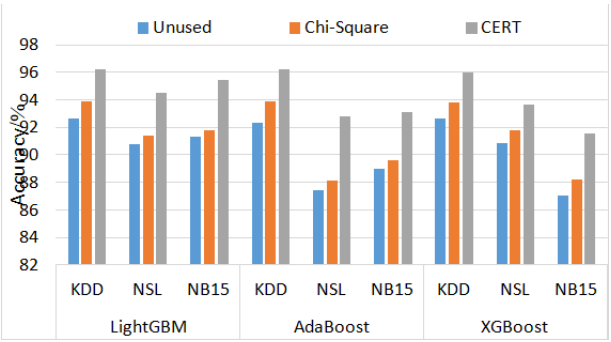


Figure 1: Detection accuracy

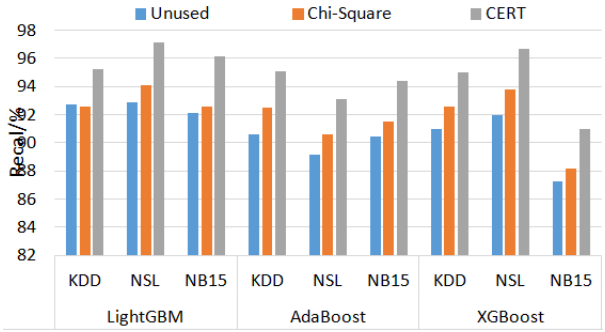


Figure 2: Detection accuracy

From Figure 1, compared with the detection algorithms without feature selection and chi-square feature selection methods, the CERT feature selection method improves the detection accuracy. Among them, LightGBM ensemble learning algorithm is stabler than AdaBoost and XGBoost ensemble learning algorithms, and its detection accuracy rate is more than 94%. From the detection accuracy rate, LightGBM ensemble learning algorithm is more suitable for network abnormal traffic detection.

Figure 2 shows the detection recall rate of LightGBM, AdaBoost, and XGBoost ensemble learning algorithms under the KDD CUP99, NSL-KDD, and NUSW-NB15 datasets.

From Figure 2, compared with the detection algorithms without feature selection and chi-square feature selection methods, the CERT feature selection method improves the detection accuracy. Among them, LightGBM ensemble learning algorithm has the highest detection recall rate compared to AdaBoost and XGBoost ensemble learning algorithm. From the detection of recall rate, LightGBM ensemble learning algorithm is more suitable for network abnormal traffic detection.

Figure 3 shows the detection time of LightGBM, AdaBoost, and XGBoost ensemble learning algorithms after using different feature selection methods under the KDD CUP99, NSL-KDD, and NUSW-NB15 datasets.

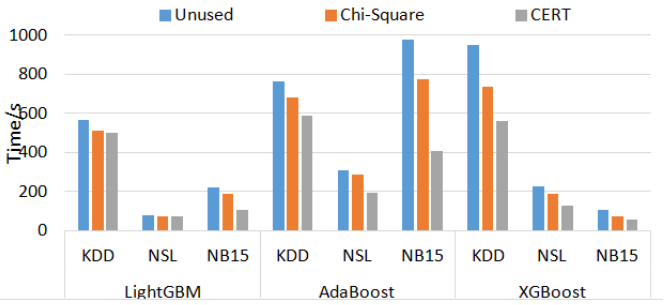


Figure 3: Detection accuracy

From Figure 3, compared with the detection algorithms without feature selection and chi-square feature selection methods, the CERT feature selection method reduces the detection time. Among them, compared with AdaBoost

Table 10: Detection results of the NUSW-NB15 dataset

Method	Accuracy (%)			Recall (%)		
	Unused Feature Selection	Chi-Square	CERT	Unused Feature Selection	Chi-Square	CERT
LightGBM	91.325	91.802	95.464	92.123	92.577	96.179
AdaBoost	88.979	89.587	93.076	90.436	91.492	94.426
XGBoost	87.06	88.187	91.559	87.238	88.162	91.014

and XGBoost ensemble learning algorithms, the LightGBM ensemble learning algorithm reduces the detection time and improves the detection efficiency. From the detection time, LightGBM is more suitable for network abnormal traffic detection.

From the analysis of the above experimental results, it can be seen that the CERT feature selection method improves accuracy and recall, effectively reduces the dimension of the dataset, and reduces the detection time of the LightGBM, AdaBoost, and XGBoost ensemble learning algorithms. Based on the overall performance of the three ensemble learning algorithms, LightGBM ensemble learning algorithm is more suitable for network abnormal traffic detection.

5 Conclusion

Compared with the detection algorithms using other feature selection methods, the CERT feature selection method proposed in this paper improves the detection accuracy and reduces the detection time. Among them, LightGBM integr ated learning algorithm is the most stable compared with AdaBoost and XGBoost integrated learning algorithm, with detection accuracy of over 94% and recall rate of over 95%.From the perspective of detection accuracy, recall rate and detection time, LightGBM integrated learning algorithm is more suitable for the detection of network abnormal traffic, and has good application value in the field of network abnormal traffic detection. The future of our work is to make out an embedded- module using our algorithm, and then put it into router to deal with abnormity in time, which should not debase the performance of router. In a word, our algorithm offers gist for processing failure of network.

References

[1] M. Jiwei, L. Zhipeng and L. Xuejiao, "Feature contour construction methods based on neural network for network abnormal behavior detection," in *Journal of Physics Conference Series*, vol. 1693, pp. 012001, 2020.

[2] N. Acharya and S. Singh, "An IWD-based feature selection method for intrusion detection system," *Soft Computing*, vol. 22, pp. 4407–4416, 2017.

[3] S. Alhaidari, A. Alharbi, M. Alshaikhsaleh, M. Zohdy, and D. Debnath, "Network traffic anomaly detection based on viterbi algorithm using SNMP MIB data," in *The 3rd International Conference*, pp. 92-97, 2019.

[4] H. Bostani and M. Sheikhan, "Hybrid of binary gravitational search algorithm and mutual information for feature selection in intrusion detection systems," *Soft Computing*, vol. 21, pp. 2307–2324, 2017.

[5] C. Chen and X. C. Liang, "Feature selection method based on Gini index and chi-square test," *Computer Engineering and Design*, vol. 40, no. 8, pp. 2342–2345, 2019.

[6] S. Chen, G. Zhu, X. Qi, L. Lei, J. Zhen, S. Wu, and M. Wu, "Research on abnormal network traffic detection based on machine learning," *Information & Communications*, 2017.

[7] H. H. Dang and H. D. Nguyen, "A PCA-based method for iot network traffic anomaly detection," in *The 20th International Conference on Advanced Communication Technology (ICACT'18)*, 2018. DOI: 10.23919/ICACT.2018.8323766.

[8] X. Deng and L. Wang, "Research on network traffic anomaly detection based on quasi real time traffic data reporting and information entropy technology," *Journal of Capital Normal University(Natural Science Edition)*, 2019.

[9] M. Gao, L. Ma, H Liu, Z. Zhang, Z. Ning, and J. Xu, "Malicious network traffic detection based on deep neural networks and association analysis," *Sensors (Basel, Switzerland)*, vol. 20, no. 5, 2020.

[10] S. Hosseini and B. Zade, "New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN," *Computer Networks*, vol. 173, pp. 107168, 2020.

[11] X. Huo, K Wu, W. Miao, L. Wang, H. He, and D. Su, "Research on network traffic anomaly detection of source-network-load industrial control system based on GRU-OCSVM," in *IOP Conference Series: Earth and Environmental Science*, vol. 300, no. 4, pp. 042043, 2019.

[12] B. Jiang, "Network intrusion detection model based on feature selection," *Modern Electronics Technique*, 2019.

[13] W. Jin, L. Fang, and L. Wang, "Abnormal detection and correlation analysis of communication network traffic based on behavior," in *Journal of Physics: Conference Series*, vol. 1648, no. 3, pp. 032087, 2020.

[14] L. Kong, G. Huang, and K. Wu, "Identification of abnormal network traffic using support vector machine," in *International Conference on Parallel & Distributed Computing*, 2017. DOI: 10.1109/PDCAT.2017.00054.

[15] X. Li, P. Yi, Y. Jiang, and J Yu, "A router abnormal traffic detection strategy based on active defense," in *Journal of Physics: Conference Series*, vol. 1738, no. 1, pp. 012103, 2021.

[16] M. Liu, W. Chen, and G. Liu, "Study on a network traffic anomaly detection model based on k-means algorithm," *Wireless Internet Technology*, 2019.

[17] J. Mao, Y. Hu, D. Jiang, T. Wei, and F. Shen, "CBFS: A clustering-based feature selection mechanism for network anomaly detection," *IEEE Access*, no. 99, pp. 1–1, 2020.

[18] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and adaboost algorithms," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 4, pp. 541–553, 2019.

[19] H. E. Mu-Yu and H. Zhou, "Relieff-mfo multi-label feature selection algorithm," *Computer Engineering and Design*, 2019.

[20] E. Nazarenko, V. Varkentin, and T. Polyakova, "Features of application of machine learning methods for classification of network traffic (Features, advantages, disadvantages)," in *International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon'19)*, 2019. DOI: 10.1109/FarEastCon.2019.8934236

[21] J. Niu, Y. Zhang, D. Liu, D. Guo, and Y. Teng, "Abnormal network traffic detection based on transfer component analysis," in *IEEE International Conference on Communications Workshops (ICC Workshops'19)*, 2019. DOI: 10.1109/ICCW.2019.8756996.

[22] M. Prasad, S. Tripathi, and K. Dahal, "An efficient feature selection based bayesian and rough set approach for intrusion detection," *Applied Soft Computing*, vol. 87, pp. 105980, 2019.

[23] R. H. Tsaih, S. Y. Huang, M. C. Lian, and Y. Huang, "ANN mechanism for network traffic anomaly detection in the concept drifting environment," in *IEEE Conference on Dependable and Secure Computing (DSC'18)*, 2018. DOI: 10.1109/DESEC.2018.8625108.

[24] B. Wang, M. Li, F. Shu, F. Li, and J. Fan, "Bayesian-based industrial internet service abnormal detection algorithm," in *Proceedings of the 2nd International Conference on Information Technologies and Electrical Engineering*, no. 10, pp. 1-4, 2019.

[25] R. Wang, J. Fang, Z. Yang, and H Li, "Multi feature selection based network traffic anomaly detection method," in *Journal of Physics Conference Series*, vol. 1288, pp. 012003, 2019.

[26] Y. Wang, "Wireless network traffic anomaly data information detection simulation," *Computer Simulation*, 2017. (`https://en.cnki.com.cn/Article_en/CJFDTotal-JSJZ201709091.htm`)

[27] H. Wei, Y. Wang, K. E. Wenlong, and H. Feng, "Abnormal network traffic classification based on improved extremely random tree," *Computer Engineering*, no. 11, pp. 33-39, 2018.

[28] H. Xia, B. Fang, M. Roughan, K. Cho, and P. Tune, "A basisevolution framework for network traffic anomaly detection," *Computer Networks*, vol. 135, no. apr.22, pp. 15–31, 2018.

[29] Y. Xin, C. Jwab, and H. Wei, "Hybrid fuzzy integrated convolutional neural network (hficnn) for similarity feature recognition problem in abnormal netflow detection," *Neurocomputing*, vol. 415, pp. 332–346, 2020.

[30] X. Ye, X. Chen, D. Liu, W. Wang, Y. Li, L. Gang, and G. Shao, "Efficient feature extraction using apache spark for network behavior anomaly detection," *Tsinghua Science and Technology*, vol. 023, no. 005, pp. 561–573, 2018.

[31] J. Zhang, J. Zhang, C. Yang, L. I. Yong, L. I. Kangyi, X. Wang, S. O. Automation, and H. D. University, "Abnormal traffic detection on process layer network of smart substation based on cyber physical fusion," *Automation of Electric Power Systems*, vol. 43, no. 14, pp. 173-181, 2019.

[32] D. Zhen, L. Ma, H. Li, Q. Li, and Z. Liu, "Network traffic anomaly detection based on wavelet analysis," in *IEEE 16th International Conference on Software Engineering Research, Management and Applications (SERA'18)*, 2018. DOI: 10.1109/SERA.2018.8477230.

Biography

Yongxin Feng received the Ph.D. degree in computer application technology from Northeastern University, Shenyang, China, in 2003. She is currently a Professor in the School of Information Science and Engineering, Shenyang Ligong University. She has authored over 80 papers in related international conferences and journals. She is the holder of 30 patents and software copyrights. Her research interests are in the areas of intelligent information processing, wireless sensor network, and communication and information systems.

Wenxin Li received the master degree in Communication and Information Engineering from Shenyang University of Technology, Shenyang, China, in 2022. Her research interests include mainly deep Learning, artificial intelligence, data analysis, network security.

Yuntao Zhao received the Ph.D. degree in control science and engineering from Nanjing University of Science and Technology, Nanjing, China, in 2013. He is a Post-Doctoral Researcher with the pattern recognition and artificial intelligence, Northeastern University, Shenyang, China, in 2015. He is currently a Professor with the Communication and Network Institute and also with the School of Information Science and Engineering, Shenyang Ligong University, Shenyang. He has authored over 30 papers published in related international conference proceedings and journals. He is the holder of 10 patents and software copyrights. His research interests include mainly deep Learning, AI algorithm, Cyberspace

security, protocol analysis and data mining.

Shengnan Geng received the Ph.D. degree in instrument science and technology from Tsinghua University, Beijing, China, in 2012. She is currently a senior engineer in Beijing Institute of Astronautical System Engineering, China. She has authored over 10 papers published in international conference proceedings and journals. Her research interests include mainly sensing technology, measurement and control, AI algorithm and data mining.

Bo Yu received the master degree in Communication and Information from Shenyang University of Technology, Shenyang, China, in 2019. Her research interests include mainly deep Learning, artificial intelligence, data analysis.

Junxing Jia received the master degree in Communication and Information Engineering from Shenyang University of Technology, Shenyang, China, in 2020. His research interests include mainly deep Learning, artificial intelligence, data analysis.

Comparison of Multiple Algorithmic Models for Malicious Attack Data Detection of Network Intrusion

Ronghua Ma

(Corresponding author: Ronghua Ma)

Student Affairs Office, Zhengzhou Railway Vocational & Technical College
Zhengzhou, Henan 450000, China
Email: amavhi6@163.com

(Received Sept. 19, 2020; Revised and Accepted Mar. 6, 2022; First Online Apr. 21, 2022)

Abstract

The existence of malicious attack data has impacted the security of networks. This paper introduced several algorithmic models, the K-means model, the classification and regression tree (CART) model, and the improved particle swarm optimization (IPSO) - backpropagation neural network (BPNN) model, analyzed their computational processes and compared the detection performance of these models on UNSW-NB15. We found that the running time of the K-means model was the longest, followed by the CART model and the IPSO-BPNN model; the accuracy of the IPSO-BPNN model was 92.65%, which was 10.01% higher than the K-means model and 5.94% higher than the CART model; the false alarm rate and missed alarm rate of the IPSO-BPNN model were significantly lower than the other two models. The results demonstrate the reliability of the IPSO-BPNN model for malicious attack data detection of network intrusion. Therefore, the IPSO-BPNN model can be further promoted and applied in practice.

Keywords: Data Detection; Decision Tree; Malicious Attack; Network Intrusion; Neural Network

1 Introduction

With the continuous development of the network, the popularity of the network has improved, and the network users are growing rapidly. The data generated in the network operation is also increasing [1], but includes a large part of malicious attack data, which has caused a serious impact on the security of the network. The increasingly complex and diversified intrusion methods [2] cause difficulties in detecting malicious attack data. With the development of data mining, more and more different algorithmic models have been applied to detect malicious attack data [3]. Liu *et al.* [4] designed a greedy algorithm-based clustering method, proposed the fuzzy rough set-based feature selection, and conducted extensive experiments on the NSL-KDD dataset and a self-built Nidsbench-based network simulation platform to demonstrate the precision of the network intrusion detection.

Dong *et al.* [5] experimented with a modified long-short memory neural network (LSTM) on the NSL-KDD dataset for a five-classification task and found that the accuracy of the method reached 82.15%. Zhang *et al.* [6] used an open set classification network (OCN) to detect unknown attacks and combined it with a clustering method to perform experiments on the KDDCUP'99 dataset and CICIDS2017 dataset. They found that the method was reliable in detecting unknown attacks. Jiang *et al.* [7] performed data dimensionality reduction by sequence backward selection (SBS) for the detection of wireless sensor networks (WSNs), used the LightGBM algorithm to detect different attacks, and found through experiments that the method had good detection performance. The detection of malicious attack data can be considered as a classification problem, i.e., to distinguish normal data from malicious attack data in the network. Therefore, this paper selected several models for data classification and compared them on the UNSW-NB15 dataset to understand which model had the best performance in detection. This work provides theoretical support for better detecting malicious attack data for network intrusion.

2 Introduction of Several Algorithmic Models

2.1 K-means Model

Clustering is a method to distinguish things according to their similarity [8], i.e., to divide the data into different groups. The main clustering algorithms include K-means, Density-Based Spatial Clustering of Applications with Noise (DBSCAN) and Agglomerative Nesting

(AGENES) algorithms [9]. The K-means algorithm was used in this paper.

The K-means algorithm is distance-based [10]. It uses Euclid distance when calculating clusters and updates the cluster centers by continuous iterations. The specific process of the algorithm is as follows.

1) Suppose there are n samples with m dimensions. K samples are randomly selected as the initial clustering centers.

2) The Euclid distance of all samples to the centers are calculated, and they are classified into the nearest class:

$$c_i = arg \min_{j-1}^{k} ||x_i - u_i||^2,$$

where c_i refers to the class to which the i-th data belongs, x_i refers to the vector of dimensions of the i-th data, and u_i refers to the vector of dimensions of the i-th cluster center.

3) According to Step (2), the mean values of dimensions of all classes are calculated, and the cluster centers are updated:

$$u'_j = \frac{\sum_{i=1}^{n} IF\{c_i = j\} \cdot x_i}{\sum_{i=1}^{n} IF\{c_i = j\}}$$

where u'_j refers to the updated center of the j-th class and $IF\{\}$ represents judgment, 1 if true and 0 if false.

4) Steps (2) and (3) are repeated until the centers no longer change. The termination condition is:

$$||u' - u||^2 < a$$

where a is an artificially specified small value.

5) The algorithm ends, and the clustering results are output.

2.2 Classification and Regression Tree Model

The decision tree is a widely used classifier [11], which builds a tree diagram based on the relationship between attributes and classes. The common decision tree algorithms include the ID3 algorithm [12], the C4.5 algorithm [13] and the classification and regression tree (CART) algorithm [14], etc. The CART algorithm was mainly studied in this paper.

The CART algorithm divides the data based on the Gini coefficient [15]. Gini coefficient refers to the probability that two randomly selected data from a dataset belong to different classes, which is used for measuring the purity of a dataset; the purer a dataset is, the lower its GINI coefficient is. The specific calculation process is as follows.

Suppose that there are n classes, $\{C_1, C_2, \cdots, C_n\}$, in the sample set S, and every class corresponds to a subset (S_i). If $|S|$ is the number of samples in S and $|C_i|$ is the number of samples belonging to C_i in S, then the formula for calculating the Gini coefficient is:

$$\begin{aligned} GINI(S) &= 1 - \sum_{i=1}^{n} p_i^2, \\ p_i &= \frac{|C_i|}{|S|} \end{aligned}$$

If there is a binary split, i.e., attribute A divides S into subsets S_1 and S_2, then the calculation formula of the Gini coefficient can be written as:

$$GINI_A(S) = \frac{|S_1|}{|S|} GINI(S_1) + \frac{|S_2|}{|S|} GINI(S_2).$$

According to the calculation result of the Gini coefficient, the smallest attribute is used as the dividing attribute, and so on, until all samples in the child nodes belong to the same class, or no attribute can be split. Finally, the decision tree is completed by the post-pruning method.

2.3 Improved Particle Swarm Optimization-Back Propagation Neural Network Model

Neural networks can solve practical problems by simulating the human brain [16], which has strong self-learning ability [17], fault tolerance and parallelism. Neural networks have wide applications in financial investment [18], industrial control [19], etc. The back propagation neural network (BPNN) was used in this paper [20].

BPNN trains the network by back propagation of errors. For a simple BPNN structure, the output of the j-th node of the hidden layer can be written as:

$$H_j = f(\sum_{i=1}^{n} w_{ij} x_i + a_j),$$

and the output of the k-th node of the output layer can be written as:

$$O_k = \sum_{j=1}^{l} H_j w_{jk} + b_k,$$

where $f(\cdot)$ is an activation function, n and l are the numbers of nodes in the input layer and the hidden layer, and w_{ij} and a_j are the weight and bias of the input layer to the hidden layer, and w_{jk} and b_k are the weights and biases of the hidden layer to the output layer.

Let the desired output be Y_k, the formula for the error can be written as:

$$\begin{aligned} x^1 E &= \frac{1}{2} \sum_{k=1}^{m} (Y_k - O_k)^2 \\ &= \frac{1}{2} \sum_{k=1}^{m} e_k^2. \end{aligned}$$

To reduce the error, BPNN adjusts the weight and bias by back propagation of the error. The update formula for the weight is:

$$\begin{aligned} w_{ij} &= w_{ij} + \eta H_j(1-H_j)x_i \sum_{k=1}^{m} w_{jk}e_k \\ w_{jk} &= w_{jk} + \eta H_j e_k. \end{aligned}$$

The update formula for the bias is:

$$\begin{aligned} a_j &= a_j + \eta H_j(1-H_j) \sum_{k=1}^{m} w_{jk}e_k \\ b_k &= b_k + \eta e_k \end{aligned}$$

where η refers to the learning rate. BPNN is sensitive to the initial weight, and different values will lead to different results. To improve the performance of BPNN in attack data detection, an improved particle swarm algorithm (IPSO) was designed in this paper to optimize the parameters of BPNN.

The PSO algorithm is based on the foraging behavior of birds [21]. Firstly, the PSO algorithm initializes a random set of particles as random initial solutions. It is assumed that in D-dimensional space, there are N particles, the position and velocity of the i-th particle are $X_i = (x_{i_1}, x_{i_2}, \cdots, x_{i_D})$ and $V_i = (v_{i_1}, v_{i_2}, \cdots, v_{i_D})$, the individual best position is $P_{best} = (P_{best_1}, P_{best_2}, \cdots, P_{best_D})$, and the global best position is $G_{best} = (G_{best_1}, G_{best_2}, \cdots, G_{best_D})$. The update formulas for the velocity and position of the particles can be written as:

$$\begin{aligned} V_i^{k+1} &= wV_i^k + c_1 rand()(P_{best} - X_i^k) \\ &\quad + c_2 rand()(G_{best} - X_i^k) \\ X_i^{k+1} &= X_i^k + V_o^{k+1} \end{aligned}$$

where k refers to the number of current iterations, w refers to the inertia weight, c_1 and c_2 are learning factors, and $rand()$ is a random number between 0 and 1.

In order to optimize the performance of the PSO algorithm, it was improved by exponentially decreasing inertia weight. The particle velocity update formula of IPSO is:

$$\begin{aligned} V_i^{k+1} &= \beta V_i^k + c_1 rand()(P_{best} - X_i^k) \\ &\quad + c_2 rand()(G_{best} - X_i^k) \\ \beta &= \beta_{end} \cdot (\frac{\beta_{start}}{\beta_{end}})^{1/(1+10k/k_{max})} \end{aligned}$$

where k_{max} refers to the maximum number of iterations, β_{start} is the initial inertia weight, β_{end} is the inertia weight when the number of iterations is maximum.

The IPSO-BPNN model is obtained by optimizing the parameters of BPNN with IPSO, which is used for the detection of malicious attack data.

3 Experimental Analysis

3.1 Experimental Setup

The experimental environment was a 64-bit Windows 10 operating system with 8 GB memory and 2.5 GB main frequency. The algorithms were implemented by the Python language. The experimental dataset was UNSW-NB15 [22], including nine types of malicious attack data and one type of normal data, as shown in Table 1. There were 49 features in the dataset, including traffic features, content features, etc. This paper used one of the subsets for the experiments, as shown in Table 2.

Table 1: UNSW-NB15 dataset

Data type	Quantity
Normal	2218761
Fuzzers	24246
Analysis	2677
Backdoors	2329
Dos	16353
Exploits	44525
Beneric	215481
Reconnaissance	13987
Shellcode	1511
Worms	174

Table 2: Experimental dataset

Data type	Training set	Test set
Normal	6522	1673
Fuzzers	1389	432
Analysis	275	74
Backdoors	274	74
Dos	578	146
Exploits	1868	432
Generic	1449	355
Reconnaissance	1294	301
Shellcode	1118	287
Worms	130	29

Based on the confusion matrix (Table 3), the performance of different models was compared, and the evaluation indicators were as follows.

1) Accuracy: $A_c = \frac{TP+TN}{TP+TN+FP+FN}$

2) False alarm rate: $F_A = \frac{FP}{TN+FP}$.

3) Missed alarm rate: $M_A = \frac{FN}{TP+FN}$.

Table 3: Confusion matrix

		Test results	
		Positive example	Counter-example
Actual situation	Positive example	TP	FN
	Counter-example	FP	TN

3.2 Model Performance Comparison Results

The running time of different models is shown in Figure 1.

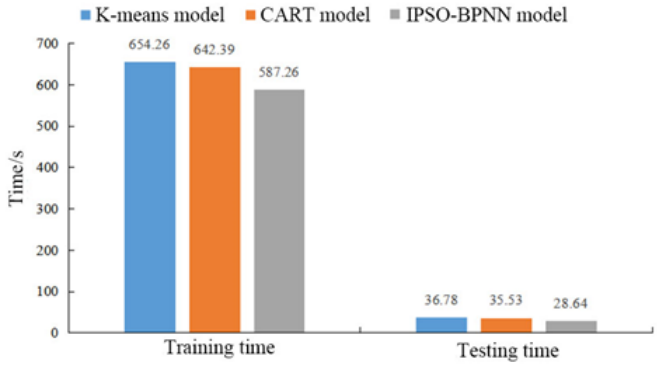


Figure 1: Comparison results of the running time of different models

It was seen from Figure 1 that among the three models, the K-means model had the longest training time, 654.26s, while the IPSO-BPNN model had the shortest running time, which was 10.24% shorter than the K-means model and 8.58% shorter than the CART model. As to the testing time, the situation was the same, i.e., the K-means model > the CART model > the IPSO-BPNN model. The testing time of the IPSO-BPNN model was 22.13% shorter than the K-means model and 1.39% shorter than the CART model, indicating that the IPSO-BPNN model had the most advantage in terms of running time.

The comparison of the detection performance between different models for malicious attack data is shown in Table 4.

It was seen from Table 4 that the accuracy of the three models were 82.64%, 86.71% and 92.78%, respectively, and the accuracy of the IPSO-BPNN model for malicious attack data detection was 10.01% higher than the K-means model and 5.94% higher than the CART model; the K-means model had the highest false alarm rate, 2.12%, and the IPSO-BPNN model had the lowest false alarm rate, 0.33%; in terms of the missed alarm rate, the K-means model > the CART model > the IPSO-BPNN model, and the IPSO-BPNN model was 8.03% lower than the K-means model and 4.05% lower than the CART model. Overall, the IPSO-BPNN model had the best performance in detecting malicious attack data.

Finally, the detection accuracy of the ISPO-BPNN model on different types of data is analyzed, and the results are shown in Figure 2.

It was seen from Figure 2 that the highest and lowest accuracy of the model was 97.64% and 88.64%, respectively; the accuracy of the model was the highest when detecting the normal data; when detecting malicious attack data, the accuracy of the model was the highest (95.21%) for Fuzzers, and the detection accuracy for the other data was above 85%. It was seen from Figure 2 and Table 2 that the more the data samples were, the higher the accuracy of the model was. The sample size of Worms was the smallest, 130 in the training set and 29 in the test set; thus, the accuracy of detecting Worms was the lowest.

4 Conclusion

This paper compared and analyzed the performance of three models, the K-means model, the CART model and the IPSO-BPNN model, in detecting malicious attack data for network intrusion with the UNSW-NB15 dataset. The results showed that the IPSO-BPNN model not only had advantages in running time but also had superior accuracy, false alarm rate and missed alarm rate than the K-means model and the CART model, i.e., the IPSO-BPNN model was the most suitable for malicious attack data detection and can be better applied in practice.

References

[1] M. Belouch, S. El Hadaj, M. Idhammad, "Performance evaluation of intrusion detection based on machine learning using apache spark," *Procedia Computer Science*, vol. 127, pp. 1-6, 2018.

[2] L. Breiman, J. Friedman, R. Olshen, C. Stone, "Classification and regression trees," *Encyclopedia of Ecology*, vol. 57, no. 1, pp. 582-588, 2015.

[3] I. Cordova, T. S. Moh, "DBSCAN on resilient distributed datasets," in *International Conference on High Performance Computing & Simulation*, pp. 531-540, 2015.

[4] R. H. Dong, X. Y. Li, Q. Y. Zhang, H. Yuan, "Network intrusion detection model based on multivariate correlation analysis – long short-time memory network," *IET Information Security*, vol. 14, no. 2, pp. 166-174, 2020.

[5] D. G. Ferrari, L. De Castro, "Clustering algorithm selection by meta-learning systems: A new distance-based problem characterization and ranking combina-

Table 4: Comparison results of detection performance of different models

	K-means model	CART model	IPSO-BPNN model
Accuracy rate/%	82.64	86.71	92.65
False alarm rate/%	2.12	1.89	0.33
Missed report rate/%	16.74	12.76	8.71

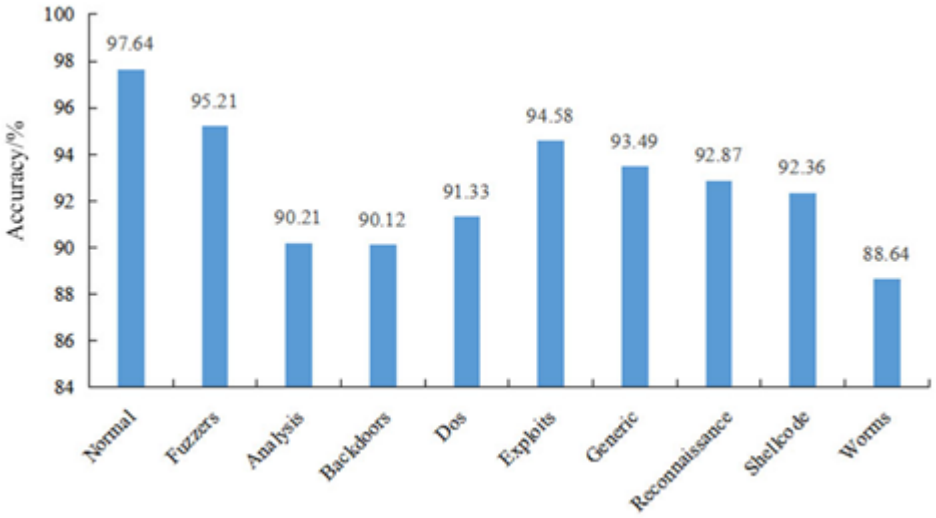


Figure 2: Detection results of the IPSO-BPNN model

tion methods," *Information Sciences*, vol. 301, pp. 181-194, 2015.

[6] M. M. Ghiasi, S. Zendehboudi, A. A. Mohsenipour, "Decision tree-based diagnosis of coronary artery disease: CART model," *Computer Methods and Programs in Biomedicine*, vol. 192, no. 6, pp. 105400, 2020.

[7] E. Gokgoz, A. Subasi, "Comparison of decision tree algorithms for EMG signal classification using DWT," *Biomedical Signal Processing & Control*, vol. 18, pp. 138-144, 2015.

[8] A. K. Jain, J. Mao, K. M. Mohiuddin, "Artificial neural networks: A tutorial," *Computer*, vol. 29, no. 3, pp. 31-44, 2015.

[9] S. Jiang, J. Zhao, X. Xu, "SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments," *IEEE Access*, vol. 8, pp. 169548-169558, 2020.

[10] V. Jyothsna, K. Munivara Prasad, K. Rajiv, G. Ramesh Chandra, "Flow based anomaly intrusion detection system using ensemble classifier with feature impact scale," *Cluster Computing*, vol. 3, pp. 1-18, 2021.

[11] C. Kiennert, Z. Ismail, H. Debar, J. Leneutre, "A survey on game-theoretic approaches for intrusion detection and response optimization," *ACM Computing Surveys*, vol. 51, no. 5, pp. 90.1-90.31, 2019.

[12] P. Kumar, G. P. Gupta, R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9555-9572, 2021.

[13] J. Liu, W. Zhang, Z. Tang, Y. Xie, T. Ma, J. Zhang, G. Zhang, J. P. Niyoyita, "Adaptive intrusion detection via GA-GOGMM-based pattern learning with fuzzy rough set-based attribute selection," *Expert Systems with Applications*, vol. 139, pp. 112845, 2020.

[14] V. Phu, V. Tran, V. Chau, N. D. Dat, K. L. D. Duy, "A decision tree using ID3 algorithm for English semantic analysis," *International Journal of Speech Technology*, vol. 20, no. 3, pp. 593-613, 2017.

[15] B. Shao, C. Ni, J. Wang, Y. Wang, "Research on venture capital based on information entropy, BP neural network and CVaR model of digital currency in Yangtze River Delta," *Procedia Computer Science*, vol. 187, pp. 278-283, 2021.

[16] W. Song, W. Ma, Y. Qiao, "Particle swarm optimization algorithm with environmental factors for clustering analysis," *Soft Computing*, vol. 21, no. 2, pp. 283-293, 2017.

[17] B. Wang, X. Gu, M. Li, S. Yan, "Temperature error correction based on BP neural network in meteorological wireless sensor network," *International Journal of Sensor Networks*, vol. 23, no. 4, pp. 265, 2017.

[18] J. Wang, J. Wang, J. Song, X. Xu, H. Shen, S. Li, "Optimized cartesian K-Means," *IEEE Transactions*

on Knowledge & Data Engineering, vol. 27, no. 1, pp. 180-192, 2015.

[19] X. Wang, C. Zhou, X. Xu, "Application of C4.5 decision tree for scholarship evaluations - ScienceDirect," *Procedia Computer Science*, vol. 151, pp. 179-184, 2019.

[20] F. F. Zhai, S. L. Ma, W. Liu, "A study on PID control and simulation based on BP neural network," *Advanced Materials Research*, vol. 468-471, pp. 742-745, 2012.

[21] Y. Zhang, X. Gao, S. Katayama, "Weld appearance prediction with BP neural network improved by genetic algorithm during disk laser welding," *Journal of Manufacturing Systems*, vol. 34, pp. 53-59, 2015.

[22] Z. Zhang, Y. Zhang, D. Guo, M. Song, "A scalable network intrusion detection system towards detecting, discovering, and learning unknown attacks," *International Journal of Machine Learning and Cybernetics*, vol. 12, pp. 1649–1665, 2021.

Biography

Ronghua Ma is born in Lixian county,Hunan Province,has received the master's degree from Wuhan University. She is an associate professor. Her research directions are wireless sensor network, network security, and artificial intelligence.

A Statistical P2P Botnet Detection Resilient to Mimicry Attacks

Fateme Faraji Daneshgar, Atiye Mohammadkhani, and Maghsoud Abbaspour
(Corresponding author: Maghsoud Abbaspour)

Faculty of Computer Science and Engineering, Shahid Beheshti Univercity
GC, Evin, Tehran 1983969411, Iran
Email: maghsoud@sbu.ac.ir

(Received Mar. 7, 2021; Revised and Accepted Mar. 3, 2022; First Online Apr. 24, 2022)

Abstract

Botnet technology has continued to evolve rapidly, making detection a very challenging problem. P2P botnets are more dangerous and resistant than all emerged botnets due to their distributed architecture. The most proposed P2P botnet detection schemes are designed, relying on the statistical behavior of bots. However, considering the adversarial nature of the botnet detection problem, the bots can be designed to mimic normal behavior and fly under the radar. Thereupon, designing a P2P botnet detection system resilient to the mimicry attack is paramount. In this paper, we implement a mimicry P2P botnet to investigate the resiliency of existing P2P botnet detection schemes. Furthermore, a statistical feature set is proposed to leverage botnets' inherent properties. Our experimental results showed that the proposed feature set is resilient to mimicry attacks and can detect P2P bots with high accuracy.

Keywords: Mimicry Botnet Detection; P2P Botnet Detection; Resilient P2P Botnet Detection

1 Introduction

A 'botnet' is a set of compromised devices as 'bot' (zombie), which is infected by malware instances. It is managed remotely by 'botmaster' through a command and control (C&C) channel. Botnets are becoming increasingly prevalent as the primary enabling technology in a variety of malicious campaigns such as email spam, click fraud, distributed denial-of-service (DDoS) attacks, and Cryptocurrency mining.

To eliminate P2P botnets many P2P botnet detection schemes are proposed. However, despite the impressive efforts of security researchers, they do not achieve much success in the cybersecurity arms race. Malware authors continuously utilize advanced technologies to harden the process of detection [3, 19]. P2P bots are designed to mimic legitimate cyber behavior to fly under the radar and disguise their malicious actions [16,25,26]. For example, Matta *et al.* [16] proposed a botnet with the ability to emulate normal behavior by continually learning admissible patterns from the environment. The bots mimic normal patterns by picking messages from an emulation dictionary, which is learned continually, to ensure that a reasonable innovation rate can be sustained.

The botnet detection mechanisms are based on the distinguishing characteristics of malicious and benign traffic, which are utilized as botnet footprints. Although the proposed approaches are finely tuned to distinguish between benign and malicious behavior, their resiliency against mimicry attacks does not receive much attention. In our previous study [5], we analyzed P2P botnet detection footprints utilized in detection systems in terms of their resilience against the existence of legitimate P2P traffic and mimicry attacks. We observed that the most proposed footprints could be disrupted using mimicry attacks. However, the effect of mimicry attacks on the accuracy of proposed P2P botnet detection schemes is not investigated.

One of the most common approaches to detect botnets is statistical botnet detection, in which a detection model is trained using a machine learning method and some statistical features (like the average of "packet length" and "inter-arrival time between packets" in a flow). The inspiration behind these approaches is that the behavior of bots is statistically different from benign hosts. For example, since the bots communicate with each other to conserve their connectivity and request the botmaster's commands, the length of the packets in malicious traffic is different from that of the benign traffic in which the network flows are utilized to exchange data. However, P2P bots can be designed to mimic normal behavior in terms of these features and subvert the detection mechanisms based on these statistical behaviors.

The resiliency of detection systems is highly dependent on the security of utilized machine learning methods and features. The security of machine learning approaches applied in botnet detection systems is investigated in previous studies [8]. However, the resilience of proposed ap-

proaches from the utilized features point of view is not considered. Consequently, investigating the proposed statistical detection approaches in terms of their resilience against the mimicry attack could shed light on the drawbacks of existing schemes and help to design the more resilient approaches.

In this paper, we implemented a mimicry P2P botnet in which the length of the packets is manipulated to mimic normal behavior. The "length of packets" is selected since the most important features used in most proposed approaches with high "information gain" are based on the "packet length" properties. Then, we utilize this botnet to investigate the resilience of the proposed statistical P2P botnet detection systems using this botnet. Furthermore, a feature set is proposed to build a statistical detection model. The proposed feature set is not only resilient to mimicry attacks but also results in botnet detection with high precision.

The rest of this paper is organized as follows. Related work is discussed in Section 2, followed by the implementation details of the mimicry P2P botnet described in Section 3. Section 4 explains our resilient feature set. The evaluation and the experimental results are given in Section 5, and Section 6 concludes the paper.

2 Related Work

The most proposed P2P botnet detection schemes are based on the models built from the network behavior of bots using some machine learning and data mining approaches. However, the problem of botnet detection is adversarial, as the botmaster can change the behavior of bots or mimics the normal behavior to subvert the detection systems. Therefore, in this section, we review the related works in two Subsections. In Subsection 2.1, the previous studies aim at analyzing and evaluating the security of botnet detection proposals are introduced. Then, the proposed P2P botnet detection schemes based on machine learning approaches are reviewed in Subsection 2.2.

2.1 Security Evaluation of Botnet Detection Schemes

Although the security of botnet detection poses critical challenges, it has been addressed in a few studies [5,8,13,22,23]. As mentioned earlier, machine learning techniques are applied in many botnet detection proposals to build the detection model. Therefore, the security flaws of machine learning approaches can be misused by the adversary to subvert the detection system. Thereupon, Gardiner *et al.* [8] systematically investigated attacks against the ML components used in these approaches using existing models from the adversarial machine learning literature.

Stinson and Mitchell [22] introduced a systematic framework for evaluating the evasion ability of bot/botnet detection schemes in terms of the cost of evasion techniques against bot/botnet detection methods. Two costs are considered to evaluate the efficiency of a technique: implementation complexity and the effect of the attack on botnet utility. Implementation complexity is based on the ease with which bot writers can incrementally modify current bots to evade detection. To analyze the impact of an evasion tactic on botnet utility, they introduced five aspects of botnet utility as the diversity of attacks, lead time required to launch an attack, botnet size, attack rate, and synchronization level. They analyzed different evasion tactics in terms of the implementation cost and its impact on botnet utility using the five mentioned criteria.

Knysz *et al.* [13] presented several novel mimicry attack techniques that allow botmaster to avoid fast-flux based detection. In this study, they first analyzed the state-of-the-art fast-flux detectors and their effectiveness against the current botnet threat, demonstrating how botmasters can thwart detection strategies.

Su *et al.* [23] introduced the forward-backward feature that is robust against the variation over payload length, the inter-arrival of packets, and the number of packets in the flow. In this approach, each flow is translated into a string of ¡in¿,¡out¿ representing the direction of the packets in the flow. Then, the corresponding directionless string is computed using the xor operation. Afterward, the produced forward-backward strings with any arbitrary length are mapped to the same dimension feature using n-gram. They showed that adding this feature to traditional feature sets can improve the accuracy of proposed schemes by around 5%, and it solely can achieve an accuracy of 90%. The authors showed that the resilience of previous approaches against the noise could be improved by adding the forward-backward string feature to the traditional feature sets. However, the forward-backward string feature also is not resilient against mimicry attacks as the adversary can insert junk packets between the main packets to disrupt the order of ¡in¿ ¡out¿ strings.

In our previous work [5], we investigated the resilience of proposed P2P botnet detection footprints against three scenarios, including 1) the coexistence of malicious and benign traffic, 2) parasite P2P botnets, and 3) mimicry attacks. We defined the *resilience* using two criteria of distortion of the footprint and the ability of the footprint to distinguish the malicious traffic. If a footprint does not be distorted and could detect the malicious traffic in the evaluation scenario, the footprint is resilient to that scenario. We observed that the most proposed P2P botnet footprints are not resilient to the evaluation scenarios. Therefore, designing the more resilient botnet detection schemes is desirable.

2.2 Machine Learning Based P2P Botnet Detection Schemes

The studies introduced in this Subsection aim at finding the most relative statistical features and most efficient ML approach to train the detection model. We considered

these studies to evaluate the resiliency of their proposed statistical feature set against mimicry attacks. As a consequence, the detection rate and results of the papers are not reported.

Garg *et al.* [9] proposed a statistical P2P botnet detection method based on the Random Forest classifier. The authors introduced 12 features related to some flow statistics like duration, number of bytes, and number of packets. They also tackled the problem of imbalanced data using some techniques like downsampling and cost-sensitive learning.

Liao *et al.* [14] used a methodology based on packet size to distinguish between P2P Botnet traffic and legitimate P2P traffic. The authors showed that the size of P2P Botnet packets is smaller than that of any other P2P application. They utilized a feature set based on the statistical characteristics of flows and sessions to detect the bot traffic. Bayesian networks, Naive Bayes and J48, are used to classify network traffic.

Saad *et al.* [18] studied the ability of five different commonly used machine learning techniques to meet online botnet detection requirements, namely adaptability, novelty detection, and early detection. The authors utilized a set of seven flow-based and four host-based features to characterize the malicious p2P traffic. They selected the most common machine learning classification techniques that were used in the literature to detect botnet as Nearest Neighbors Classifier, Linear Support Vector Machine, Artificial Neural Network, Gaussian Based Classifier, and Naive Bayes classifier. However, they found that none of the studied techniques can address all the above requirements at once.

Zhao *et al.* [28] proposed an approach to detect botnet activity by classifying network traffic behavior. The authors selected a set of attributes based on the behavior of various well-known protocols as well as the behavior of known botnets such as Storm, Nugache, and Waledac. For example, the bot queries for updates or instructions on the network continuously, resulting in many uniform-sized, small packets that continuously occur. They utilized a set of seven flow-based and one host-based attributes to train the detection model based on the Bayesian Network and a Decision Tree algorithm.

Yu *et al.* [27] proposed a data mining-based approach for botnet detection base on similarity search and incremental discrete Fourier transform (DFT). To represent raw traffic flows, they captured network flows and converted these flows into a feature stream consisting of some flow-based attributes such as average bytes-per-packet, average packets-per-second, and flow duration. Then, the feature streams were clustered based on the average Euclidean distance. To deal with the challenge of computing the similarities among huge feature streams, the authors used the DFT as the method of similarity search.

Barthakur *et al.* [4] claimed a novel approach to set small rules using Fuzzy logic for P2P botnet detection with the intuition that fuzzy rules with soft boundaries might improve the detection accuracy. They generated fuzzy rules using the Fuzzy Unordered Rule Induction Algorithm (FURIA) from a dataset of four statistical flow-based features extracted from C&C traffic. Ullah Khan *et al.* [12] proposed a P2P botnet detection scheme based on a two-stage traffic classification method. At the first stage, the non-P2P traffic is filtered to reduce the amount of network traffic through well-known ports, DNS queries, and flow counting. To reveal the similarity of C&C communication between zombie hosts in the second stage, they introduced 9 features extracted from network conversation. They utilized three Machine Learning Classifiers of Naive Bayes, Decision Tree, and ANN to train the detection model.

Alauthman *et al.* [2] proposed a P2P Bot detection based on an adaptive multilayer feed-forward neural network in cooperation with decision trees. In this study, 29 features are extracted based on the definition of a connection as a group of packets exchanged between two different hosts, which are identified by the 4-tuple (source IP address, destination IP address, source port, and destination port). Most of the features are related to TCP control packets like SYN, ACK, FIN, etc.

In a more recent study, Alauthman *et al.* [1] developed a reinforcement learning-based P2P botnet detection system, which comprises a traffic reduction method, to deal with a high volume of network traffic. The authors claimed that their proposed system is capable of detecting the bots before the bot launches any malicious activity. In this study, 43 flow-level features and 16 host-level features are collected. Then, a classification and regression tree (CART) [15] is used as the feature reduction technique, and 22 features are selected as significant features. Finally, a detection model is trained using the Reinforcement Learning method.

Gadelrab *et al.* [7] proposed BotCap, a botnet detection system based on statistical characteristics. The authors analyzed several botware samples of known botnets and collected a set of 52 statistical features (mostly introduced in previous studies) to distinguish between benign and malicious traffic. Then, they conducted some experiments to test the suitability of ML techniques and also to pick a minimal subset of the identified features that provide the best detection. However, their testbed includes IRC and HTTP-based botnets lacking the P2P botnets.

Homayoun *et al.* [10] proposed a deep learning-based botnet traffic analyzer called Botnet Traffic Shark (BoTShark). To detect malicious botnet traffics, the authors adopted two deep learning techniques, namely Autoencoders and Convolutional Neural Networks (CNNs), to eliminate the dependency of detection systems to primary features achieved by NetFlow extractor tools. Botshark has the capability of detecting malicious traffics from botnets of two common topologies, namely centralized and decentralized botnets. Furthermore, it does not pre-filter any primary extracted features and does not need expert knowledge in selecting proper features to extract features automatically.

Wang *et al.* [24] proposed BotMark, an automated

model that detects botnets with hybrid analysis of flow-based and graph-based network traffic behaviors. They utilized 15 statistical flow-based traffic features as well as 3 graph-based features in building the detection model. For flow-based detection, they consider the similarity and stability of C-flow as measurements in the detection. In particular, they employ k-means to measure the similarity of C-flows and assign similarity scores and calculate the stability score of C-flows through the distribution of packet length within a C-flow. The flows that share the same protocol, source IP, destination IP and port within an epoch are defined as a C-flow. The graph-based detection is based on the observation that the neighborhoods of anomalous nodes significantly differ from those of normal nodes in communication graphs. The least-square technique and Local Outlier Factor (LOF) is utilized to calculate anomaly scores that measure the differences of their neighborhoods. BotMark performs automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors by an ensemble of the detection results based on similarity scores, stability scores, and anomaly scores.

3 A Mimicry P2P Botnet

To evaluate the resilience of proposed statistical P2P botnet detection schemes against the mimicry attacks, we designed and implemented a mimicry P2P botnet in which the bots mimic the normal behavior in terms of "packet size." Our mimicry botnet is based on a proof of concept P2P botnet written in Python [11]. This botnet is resistant to targeted takedown attempts and protects the identity of the botnet owner. These characteristics are achieved by using a Kademlia distributed hash table (DHT) and three basic components:

- Bots- The compromised nodes that join the network, query a specific hash in the DHT, post their unique ID, and then wait for an acknowledgment from a commander.
- Commander - A commander that continuously checks the login location for new bots, and sends out ACKs when new bots join the network. Commands are sent via specific query locations that are unique to each bot. Every bot has a unique command location; therefore, it is easy to send commands to individual clients while still being easy to send global commands to all clients. The commander never has direct contact with a bot. All communication is performed through DHT queries, and it protects the commander from being compromised by a rogue client.
- Server - a Kademlia server for clients to bootstrap into the network

There are many tools to manipulate the packet length alive [20] such as Hping, Ostinato, Scapy, and NetfilterQueue Scapy. We utilized NetfilterQueue Scapy, which provides access to the packets that are matched by an iptables rule in Linux. The packets can be accepted, dropped, altered, or given a mark. A NetfilterQueue object represents a single queue. Iptables is an application that allows users to configure specific rules that will be enforced by the kernel's netfilter framework. It acts as a packet filter and firewall that examines and directs traffic based on the port, protocol, and other criteria. To capture the C&C traffic of the bots, we defined the Iptables rule as:

Iptables -A OUTPUT -p udp –dport 8468 -j NFQUEUE –queue-num 1

Then a NetfilterQueue is created and bound to that rule. The packets are matching the rule wait in the queue for manipulation.

Algorithm 1 shows the mimicking process in which the packet size is justified using the normal frequency distribution. For each packet in the queue, the length of its payload is computed, and a random length is selected from F. This length should be greater than the payload length; otherwise, the random selection is repeated. Afterward, some junk bytes are inserted to the payload to reach the Mimicrylen. Finally, the mimicry packet is accepted and sent.

Algorithm 1 Pseudo code of packet manipulation

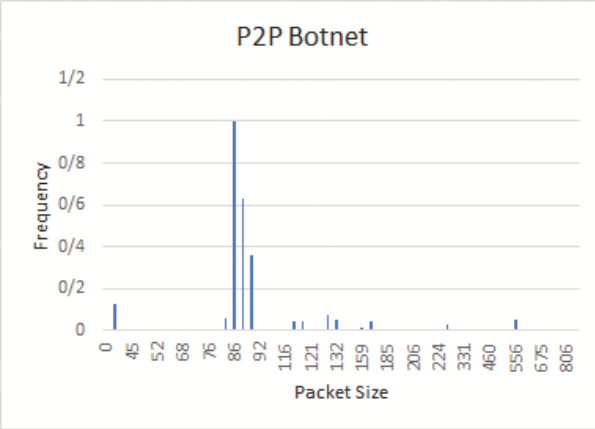
Input: Q: The C&C packet queue, F: The frequency distribution of normal packet size
Output: The mimicry C&C packet

```
for each packet, p, in Q do
    packetLen = The payload length of p
    Mimicrylen = a randomly selected number from F
    while Mimicrylen¡packetLen do
        Mimicrylen = a randomly selected number from F
    end while
    insert Mimicrylen − packetLen junk bytes to the payload of p
    accept p
end for
```

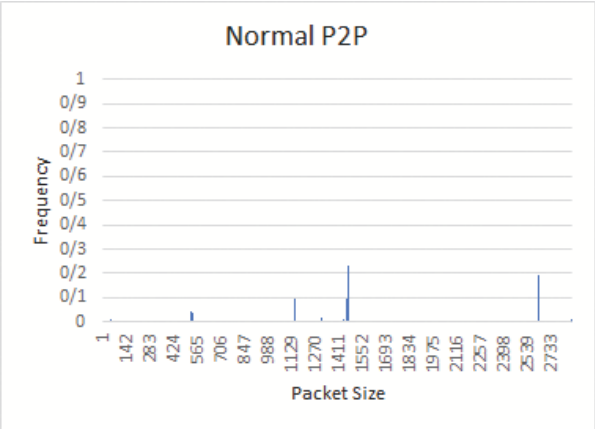
Fig. 1 shows the frequency of the packet size distribution related to the traffic of a P2P bot, an eMule peer, and a mimicry bot. As it is illustrated in the figure, the distribution of packet size in mimicry bot and eMule peer is very similar.

4 A Statistical Feature Set to Characterize P2P Bots Resilient to Mimicry Attack

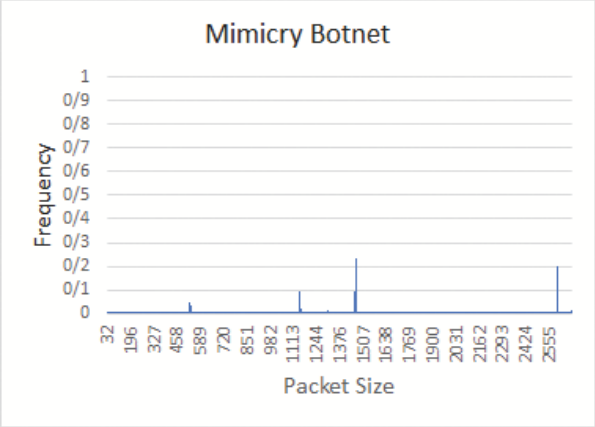
As mentioned before, most statistical botnet detection frameworks are relying on the correlation of flows based on the *Packet Size* and *Timing* behavior of bots to distinguish between malicious and benign traffic. We showed in the previous section that the adversary could mimic



(a) P2P botnet



(b) Normal P2P application



(c) Mimicry botnet

Figure 1: Packet Length Distribution in P2P botnet, Normal P2P application and Mimicry botnet

the normal behavior in terms of the "packet size" characteristics by selecting a random packet size from normal packet size distribution and injecting the required number of junk bytes into the bot packet.

On the other hand, since bots are predetermined programs, there exists some regularity or periodicity in terms of timing behavior, while no regularity can be seen in human-driven activities. Consequently, to mimic the normal behavior and to fly beneath the radar, the adversary should perturb the timing regularity. This can be done by injecting a bit of random delay between packets sending by bots. Therefore, the main question arises; could we build a detection model based on the statistical characteristics being resilient to mimicry attack?

To define the resilient features, we should focus on the fundamental characteristics of the botnets that are essential to the connectivity of bots and the utility of botnet. In our previous work [5], we analyzed the botnet detection footprints introduced in proposed botnet detection schemes in terms of their resilience against the coexistence of benign P2P traffic, parasite P2P botnets, and mimicry efforts. Based on these analyses and some experimental investigations, we introduced some resilient characteristics. One of the main resilient characteristics of P2P bots is that they keep up persistent communications with each other for efficiency reasons. On the other hand, to conserve stealthiness, they maintain a list of known peers to bootstrap into the network aiming at limiting the number of active connections. Thereupon, P2P bots contact a smaller set of peers in comparison to the benign P2P nodes. Therefore, two resilient characteristics of P2P bots in comparison to benign P2P nodes are:

- long-lived flows
- small set of contact

Thereupon, a statistical feature set defined based on these characteristics would be resilient to mimicry attacks. To capture the "long-lived flows" attribute, the "flow duration" feature is used, which is one of the most informative features in most proposed statistical botnet detection schemes. The network flows are generated using 5-tuple <source address, destination address, source port, destination port, protocol >, and the *Flowgap* threshold denoted as W_f. The *Flowgap* threshold indicates the maximum allowed time between the packets in a flow.

However, the network flows in some legitimate P2P applications (like skype) also are long-lived. Nevertheless, our analyses show that the network traffic between two skype peers and two P2P bots is distinguishable using some other statistical characteristics like "the number of flows in a time window". As a consequence, to extract these features, the network flows of every two hosts are group into a *Flowgroup* using the *Convgap* threshold denoted as W_c. In other words, these features are computed from network conversations.

The second fundamental attribute of P2P bots is the "small set of contacts". To capture this behavior, the net-

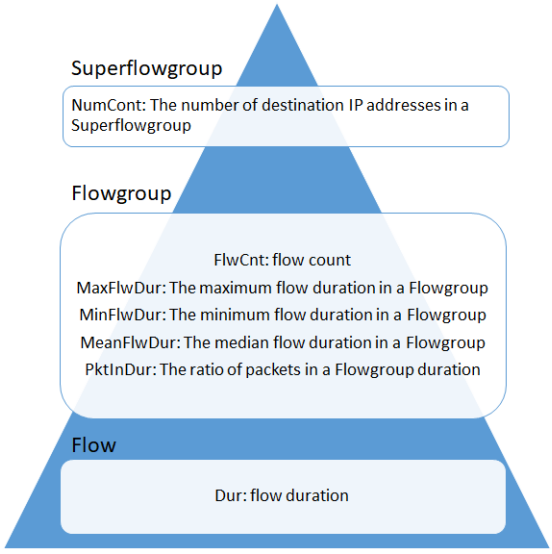


Figure 2: Proposed resilient feature set

work flows of each host, are aggregated into a *Superflowgroup* using the *Hostgap* threshold denoted as W_h. Then the number of destination IP addresses is computed as "the number of contacts" feature. Fig. 2 shows the proposed statistical features.

Therefore, our proposed resilient feature set is computed from three different flow granularity of *Flow*, *Flowgroup*, and *Superflowgroup*. The statistical features based on the fundamental characteristics of P2P bots Computed from different levels of traffic aggregation could result in resiliency against the mimicry attacks.

5 Evaluation

To evaluate the performance and resilience of the proposed approach, a series of experiments are conducted. The detailed description of evaluation datasets is described in Subsection 5.1. The efficiency of our proposed statistical feature set is evaluated in Subsection 5.2. Finally, in Subsection 5.3, we examine the resilience of the proposed feature set against the mimicry attacks.

5.1 Evaluation Datasets

To experiment with the efficiency and resilience of the proposed statistical feature set, we need two types of datasets. The first one includes the real-world P2P botnet traffic utilized in most proposed P2P botnet detection schemes to evaluate the detection accuracy along with the legitimate P2P traffic and the network background traffic. On the other hand, the second dataset includes the laboratory P2P botnet and the mimicry botnet to investigate the resilience of the proposed feature set in comparison to the previously proposed feature sets. In continue, the evaluation datasets are described in more detail.

5.1.1 Performance Evaluation Datasets

There are two datasets of network traces related to the real-world botnets [17, 18] that are utilized for performance evaluation in most proposed P2P botnet detection schemes. Therefore, to evaluate the detection rate of our proposed feature set along with the previous approaches, we utilized two datasets, D1 and D2, each containing three types of network traces:

- **P2P Botnet network traces**: The ISOT dataset [18] contains the malicious traffic of two Storm bots for 1 hour and a Waledac bot for near one hour. This traffic is utilized as the P2P botnet traffic in D1. The dataset obtained from [17] contains network traces of three P2P botnets, Storm, Waledac, and Zeus. This dataset includes the network traffic of 13 Storm bots for 7 days and 3 Waledac bots for 3 days and a Zeus bot for 34 days. The randomly selected one hour of network traces from three Storm bots and a Waledac bot and a Zeus bot is considered as P2P botnet traffic in the D2 dataset.

- **Legitimate P2P network traces**: The dataset obtained from [17] contains the network traffic of five benign P2P applications, namely uTorrent, eMule, Vuze, Skype, and FrostWire, for several contentious days. We randomly selected one hour of each application's network traces as legitimate P2P traffic for both D1 and D2 datasets.

- **Network background traffic**: The ISCX IDS dataset [21] has been generated in a physical testbed implementation using real devices that generate real (e.g., SSH, HTTP, and SMTP) traffic. We utilize the randomly selected three hours of this traffic as network background traces for both D1 and D2 datasets.

5.1.2 Resilience Evaluation Dataset

As it is described earlier, we implement a mimicry P2P botnet to evaluate the resilience of proposed statistical P2P botnet detection schemes against the mimicry attack. The mimicry botnet is based on a proof of concept P2P botnet [11], which utilizes Kademlia DHT as its C&C channel. We set up both P2P botnet and mimicry botnet in our college lab in a controlled environment consisting of 15 virtual machines as P2P bots, and two virtual machines as bootstrap and commander servers. The C&C traffic of bots from both botnets is captured for one day using Wireshark. Table 1 shows the statistics of the D3 dataset consisting of the randomly selected 6 hours of the collected C&C traffic of the P2P bots ($D3_1$) and the mimicry P2P bots ($D3_2$). It should be noted that the legitimate P2P traffic and the network background traffic in $D3_1$ and $D3_2$ datasets are the same as the D1 and D2 datasets.

Table 1: Statistics of mimicry and P2P traces

C&C traffic	#Packets	#Flows
P2P Botnet ($D3_1$)	771264	1082
Mimicry Botnet ($D3_2$)	737635	1051

5.2 Performance Evaluation and Results

The first step to evaluate the efficiency of the proposed statistical feature set is parameter tuning. Our proposed features are extracted from three levels of Flow, Flowgroup, and Superflowgroup, which are defined using Flowgap (W_f), Convgap (W_c), and Hostgap (W_h) parameters. To find the best values of these parameters, we conducted several experiments with W_f ranging from 20 to 80, and W_c ranging from 120 to 600, and W_h ranging from 900 to 1800 seconds. The J48 decision tree is selected as the classification approach, and 10-fold cross-validation is used to estimate the error rate of the classifier. Tables 2 and 3 show the results of these experiments for D1 and D2 datasets, respectively.

The values of *TPR (True Positive Rate)* and *FPR (False Negative Rate)* are reported as the measures of detection accuracy, and the *Treesize* values (the size of the J48 tree) are reported as the measure of model complexity. The best result is highlighted in each row. The results of this experiment indicate that the accuracy of the detection model built using our proposed resilient feature set is reasonable for a massive range of parameters. Our detection model achieves the TPR= 100% and FPR=0 for some parameter settings.

It can be seen from the tables that the best results are obtained for $W_h = 1500$s and $W_h = 1800$s. In other words, it needs at least 1500 seconds for the host-level behavior of bots to be revealed. However, to select distinct parameter values for remainder of evaluation experiments, we choose $W_f = 60$, $W_c = 600$, and $W_h = 1800$.

To estimate the effect of different machine learning approaches on our proposed detection model, we utilize four commonly used classifiers, namely, Bayesian network(BN), J48 decision tree, Random forest (RF), and Support Vector Machine (SVM) to build the P2P botnet detection model. Table 4 shows the results of this experiment in terms of TPR, FPR, and F-Measure criteria for D1 and D2 datasets. It is evidenced that the detection models built using the proposed feature set and J48 and RF as classification approaches achieve the high TPR of 100% and low FPR of 0%. Despite the lower performance of the detection model built based on SVM and BN, they are yet acceptable and comparable with other published detection schemes.

Table 5 shows the detection performance of our proposed P2P botnet detection model along with the best-reported results of some published P2P botnet detection schemes. It is observed that our proposed approach achieves the highest TPR and lowest FPR. It should be noted that this significant performance is achieved with the cost of computation complexity as our proposed feature set is computed from three different levels of Flow, FlowGroup, and Superflowgroup. Nevertheless, considering the fact that the detection model is learned once in offline mode, this overhead is rational. Furthermore, using this 3-level feature set, we aim at achieving a resilient P2P botnet detection scheme that is investigated in the next subsection.

5.3 Resilience Evaluation of Proposed Statistical Feature Set

To investigate the resilience of our proposed Resilient Feature Set (RFS) in comparison with some other statistical feature sets introduced in the literature, we conducted two experiments. In the first experiment, a P2P botnet detection model is built for each statistical feature set using the J48 decision tree classification approach. These models are trained using the randomly selected 60% of the $D3_1$ dataset (the network traces of a P2P botnet) and then are tested using the remaining 40% of this dataset. The first experiment aims at evaluating our proposed and existing statistical feature set in the same testbed including the same dataset and model training approach.

However, in the second experiment, we consider the resilience evaluation of our proposed feature set in comparison with other statistical feature sets. To this end, we conducted a mimicry attack to the trained P2P botnet detection models trained in the first experiment. In other words, the P2P botnet detection models trained in the first experiments are verified using the randomly selected 40% of the $D3_2$ (the network traces of the mimicry P2P botnet).

The statistical feature sets introduced in other P2P botnet detection proposals are listed in table 6. The descriptions of these features are described Table 7.

To build the detection models, we utilize the J48 decision tree classification implemented in Weka [6]. The process of aggregating the network packets into flows and extracting the features is implemented in python.

Table 8 shows the results of these experiments. The second and third columns show the TPR and FPR of the first experiment and the fourth and fifth columns show the results of the second experiment. It can be seen that the P2P botnet detection model trained using the RFS achieves the best results with the TPR of 99.4% and FPR of 0%.

Furthermore, the P2P botnet detection models trained using the previous statistical feature sets can not resist against the mimicry attack. Fig. 3 shows the reduction in TPR of P2P botnet detection models due on the mimicry attack. The TPR and FPR of 0% related to these models indicate that the whole test samples are detected as normal and no mimicry bot sample is detected. However, the P2P botnet detection model trained using the RFS can detect the mimicry P2P bots with the TPR of 92.9% with a 6.5% decrease compared to the P2P bots.

Table 2: Detection Performance with Different Parameters for D1 dataset

W_f	W_c	$W_h = 900$			$W_h = 1200$			$W_h = 1500$			$W_h = 1800$		
		TPR	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**
20	120	0.997	0.002	363	**1.000**	**0.000**	**65**	1.000	0.000	75	1.000	0.000	87
	200	0998	0.002	303	0.999	0.000	61	1.000	0.000	81	**1.000**	**0.000**	**73**
	400	0.998	0.001	293	0.999	0.000	63	**0.999**	**0.000**	**45**	0.998	0.000	117
	600	0.996	0.002	407	0.998	0.001	243	0.999	0.001	91	**1.000**	**0.000**	**51**
40	120	0.998	0.002	299	0.998	0.001	153	**0.999**	**0.000**	**47**	0.998	0.000	181
	200	0.997	0.002	323	0.998	0.001	137	**0.999**	**0.000**	**47**	0.998	0.000	113
	400	0.997	0.002	317	0.998	0.001	179	**0.999**	**0.000**	**105**	0.999	0.001	81
	600	0.997	0.002	341	0.998	0.001	255	**0.999**	**0.000**	**103**	0.998	0.001	27
60	120	0.997	0.002	241	0.999	0.001	167	**0.999**	**0.000**	**133**	0.998	0.001	163
	200	0.997	0.002	239	0.998	0.001	149	**0.999**	**0.001**	**67**	0.998	0.001	181
	400	0.997	0.002	259	0.999	0.001	93	**0.999**	**0.000**	**33**	0.998	0.001	185
	600	0.997	0.003	351	0.998	0.001	185	0.999	0.000	37	**1.000**	**0.000**	**17**
80	120	0.998	0.002	165	**1.000**	**0.000**	**35**	1.000	0.000	51	0.998	0.000	67
	200	0.997	0.002	245	0.998	0.002	131	**1.000**	**0.000**	**47**	0.998	0.001	119
	400	0.998	0.002	173	**0.999**	**0.000**	**33**	0.999	0.000	43	0.998	0.001	19
	600	0.998	0.002	295	0.999	0.000	109	0.998	0.000	115	**1.000**	**0.000**	**21**

Table 3: Detection Performance with Different Parameters for D2 dataset

W_f	W_c	$W_h = 900$			$W_h = 1200$			$W_h = 1500$			$W_h = 1800$		
		TPR	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**	**TPR**	**FPR**	**TreeSize**
20	120	1.000	0.000	85	1.000	0.000	35	**1.000**	**0.000**	**15**	1.000	0.000	23
	200	1.000	0.000	35	1.000	0.000	49	**1.000**	**0.000**	**15**	1.000	0.000	23
	400	1.000	0.000	39	1.000	0.000	51	**1.000**	**0.000**	**15**	1.000	0.000	27
	600	0.999	0.002	265	1.000	0.000	59	1.000	0.000	31	**1.000**	**0.000**	**19**
40	120	0.999	0.003	171	1.000	0.000	87	**1.000**	**0.000**	**15**	1.000	0.000	19
	200	0.999	0.002	171	1.000	0.000	39	**1.000**	**0.000**	**15**	1.000	0.000	19
	400	0.996	0.006	541	1.000	0.000	47	**1.000**	**0.000**	**15**	1.000	0.000	23
	600	0.999	0.002	461	1.000	0.000	47	1.000	0.000	31	**1.000**	**0.000**	**23**
60	120	0.998	0.009	213	1.000	0.000	35	**1.000**	**0.000**	**19**	**1.000**	**0.000**	**19**
	200	0.999	0.003	225	1.000	0.000	43	**1.000**	**0.000**	**19**	1.000	0.000	23
	400	0.997	0.003	193	0.999	0.000	109	**1.000**	**0.000**	**19**	1.000	0.000	23
	600	0.997	0.008	741	1.000	0.000	43	**1.000**	**0.000**	**31**	**1.000**	**0.000**	**31**
80	120	0.999	0.003	199	1.000	0.000	77	1.000	0.002	73	**1.000**	**0.000**	**27**
	200	0.999	0.002	221	1.000	0.000	69	0.997	0.011	143	**1.000**	**0.000**	**27**
	400	0.997	0.004	101	1.000	0.000	59	**1.000**	**0.000**	**39**	0.998	0.001	105
	600	0.996	0.002	123	0.999	0.006	287	**1.000**	**0.000**	**47**	1.000	0.000	49

It can be concluded that the statistical feature set without using the features related to the packet length and timing characteristics of P2P bots is not only resilient to the mimicry attacks but also can achieve a high accuracy

Table 4: Detection Performance with Different Machine Learning Methods

Dataset	Method	TPR	FPR	F-Measure
D1	BN	98.3%	1.3%	98.3%
	J48	100%	0%	100%
	RF	100%	0%	100%
	SVM	93.2%	3.8%	94.1%
D2	BN	99.6%	1%	99.8%
	J48	100%	0%	100%
	RF	100%	0%	100%
	SVM	99.8%	3.4%	91.3%

Table 5: Comparison with other published P2P botnet detection approaches

P2P Botnet Detection Scheme	TPR	FPR
Garg *et al.* [9]	97.93%	0.38%
Saad *et al.* [18]	97.9%	5.1%
Zhao *et al.* [28]	98.1%	2.1%
Yu *et al.* [27]	100%	12.5%
Barthakur *et al.* [4]	99.7%	0.6%
Alauthman *et al.* [2]	99.20%	0.75%
Alauthman *et al.* [1]	99.10%	0.01%
Homayoun *et al.* [10]	91%	13%
Wang *et al.* [24]	98.3%	0.5%
Proposed Approach	100%	0%

to detect the P2P bots.

6 Conclusion

P2P botnets are one of the most serious threats to Internet security. Numerous studies have been done to eliminate P2P botnets. However, malware authors continuously utilize advanced technologies to harden the process of detection. Mimicry attack is one of these efforts in which the P2P bots are designed to mimic cyber behavior to fly under the radar and disguise their malicious actions. Therefore, designing a P2P botnet detection scheme resilient to mimicry attacks is of paramount importance.

Many P2P botnet detection proposals are based on the packet length and timing behavior of the network traffic of P2P bots. Nevertheless, these characteristics can be mimic by P2P bots to subvert these detection systems.

As a consequence, in this paper, we propose a statistical feature set without using the features related to the packet length and timing behavior of bots. The proposed feature set is extracted from the intrinsic characteristics of P2P bots, naming, long-lived flows, and the small set of contacts. These behaviors can not be modified without losing the functionality and efficiency of botnets.

To evaluate the resilience of the proposed feature set we implement a P2P botnet and a mimicry P2P botnet in a controlled environment in our lab. The evaluation experiments show that our proposed statistical feature set is not only resilient to the mimicry attack but also can detect P2P bots with high accuracy.

Table 6: Feature sets used in other published P2P botnet detection approaches

Number	Features	Reference
1	IOP-byte, APL, TBT, PPS, BPS, PL, IOP-frame, DUR, Fromframe, Toframe, Tobyte , Frombyte	[9]
2	IOP, APL, FPL, TPC, TBT, DPL, PL	[18]
3	FPL, APL, PV, TPC, PPS, TBP, NR	[28]
4	TPC, DUR, TBT, ABPP, BitPS, PPS	[27]
5	TPC, LSP, TBLSP, TBT, PLSP, VIT, APL, PV, RPD, RTD	[4]
6	TCPC, TCPR,TCPT, ATCPL, ARCPL, ACPL, TFC, TBT, RAOAC, ATBC	[2]
7	TCPC, TCPT, TCPR, TSYN, RSYN, TACK, RACK, TFC, TSYNACK, RSYNACK, TSYN-RSYNACK, TFINACK, RFINACK, TRST, RRST, TRSTACK, RRSTACK, SYN-ACKTime, SYN-RSTTime, SYNRST-ACKTime, DUR	[1]
8	DUR, TPC, Fromframe, Toframe, SIntPkt, SIntPktIdl, DIntPkt, DIntPktIdl, TBT, Tobyte, Frombyte, SIntPktAct, DIntPktAct, sMeanPktSz, dMeanPktSz, sMinPktSz, dMinPktSz, sMaxPktSz, dMaxPktSz, BitPS, SrcLoad, DstLoad, PPS, SrcLoad, DstLoad	[10]
9	DUR, TPC, NSP, AIT, TBT, APL, PV, FPL, DPL, LSP, MP, TBLSP, BPS, PPS, FPH	[24]

References

[1] M. Alauthman, N. Aslam, M. Al-Kasassbeh, S. Khan, A. Al-Qerem, and K.-K. R. Choo, "An efficient reinforcement learning-based botnet detection

Table 7: Description of statistical features used in published approaches

Feature Name	Description	Feature Name	Description
FPL	Length of the first packet in the flow	TPC	Total number of packets per flow
TBT	Total number of bytes per flow	APL	Average packet length per flow
IOP	Ratio of the number of incoming packets over the number of outgoing packets	DPL	Total number of subsets of packets of the same length over the total number of packets in the same flow
PV	Variance of payload packet length	DUR	Flow duration
PPS	Number of packets exchanged per second	BPS	Number of bytes exchanged per second
BitPS	Average bits-per-second for flow	Tobyte	Number of outgoing bytes
Frombyte	Number of incoming bytes	IOP-byte	Ratio of incoming over output bytes in the flow
IOP-frame	Ratio of incoming over outgoing number of frames in the flow	Fromframe	Number of Incoming frames in the flow
Toframe	Number of outgoing frames in the flow	LSP	Size of the packet carrying maximum bytes in a flow
TBLSP	Total bytes transferred with largest sized packets	PLSP	Portion of largest sized packet
VIT	Variance of inter-arrival time	RPD	Difference in number of packets between two responding flows
RTD	Difference in time of last packet received for two responding flows	ABPP	Average Byte-per packet
PL	Total number of bytes of all the packets over the total number of packets in the flow	TBP	Average time between packets
NR	Number of reconnects	TCPC	Number of control packets in the flow
TCPT	Number of transmitted control packets in the flow	TCPR	Number of received control packets in the flow
TSYN	Number of transmitted SYN packets in the flow	RSYN	Number of received SYN packets in the flow
TACK	Number of transmitted ACK packets in the flow	RACK	Number of received ACK packets in the flow
TFC	Number of transmitted failed connection in the flow	TSYNACK	Number of transmitted SYN-ACK packets in the flow
RSYNACK	Number of received SYN-ACK packets in the flow	TSYN-RSYNACK	Transmitted SYN-Received SYN-ACK
TFINACK	Number of transmitted FIN-ACK packets	RFINACK	Number of received FIN-ACK packets
TRST	Number of transmitted RST packets	RRST	Number of received RST packets
TRSTACK	Number of transmitted RST-ACK packets	RRSTACK	Number of received RST-ACK packets
SYN-ACKTime	Inter-arrival time between SYN and ACK	SYN-RSTTime	Inter-arrival time between SYN and RST
SYNRST-ACKTime	Inter-arrival time between SYN and RST-ACK	ATCPL	Average length of transmitted control packets in the flow
ARCPL	Average length of received control packets in the flow	ACPL	Average length of control packets in the flow
RAOAC	Ratio of average length of outgoing packets over the average length of control packets	ATBC	Average time between an attempt to create connection
SIntPkt	Source inter-packet arrival time	SIntPktIdl	Source idle inter-packet arrival time
DIntPkt	Destination inter-packet arrival time	DIntPktIdl	Destination idle inter-packet arrival time
SIntPktAct	Source active inter packet arrival time	DIntPktAct	Destination active inter packet arrival time
sMeanPktSz	Average of transmitting bytes	dMeanPktSz	Average of received bytes
sMinPktSz	Minimum transmitted packet size	dMinPktSz	Minimum received packet size
sMaxPktSz	Minimum transmitted packet size	dMaxPktSz	Minimum received packet size
SrcLoad	Transmitted bits per second	DstLoad	Received bits per second
SrcRate	Transmitted packets per second	DstRate	Received packets per second
NSP	Number of small packets	AIT	Average arrival time of packets
MP	The number of maximum packets	FPH	The number of C-flows per hour

Table 8: TPR and FPR of Resilience evaluation experiments

Feature set	TPR-P2P	FPR-P2P	TPR-mimicry	FPR-mimicry
1	95.4%	0.1%	0	0
2	98.5%	0%	0	0
3	98.7%	0%	0	0
4	95.4%	2.7%	0	0
5	96.5%	0.1%	0	0
6	97.5%	0.1%	-	-
7	97.1%	0.1%	-	-
8	92.3%	7.9%	0	0
9	98.3%	0.5%	0	0
RFS	99.4%	0%	92.9%	0

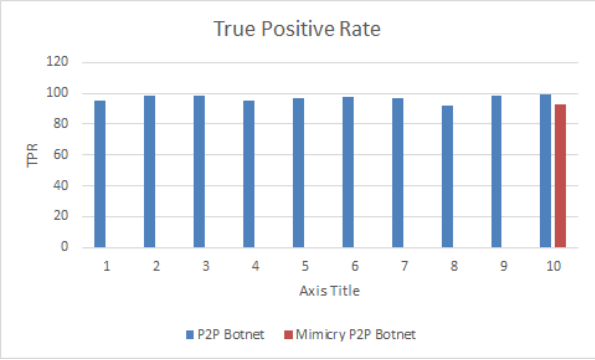


Figure 3: True Positive Rate of P2P botnet detection models for P2P and mimicry P2P botnets traces

approach," *Journal of Network and Computer Applications*, vol. 150, p. 102479, 2020.

[2] M. Alauthaman, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "A p2p botnet detection scheme based on decision tree and adaptive multilayer neural networks," *Neural Computing and Applications*, vol. 29, no. 11, pp. 991–1004, 2018.

[3] S. T. Ali, P. McCorry, P. H. J. Lee, and F. Hao, "Zombiecoin 2.0: managing next-generation botnets using bitcoin," *International Journal of Information Security*, vol. 17, no. 4, pp. 411–422, 2018.

[4] P. Barthakur, M. Dahal, and M. K. Ghose, "Adoption of a fuzzy based classification model for p2p botnet detection." *IJ Network Security*, vol. 17, no. 5, pp. 522–534, 2015.

[5] F. F. Daneshgar and M. Abbaspour, "On the resilience of p2p botnet footprints in the presence of legitimate p2p traffic," *International Journal of Communication Systems*, vol. 32, no. 13, p. e3973, 2019.

[6] E. Frank, M. A. Hall, and I. Witten, "The weka workbench. online appendix," *Data mining: practical machine learning tools and techniques*, 2016.

[7] M. S. Gadelrab, M. ElSheikh, M. A. Ghoneim, and M. Rashwan, "Botcap: Machine learning approach for botnet detection based on statistical features," *International Journal of Communitation Networks and Information Security*, vol. 10, no. 3, p. 563, 2018.

[8] J. Gardiner and S. Nagaraja, "On the security of machine learning in malware c&c detection: A survey," *ACM Computing Surveys*, vol. 49, no. 3, pp. 1–39, 2016.

[9] S. Garg, A. K. Sarje, and S. K. Peddoju, "Improved detection of p2p botnets through network behavior analysis," in *International Conference on Security in Computer Networks and Distributed Systems*. Springer, 2014, pp. 334–345.

[10] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "Botshark: A deep learning approach for botnet traffic detection," in *Cyber Threat Intelligence*. Springer, 2018, pp. 137–153.

[11] J. Howard, "Pythonp2pbotnet," Tech. Rep. https://github.com/jhoward321/PythonP2PBotnet, April 2018.

[12] R. U. Khan, R. Kumar, M. Alazab, and X. Zhang, "A hybrid technique to detect botnets, based on p2p traffic similarity," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 136–142.

[13] M. Knysz, X. Hu, K. G. Shin, and M. S. Hwang, "Good guys vs. bot guise: Mimicry attacks against fast-flux detection systems," in *Proceedings of IEEE INFOCOM*, April 2011, pp. 1844–1852.

[14] W. H. Liao and C. C. Chang, "Peer to peer botnet detection using data mining scheme," in *2010 International Conference on Internet Technology and Applications*. IEEE, 2010, pp. 1–4.

[15] W. Y. Loh, "Classification and regression trees," *Wiley interdisciplinary reviews: data mining and knowledge discovery*, vol. 1, no. 1, pp. 14–23, 2011.

[16] V. Matta, M. D. Mauro, P. H. J. Lee, and M. Longo, "Ddos attacks with randomized traffic innovation: Botnet identification challenges and strategies," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1844–1859, 2017.

[17] B. Rahbarinia, R. Perdisci, A. Lanzi, and K. Li, "Peerrush: Mining for unwanted p2p traffic," in *International conference on detection of intrusions and malware, and vulnerability assessment*. Springer, 2013, pp. 62–82.

[18] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, J. Felix, and P. Hakimian, "Detecting p2p botnets through network behavior analysis and machine learning," in *2011 Ninth annual international conference on privacy, security and trust*. IEEE, 2011, pp. 174–180.

[19] SECTOR, "Building botnets on the blockchain," Tech. Rep., Nov. 2017. (https://sector.ca/building-botnets-on-the-blockchain/)
[20] P. Shankdhar, "15 best free packet crafting tool," Mar. 4, 2018. (https://resources.infosecinstitute.com/15-best-free-packet-crafting-tools)
[21] 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, no. 3, pp. 357–374, 2012.
[22] E. Stinson and J. C. Mitchell, "Towards systematic evaluation of the evadability of bot/botnet detection methods," *WOOT*, vol. 8, pp. 1–9, 2008.
[23] Y. H. Su, A. Rezapour, and W. G. Tzeng, "The forward-backward string: A new robust feature for botnet detection," in *2017 IEEE Conference on Dependable and Secure Computing*. IEEE, 2017, pp. 485–492.
[24] W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, "Botmark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors," *Information Sciences*, vol. 511, pp. 284–296, 2020.
[25] Z. Wang, M. Qin, M. Chen, C. Jia, and Y. Ma, "A learning evasive email-based p2p-like botnet," *China Communications*, vol. 15, no. 2, pp. 15–24, 2018.
[26] S. Yu, S. Guo, I. Chen, and I. Stojmenovic, "Fool me if you can: Mimicking attacks and anti-attacks in cyberspace," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 139–151, 2013.
[27] X. Yu, X. Dong, G. Yu, Y. Qin, D. Yue, and Y. Zhao, "Online botnet detection based on incremental discrete fourier transform," *Journal of Networks*, vol. 5, no. 5, p. 568, 2010.
[28] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, A. Ghorbani, and D. Garant, "Botnet detection based on traffic behavior analysis and flow intervals," *computers & security*, vol. 39, pp. 2–16, 2013.

Biography

Fateme Faraji Daneshgar received her bachelor's degree in software engineering from Tarbiat Moallem University in Tehran in 2004. Immediately after graduation, she was accepted for a master's degree in software engineering at Tarbiat Modares University. Having completed his master's degree in 2007, she worked for about 2 years as a research associate at Bank Mellat Research Center and the National Library of Iran. He also worked as a software designer on some IT projects for 3 years before starting his Ph.D. Program at Shahid Beheshti University, Iran in 2012. She graduated in 2021 with a doctorate. Her main research interest is "network security" and "data mining" and "machine learning".

Atiyeh MohammadKhani received her B.S degree in Software Engineering from Dr. Shariati Technical and Vocational College of Tehran, Iran in 2013. She finished her Master in Information Technology Engineering from Shahid Beheshti University, Tehran, Iran in 2019. Her main research interests are network security, data mining, malware detection, social network analysis and IoT security.

Maghsoud Abbaspour received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of Tehran, Tehran, Iran, in 1992, 1995 and 2003, respectively. He is an associate professor of Faculty of Computer Science and Engineering and director of Computer Networking and Network Security Laboratory in Shahid Beheshti University, Tehran, Iran since 2005. He is interested in Wireless Sensor Networks, peer to peer and ad hoc networks, network security and Internet of Things.

Stable Transmission Algorithm for 5G Wireless Sensor Networks Based on Energy Equalization-delay Reduction Mechanism

Bo Wu

(Corresponding author: Bo Wu)

College of Information Engineering, Zhengzhou University of Industrial Technology
Zhengzhou 450000, China
Email:publicgj@163.com

(Received Mar. 21, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 24, 2022)

Abstract

Wireless sensor network (WSN) is mainly through the distribution of cheap nodes in a specific range of monitoring areas, self-organization, and other ways to build a data acquisition-transmission-processing network. The node collects the data information in the covered area by a cycling mechanism. The relay link node transmits the data information to the sink node to realize data. When a node fails to send, or the winner receives data, it must adopt a retransmission mechanism. If the jitter of the transmission link occurs at this time, the node must carry out frequent data re-transmission to ensure that the data can be completely transmitted to the sink node. The re-transmission mechanism will result in data congestion, generating more serious node energy limitations and transmission bandwidth limitations. To solve congestion control problems and cluster head node limitation in the 5G wireless sensor network, a stable transmission algorithm for wireless sensor networks based on an energy equalization-delay reduction mechanism is proposed. The channel state control index is designed, and a data transmission model is proposed to evaluate the stability of the data transmission process. A cluster head updating method based on energy equalization and delay reduction mechanism is constructed to enhance the probability of high-energy nodes being selected as cluster head nodes. The simulation results show that the proposed algorithm has higher network transmission bandwidth, lower average network delay, and lower network throughput frequency than the current wireless sensor network transmission algorithms.

Keywords: 5G Wireless Sensor Network; Cluster Head Updating Method; Energy Equalization-Delay Reduction Mechanism; Stable Transmission Algorithm

1 Introduction

Under the background of 5G, current researchers try to improve the stability of data transmission in wireless sensor networks by improving link layer, network layer, network management and other aspects [14–16]. For example, Zbigniew [6] based on the reasonable allocation of the remaining energy of cluster head nodes, adopted the unified management of sink node to conduct inter-region energy balanced scheduling, and used the optimal energy polling mechanism of nodes in the cluster to realize the stability of regional topology structure and the rapid convergence of regional re-formation process. However, the scheme did not fully consider the distance and node density factors, so that the duration of regional stable transmission was short, and it was difficult to adapt to the practical application scenarios of 5G UWB transmission. Shan *et al.* [4] proposed a regional stable transmission scheme based on the disequilibrium clustering mechanism. By adopting the disequilibrium clustering method, the nodes with higher energy were deployed in the hot region, and the nodes were updated by the polling method, thus improving the stability performance of regional transmission. However, the proposed algorithm took little consideration of data delay, which made the algorithm prone to serious data congestion in the 5G UWB deployment environment, and reduced the transmission stability of the algorithm. Yin *et al.* [12] inserted mobile high-energy nodes into the region and replace cluster head nodes with low energy in real time by trajectory routing, which effectively satisfied the problem of high energy consumption of cluster head nodes under the 5G UWB transmission condition and significantly improved the quality of network data transmission. However, the algorithm had low adaptability to node movement and was difficult to be deployed in the actual scene with high node movement speed.

In order to improve the network transmission perfor-

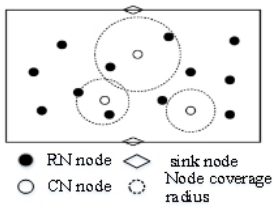


Figure 1: Network deployment

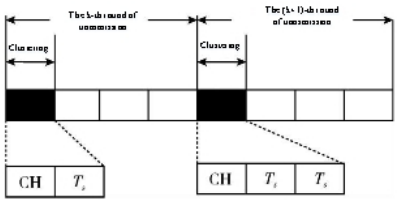


Figure 2: Cluster head node replacement and data update

mance and improve the node limitation, a stable transmission algorithm based on energy equalization-delay reduction mechanism is proposed. Firstly, a data transmission model is designed based on data segment transmission and channel slot distribution to adapt to the high flow characteristics of wireless sensor network topology under 5G conditions. The preset mode is adopted to deploy high-energy nodes, optimize the selection process of cluster head nodes, and achieve the purpose of suppressing the limitation of cluster head nodes. Combined with the sleep mode, the efficiency of data packet transmission is further improved. Then, feedback is used to improve the communication confirmation efficiency between the sink node and the cluster head node, so as to optimize the quality of region segmentation and realize the stable transmission of data. Finally, the performance of the proposed algorithm is verified by simulation experiments.

2 Proposed Network Model

2.1 Network Deployment Model

Typical deployment scenarios of wireless sensor networks under 5G conditions are shown in Figure 1. 5G wireless sensor nodes are deployed in a random distribution mode in the rectangular region. Nodes are divided into regional nodes (RN) and cluster nodes (CN). Both RN node and CN node are in a wandering state, but within the data transmission cycle, RN node and CN node will be within the same node coverage radius. As master control nodes (MCN), the sink node controls the status of RN nodes and CN nodes through the frequency-invariable control channel, records and updates the geographical coordinates of RN nodes in real time.

Cluster head nodes need to be replaced before the start of the next transmission cycle. During the replacement process, the network topology and node coverage will be optimized. After the completion of the replacement process, data will be transmitted in a stable way, as shown in Figure 2. After the selection is completed, the cluster head node will broadcast data to the node within its own coverage radius. After receiving the data message, the regional node will give feedback to the cluster head node nearest to it and update its geographical coordinate position. After receiving the data packets fed back by the regional nodes, the cluster head node will fuse all the data packets within the transmission cycle and send them to the sink node through a specific frequency channel. In the process of region formation, both the original RN node and CN node have a chance to be selected as cluster head nodes in the new round of selection. In general, the node with the highest energy should be selected as the new CN node. In this paper, the random number method is adopted to determine the CN node, and only when the random number of a node is higher than the threshold value $W(s)$, it can be selected as a cluster head node. $W(s)$ is obtained as follows:

$$W(s) = \frac{1 - k(r \mod(1/k))}{k}. \quad (1)$$

Where k represents the probability of the current node being removed from the CN node, and r represents the number of data transmission times. If the random number of a node is higher than the threshold $W(s)$, it will be selected as the cluster head node (CH) in the current round, and the threshold $W(s)$ will be set to 0. Cluster head node selection will continue to operate on the remaining nodes in the next transmission cycle.

2.2 Data Transmission Model

As can be seen from Section 2.1, network energy consumption can be reduced to some extent through cluster head node replacement and data update, and the stable cycle in the process of data transmission can be improved. However, as can be seen from the process of node replacement, repeated data feedback is required for node replacement, and the probability of data delay phenomenon will be significantly increased when network fluctuations occur [13]. In the actual application, due to the random distribution characteristics of cluster head election process [10], each node has a certain probability to become a new cluster head node in the data transmission process. In addition, wireless sensor network nodes in 5G environment also have high density characteristics [7]. With the continuous increase of network size, the energy balance performance must be fully considered to improve the network quality and prevent serious fluctuations in data transmission.

Considering that the RN node is generally in a dormant state, the data transmission process is started when the transmission channel is in an idle state [3], as shown in Figure 3. After the data transmission process is started,

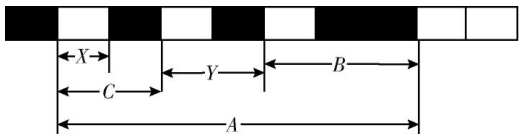


Figure 3: Data transmission

the length of the idle channel is , and the transmission period is T. In the data transmission process, three situations will occur: the cluster head node successfully receives the transmitted data, denoted as A; The network is congested and the data packet transmission is blocked, denoted as B; The channel is idle, it is ready for data transmission, denoted as C. According to the working state of the transmission channel, the channel state can be set to two states, X and Y: 1) X represents the successful data transmission of the channel (denoted as K) and data congestion (denoted by M). Obviously, the X and Y states will alternate occur throughout the working week.

Suppose that in the whole working week, the occurrence number of X and Y are m and n respectively. The total number of nodes in the network is H, and the probability that network nodes are in hibernation state is P_i. The data packet reachable probability is P, which can be obtained by the following equation,

$$P = (1 - P_1) + \cdots + (1 - P_H) = \sum_{i=1}^{H}(1 - P_i). \tag{2}$$

The probability $P(X, Y)$ of the simultaneity occurrence of the two states X and Y within the transmission week can be obtained as follows:

$$P(X, Y) = (1 - e^{-xP})^m (e^{-xP})^n. \tag{3}$$

Where x represents the length of idle channel, and P represents the data packet reachable probability. The occurrence frequency $E(X)$ in the whole working week satisfies:

$$E(X) = 1/e^{-xP}. \tag{4}$$

According to Equation (4), the average time $T(X)$ of a node in the idle state satisfies:

$$T(X) = xE(x) = x/e^{-xP}. \tag{5}$$

The occurrence frequency of $E(Y)$ in the whole working week satisfies:

$$E(Y) = 1/(1 - e^{-xP}). \tag{6}$$

Therefore, it can be seen that the average duration $T(Y)$ of a node in a busy state satisfies:

$$T(Y) = (T_s - x)E(Y) = \frac{T_s - x}{e^{-xP}}. \tag{7}$$

Where, T_s represents the data transmission cycle.

Considering that in the process of data transmission, when A happens with k times, then B occurs with $(m-k)$ times, so the probability $E(k)$ that the network successfully sends the data packet satisfies:

$$E(K) = \sum_{i=1}^{m}\sum_{j=1}^{i} C_i^k e^{-xP}(1 - xPe^{-xP})^k. \tag{8}$$

Therefore, the data length $L[E(K)]$ in the process of the event K execution satisfies:

$$L[E(K)] = \frac{x(1-x)P}{1 - xPe^{-xP}}. \tag{9}$$

According to Equations (7), (8), and (9), the probability T of network node successfully sending data message satisfies:

$$T = \frac{x(1-x)Pe^{-xP}}{1 + x - xPe^{-xP}}. \tag{10}$$

3 The Proposed Regional Stable Transmission Algorithm for WSN

As can be seen from the mentioned above network model, network nodes may encounter a variety of events during data transmission. The occurrence of each event has a certain probability, and the probability that the network node can transmit data stably satisfies Equation (10). In the process of data transmission, it is necessary to fully consider the phenomenon of energy limitation and data delay existed in nodes, so that data transmission can be carried out with a high transmission success rate [17]. Therefore, a delay reduction mechanism based on energy balance is designed in this paper, the data can be transmitted stably on the basis of energy balance. The scheme consists of two parts: cluster head updating method based on energy equalization-delay reduction mechanism and region division method based on stable transmission mechanism. The following is detailed introduced them.

3.1 Cluster Head Renewal Based on Energy Equalization-delay Reduction Mechanism

Due to the frequent data forwarding of cluster head nodes in the process of data transmission, and the frequent channel competition in the process of data transmission, serious energy loss will occur. In order to improve the life cycle of network nodes, all network nodes are divided into high energy nodes (HEN) and general nodes (GN) [11]. Wherein, the initial energy of HEN node and GN node can be expanded according to a certain proportional coefficient, and the expansion coefficient can be set as 1. The probability of HEN node being selected as cluster head node is significantly higher than that of GN node, so as

to ensure the stable performance of cluster head node and regional topology.

Let the weight of HEN and GN to be selected be P_{HEN} and P_{GN}.

$$P_{HEN} = \frac{\mu\omega}{1+\mu\omega+P}. \quad (11)$$

$$P_{GN} = \frac{(1+\mu)\omega}{(1+\mu)\mu\omega+P}. \quad (12)$$

Where ω represents the proportionality coefficient between HEN node and GN node. Since the general expansion coefficient can be set as 10 20, P_{HEN} will be higher than P_{GN}.

Suppose that the energy consumption value of the m-th node in the network is $E(i)$, and the initial energy of the network node is E. The total number of nodes currently in hibernation state is N, and the total number of nodes in the network is L, then the average energy residual $E(last)$ of the network nodes satisfies:

$$E(last) = \frac{\sum_{i=1}^{N} E - E(i)}{L-N}. \quad (13)$$

With Equations (1), (11), (12), and (13), the update thresholds T_{HEN}, T_{GN} of HEN node and GN node are set as:

$$T_{HEN} = \frac{1-(1-P_{HEN})(rmod[1/(1-P_{HEN})]}{1-P_{HEN}} \quad (14)$$

$$T_{GN} = \frac{1-(1-P_{GN})(rmod[1/(1-P_{GN})]}{1-P_{GN}} \quad (15)$$

Where T_{HEN}, T_{GN} denote the update thresholds of HEN node and GN node, respectively. r is the number of data transmission.

As the network transmits data, when the energy of HEN node and GN node trigger the update threshold as shown in Equations (14) and (15) respectively, the network will set the corresponding HEN node and GN node as sleep state, and contact the sink node for energy supplement. In this way, the nodes that reduce excessive energy consumption are selected as cluster head nodes, and node replacement can be carried out in time, which can effectively improve the network life cycle. In addition, due to differentiation factors between HEN node and GN node, HEN node has a higher probability of being selected as cluster head node, thus reducing the probability of network transmission interruption caused by node energy limitation.

3.2 Region Partitioning Based on Stable Transmission Mechanism

The cluster head updating method based on energy equalization-delay reduction mechanism can select the nodes with the best energy with a high probability for data transmission. According to Equation (10), HEN node can be selected as cluster head node to effectively improve the sending efficiency of data packets. However, due to the high mobile speed of each node under the 5G network condition, this paper builds a regional division method based on the stable transmission mechanism to realize the stable transmission of data. The details are as follows:

Step 1. Region partitioning stage. The sink node broadcasts the nodes that trigger model (14) and model (15) in the network. If the corresponding HEN node and GN node can meet the transmission requirements in the transmission cycle, the information will be fed back to the sink node and the remaining energy in the node will be updated.

Step 2. The sink node obtains the average residual energy of network nodes according to model (13), and sets the nodes in the network whose energy surplus is lower than the residual energy of the bottleneck as dormant state, as shown in Figure 4.

Step 3. According to model (11) and model (12), HEN node and GN node are initialized and assigned. If HEN node and GN node satisfy model (14) and model (15) respectively, they will be selected as cluster head nodes.

Step 4. After the cluster head node is elected, the data will be broadcast. After each regional node receives the data broadcast, the cluster-head node with the strongest energy is taken as the subordinate node and incorporated into the control region of the cluster-head node.

Step 5. Network nodes execute data transmission until the accuracy rate triggered by the corresponding cluster head nodes is lower than 50% in accordance with model (14). The selection process of cluster head nodes is re-conducted. So this round of transmission is ended. After the region segmentation is completed, cluster head nodes start to enter the data transmission state, and each regional node aggregates its own data to cluster head nodes and transmits it to the sink node through cluster head nodes. When regional nodes complete data collection and aggregation, each cluster head node will enter a dormant state. At this time, the accuracy rate of cluster head nodes will decline sharply. Therefore, the region segmentation process will need to be re-conducted, and Step 1 will be started to perform region partition.

4 Experiments and Analysis

In order to compare the performance, NS2 simulation experiment environment is adopted [9]. The network deployment environment is as follows: the node distribution area is a rectangle, and both the sending node and the receiving node of the network are located at the edge of the

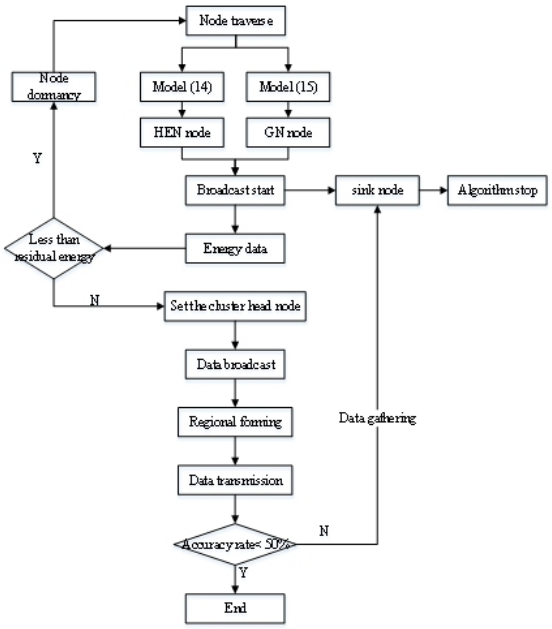


Figure 4: Region partitioning method based on stable transmission mechanism

Table 1: Comparison parameter

Parameter	Value
Network node density	Not less than 10 units(100 square meters)
Energy expansion coefficient μ of high energy nodes	Not less than 5
Node layout	Random distribution
Channel noise	Standard white Gaussian noise
Initial energy of the node	10J
Data packet packet probability	0.5
Node minimum transmission bandwidth	Not less than 1 Mbps

rectangular area with a random walk state. The node signal uses 5G signal [1]. The signal pre-emission molding technology as shown in the literature [2] is adopted. In the signal molding process, the spectrum sharpening and clearing mechanism based on the zero mode mentioned in the literature is utilized.

The network sending nodes are independent of each other, and the relevant data packet also satisfies the Poisson distribution. The remaining parameter settings are shown in Table 1. In addition, we select two newest control mechanisms in 5G sensing technology: optimized transmission algorithm of 5Gsignal bandwidth based on cross layer coding plus multiple-xing mechanism (OT-CLCPM) [8] and data transmission algorithm of mobile wireless sensor network based on power loss equalization control mechanism (DT-PLEC) [5] to make comparison. The comparison parameters select network transmission bandwidth, network average delay and network throughput frequency as shown in Table 1.

After the start of the simulation experiment, the network transmission bandwidth, network average delay and network throughput frequency at the end of the transmission cycle are recorded round by round according to the number of data transmission rounds. Considering the moving characteristics of 5G nodes, moving speeds 5m/s and 50m/s are taken as experimental control parameters to test the performance of network parameters under low/high mobile conditions.

4.1 Network Transmission Bandwidth

Table 2 shows the network transmission bandwidth tested with node moving speeds of 5 m/s and 50 m/s as experimental environment control parameters. As can be seen from Table 2, the network transmission bandwidth of the proposed algorithm is higher than that of the OT-CLCPM algorithm and the DT-PLEC algorithm. Because the proposed algorithm fully considers the network energy consumption and time delay in the process of data transmission. The cluster-head updating method based on energy equalization and delay reduction mechanism is designed to promote the stable updating of cluster-head nodes, and reduce the transmission congestion caused by the limited cluster-head nodes, so it has a high network transmission bandwidth. OT-CLCPM algorithm mainly adopts a crosstalk elimination scheme based on cross-layer coding channel interactive multiplexing mechanism. By reducing the crosstalk phenomenon caused by channel noise in the transmission process, the transmission efficiency of nodes can be increased. However, this algorithm does not suppress the transmission paralysis of cluster head nodes due to energy limitation. Therefore, the cluster head node has a high probability of limitation, which reduces the performance of network transmission bandwidth.

DT-PLEC algorithm constructs the goal sink-regional child node control packet transmission mechanism, the regional node threshold flow control mechanism and the limited bandwidth secondary confirmation mechanism to make regional transmission stable. However, since the algorithm mainly controls the data flow, it does not carry out targeted region segmentation for the energy limitation of cluster head nodes. Therefore, the failure of cluster head nodes is easy to cause data transmission paralysis in a large area, so the network transmission bandwidth is also lower than that of the proposed algorithm.

4.2 Mean Delay of Network

Table 3 shows the mean delay of network tested with node moving speeds of 5 m/s and 50 m/s as experimental en-

Table 2: Network transmission bandwidth test results

Node moving speeds=5m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	3385/Mbps	3400/Mbps	3482/Mbps
150	3000/Mbps	3100/Mbps	3396/Mbps
250	2000/Mbps	1950/Mbps	2500/Mbps
350	1200/Mbps	1100/Mbps	1800/Mbps
450	1150/Mbps	1050/Mbps	1500/Mbps
550	1120/Mbps	1020/Mbps	1500/Mbps
Node moving speeds=50m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	1250/Mbps	1250/Mbps	1350/Mbps
150	1000/Mbps	900/Mbps	1300/Mbps
250	1050/Mbps	870/Mbps	1200/Mbps
350	800/Mbps	600/Mbps	800/Mbps
450	600/Mbps	450/Mbps	700/Mbps
550	500/Mbps	400/Mbps	700/Mbps

vironment control parameters. As can be seen from the Table 3, the network average delay of the proposed algorithm is significantly lower than that of the OT-CLCPM algorithm and the DT-PLEC algorithm. Because the proposed algorithm fully considers the node energy limitation and data delay phenomenon, it introduces the dormancy mechanism of cluster nodes to reduce the energy consumption, reduces the number of data packet retransmission, improves and upgrades the network congestion control capabilities, so the network average delay is low. OT-CLCPM algorithm optimizes signal preforming and weakens the channel noise method to improve the network transmission capacity. However, because OT-CLCPM does not considers the way of optimizing the cluster nodes update to improve the network congestion control ability. Due to the failure of cluster head nodes, the network delay is likely to increase, so the network average delay performance of this algorithm is lower than that of the proposed algorithm. DT-PLEC algorithm constructs the goal sink-regional child node control packet transmission mechanism, the regional node threshold flow control mechanism and the limited bandwidth secondary data confirm system to optimize the regional transmission quality. However, because this algorithm also does not consider energy constrained factors of cluster nodes, only considers traffic overload on the impact of network average delay, so in the network bottleneck delay, the performance of the algorithm is also lower than the proposed algorithm in this paper.

4.3 Network Throughput Frequency

Table 4 shows the network throughput frequency tested with node moving speeds of 5 m/s and 50 m/s as experimental environment control parameters. As can be seen from the table, the network throughput frequency of the proposed algorithm is significantly lower than that of OT-CLCPM algorithm and DT-PLEC algorithm, which shows superior network throughput performance. Because the proposed algorithm in this paper takes the energy and region division into account, and combines the differentiation characteristics of HEN node and GN node, improves the probability of HEN node being selected as cluster head node and improves the data throughput performance of transmission node. Therefore, the probability of network jitter is low, which reflects the low network throughput frequency. OT-CLCPM algorithm only uses optimized signal preforming to improve the performance of the network, it does not improve the network jitter phenomenon of cluster nodes. Therefore, more data packets need to be re-transmitted, which reflects higher network throughput frequency. DT - PLEC algorithm optimizes the performance of data transmission mainly through flow control method to design goal sink-regional child node control packet transmission mechanism, the node threshold flow control mechanism and limited bandwidth node secondary qualification. Although the network throughput capacity is enhanced to a certain extent, the algorithm does not further stabilize the data transmission quality between regions by optimizing cluster head node update, so the network throughput performance is also lower than the proposed algorithm in this paper.

5 Conclusions

In order to solve the regional stable transmission problem of wireless sensor networks in 5G deployment environment, a regional stable transmission scheme based on energy equalization-delay reduction mechanism is proposed. Firstly, the network deployment model and data transmission model are analyzed, and the data transmission can be stabilized by energy balance and delay reduc-

Table 3: Network mean delay test results

Node moving speeds=5m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	80/ms	70/ms	60/ms
150	83/ms	75/ms	55/ms
250	135/ms	140/ms	60/ms
350	150/ms	180/ms	100/ms
450	160/ms	190/ms	120/ms
550	190/ms	220/ms	130/ms
Node moving speeds=50m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	120/ms	110/ms	90/ms
150	125/ms	120/ms	100/ms
250	160/ms	180/ms	110/ms
350	240/ms	320/ms	120/ms
450	320/ms	500/ms	200/ms
550	380/ms	530/ms	250/ms

Table 4: Network throughput frequency test results

Node moving speeds=5m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	100	105	50
150	400	500	290
250	800	1200	600
350	1000	1300	900
450	1100	1350	950
550	1300	1500	1000
Node moving speeds=50m/s			
Number of data transmission rounds	OT-CLCPM	DT-PLEC	Proposed
50	600	700	300
150	800	1500	600
250	1500	2400	1400
350	2500	3000	2000
450	2600	3200	2200
550	2800	3500	2500

tion. The cluster head update method based on energy equalization-delay reduction mechanism and the region partition method based on stability transmission mechanism are designed to improve the adaptability of the proposed algorithm to ultra-wideband and high jitter existing in 5G environment, it significantly improves the network congestion control ability, and has better network adaptation performance. In the next work, the proposed algorithm will adopt the node topology optimization mechanism to enhance the network congestion control performance and UWB data transmission ability of the proposed algorithm under the condition of low-density topology, and further improve the deployment value of the proposed algorithm in complex environments, in view of the difficulty in realizing low-density node deployment.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] H. Ansar, M. S. Noor, "Bandwidth utilization efficiency enhancement for OFDM-based WSN," *International Journal of Communication Systems*, vol. 31, no. 15, e3776, 2018.

[2] H. Chen, D. Pei, L. Shuai, "Bandwidth optimization transmission algorithm for 5G signals based on cross-layer coded additive multiplexing mechanism," *Journal of Electronic Measurement and Instrumentation*, vol. 32, no. 7, pp. 157-164, 2018.

[3] J. Du, S. Wang, B. Zhang, "Vehicle density and signal to noise ratio based broadcast backoff algorithm for VANETs," *Ad Hoc Networks*, vol. 99:102071, 2019.

[4] S. Jin, Y. Wang, Y. Sun, "Design and implementation of wireless multimedia sensor network node based on FPGA and binocular vision," *Eurasip Journal on Wireless Communications & Networking*, vol. 2018, no. 1, pp. 163-, 2018.

[5] L. J. Li, F. Q. Zhang, H. F. Liu, "Data transmission algorithm for mobile wireless sensor network based on power loss equalization control mechanism," *Telecommunications Science*, vol. 34, no. 11, pp. 1-9, 2018.

[6] Z. Lipiski, "Routing algorithm for maximizing lifetime of wireless sensor network for broadcast transmission," *Wireless Personal Communications*, pp. 251-268, 2018.

[7] K. C. Lu, C. H. Loh, Y. S. Yang, J. P. Lynch, K. H. Law, "Real-time structural damage detection using wireless sensing and monitoring system," *Smart Structures & Systems*, vol. 4, no. 6, pp. 759-777, 2008.

[8] K. Patil, K. D. Turck, D. Fiems, "A two-queue model for optimising the value of information in energy-harvesting sensor networks," *Performance evaluation*, vol. 119, pp. 27-42, 2018.

[9] S. Sivasakthiselvan, V. Nagarajan, "A new localization technique for node positioning in wireless sensor networks," *Cluster Computing*, vol. 22, no. 1, pp. 4027-4034, 2019.

[10] S. Su, S. Zhao, "An optimal clustering mechanism based on Fuzzy-C means for wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 18, 2017.

[11] Y. Sun, S. L. Yin, H. Li, L. Teng, S. Karim, "GPOGC: Gaussian pigeon-oriented graph clustering algorithm for social networks cluster," *IEEE Access*, vol. 7, pp. 99254-99262, 2019.

[12] Y. Q. Tang, F. Du, X. M. Fang, "Deadband scheduling in sensor node and controller node for wireless networked control systems," *International Journal of Wireless Information Networks*, vol. 25, pp. 241-249, 2018.

[13] X. W. Wang, S. L. Yin, H. Li, "A network intrusion detection method based on deep multi-scale convolutional neural network," *International Journal of Wireless Information Networks*. vol. 27, no. 4, pp. 503-517, 2020.

[14] X. W. Wang, S. L. Yin, M. Shafiq, A. A. Laghari, S. Karim, O. Cheikhrouhou, W. Alhakami, H. Hamam, "A new V-Net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption," *Security and Communication Networks*, vol. 2022, pp. 1-14, 2022.

[15] S. L. Yin, H. Li, S. Karim, Yang Sun, "ECID: Elliptic curve identity-based blind signature scheme," *International Journal of Network Security*, vol. 23, no. 1, pp. 9-13, 2021.

[16] S. L. Yin, H. Li, L. Teng, "A novel proxy re-encryption scheme based on identity property and stateless broadcast encryption under cloud environment," *International Journal of Network Security*, vol. 21, no. 5, pp. 797-803, 2019.

[17] L. H. Zhang, H. L. Ye, D. W. Zhang, J. Chen, "Study on image transmission mechanism of ghost imaging based on joint source and channel coding," *Applied Physics B*, vol. 125, no. 4, 2019.

Biography

Bo Wu biography. Bo Wu was born in 1983.09 in Zhengzhou City. His main interests include data mining, data security, information processing.

A Lightweight NFC Authentication Algorithm Based on Modified Hash Function

Fang-Ming Cao[1] and Dao-Wei Liu[2]
(Corresponding author: Fang-Ming Cao)
School of Data and Computer Science, Guangdong Peizheng College[1]
Guangzhou 510800, China[1]
Email: caofangming1983@163.com
Department of Computer Science and Engineering, Guangzhou College of Technology and Business[2]
(Received Apr. 5, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 24, 2022)

Abstract

In the NFC application, the leakage of user privacy information is inevitable. A lightweight NFC authentication algorithm based on a modified hash function is proposed to ensure the security of user privacy information. In the proposed algorithm, the specific implementation process using the modified hash function is given, which can provide better security requirements. In implementing the modified hash function, the Hamming weight variable of the encryption parameter itself is skillfully used, which reduces the introduction of parameters and improves the security factor of the encryption function. From the perspective of formalization and security analysis, it can be shown that the proposed algorithm satisfies the security needs of users. Furthermore, the simulation result demonstrates that the cost of the proposed algorithm is better than other NFC algorithms.

Keywords: Hamming Weight; Lightweight; Authentication Algorithm; Modified Hash Function; Near Field Communication (NFC); Privacy Leakage

1 Introduction

Near field communication (NFC) is a kind typical short-distance communication technology that can read out the information stored in objects without contacting themself [14]. The NFC technology is evolved from RFID technology, due to the low cost of the electronic tag in the RFID system, the computing power of the electronic tag is seriously restricted, it is unable to carry out the encryption and decryption calculation based on the traditional cryptography algorithm, resulting in the leakage of user privacy information [16, 17]. In order to improve the computing power of electronic tags and ensure the security of users' privacy information, therefore, the NFC technology is produced.

In general, the communication principle of NFC technology is roughly the same as that of RFID technology. The main difference [7,9] is that the user device stored information in NFC system is no longer a simple electronic tag device, but a mobile device with powerful computing power, such as mobile phone. The mobile phones have strong computing power and data storage capacity, and can carry out encryption and decryption calculation based on traditional cryptography algorithm, which can better protect the security of user privacy information. So, mobile phones can not only replace the traditional RFID electronic tags, but also bring great convenience to users. For example, users can generate electronic tag records, such as bus cards and bank cards on mobile phones, which can reduce the amount of things users bring when they go out [4, 8, 13].

This paper is organized as follows: In Section 1, we introduce the background of NFC technology. And then, we review the related work in Section 2. In Section 3, a lightweight NFC authentication algorithm based on modified hash function is proposed. In Section 4, the security analysis of NFC authentication algorithm is given. In Section 5, we analyzed the performance of NFC authentication algorithm. In Section 6, from the formal point of view, the NFC algorithm based on GNY logic formal reasoning is analyzed. In Section 7, simulation experiment is carried out from the perspective of energy consumption in the communication process. Lastly, we conclude the whole paper in Section 8.

2 Related Works

At present, NFC security research has attracted more and more attention. According to the analysis of NFC algorithm in [3], the third party can track the label position by observing the last round of failed sessions, which makes the algorithm unable to provide forward security. In [15], an authentication algorithm based on hash function is given. The disadvantage is that the tag side will call hash function for many times to calculate, which increases the calculation burden on the tag side. In [12], the

authors mainly analyzed the algorithm designed by CHO, and gave an improved algorithm, which uses hash function to complete encryption, and the computation cost at the tag side is proportional to the number of tags, which is not suitable for large-scale tag authentication environment.

In [11], an authentication algorithm based on hash function and elliptic curve is designed, which?s main drawback is that when hash function is called for more than ten times, elliptic curve needs to be called for nearly ten times. So, it can‘t be used in the existing system with the limited computation. In [2], Duc et al. proposed a new authentication algorithm?which is still based on hash function, and can‘t provide forward security and resist asynchronous attacks.

In [10], in order to resist tag location and tracking? an authentication algorithm is proposed, which has certain security requirements. But, the drawback is that the calculation cost at the tag side is heavy. In [6], an algorithm based on hash function is given. Due to low computational complexity? this algorithm can be applied to the existing system. However, the algorithm lacks the authentication of the tag to the reader, so that the attacker can launch a fake attack.

In [1], an algorithm based on physical unclonable functions (PUF) is given. The algorithm uses PUF encryption and hash function, which increases the computation cost on the label side. At the same time, the algorithm does not update the share key information after each interaction, which makes the algorithm unable to resist asynchronous attacks and provide forward security. In [5], a provably secure algorithm based on hash function is given. There are many issues to be discussed in the algorithm analysis, which can be seen in the detailed analysis in the next section.

In view of the lack of security in most classical algorithms, this paper designs an algorithm combined with modified hash function to improve the security of the algorithm. In the proposed algorithm, according to the Hamming weight of the parameters, it increases the amount of encryption parameters, and carries out different encryption methods.

3 Design of the NFC Authentication Algorithm

In [5], the proposed algorithm uses hash function and pseudo-random number function to encrypt the algorithm simultaneously, which leads to high computation cost. This algorithm has the following problems. First, what is the meaning of the symbol *psID*? There is no detailed explanation in [5]. Second, what is the meaning of symbols *symbol*? There is also no detailed explanation in [5]. Thirdly, the operation length of $r \parallel t$ is $2l$. According to the join operation rule, the value of the first bit l is r, and the value of the last bit l is t. Then, the pseudo-random number and timestamp privacy information can be analyzed, and more other privacy information can be analyzed by combining these information with other information. Fourthly, after the message $r \parallel t$ sent to the tag by the server, the tag does not verify the message sent by the server, but directly carries out the follow-up operation, which leads to the potential security risk of fake attack.

Motivated by the above algorithm framework, and the following improvements are given. Firstly, the design symbols in the algorithm are explained in detail. Second, the algorithm discards the connection operation, the attacker can‘t obtain the privacy information. Third, important information is encrypted before it is sent, so the attacker only gets ciphertext. Fourth, the receiver first verifies the source of the message. If and only if the verification is passed, the receiver will carry out the following steps, so as to avoid irrelevant operations. The fifth point is the deformation of the encryption function. There is only one encryption parameter for the traditional hash function. After the deformation, there are two encryption parameters for the hash function. Based on the Hamming weight of the two parameters, different parameters are selected for encryption to increase the difficulty of cracking.

3.1 NFC Algorithm Symbol Description

The NFC algorithm symbols are described as follows:

R: The whole constituted by the server and the reader, unified as the server;

T: Mobile devices, such as mobile phones;

K: The secret value shared between R and T;

K_{old}: The secret value shared between R and T in the last round;

K_{new}: The shared secret value between R and T in the current round;

T_{IDS}: T pseudonym;

T_{ID}: T identifier;

r_T: Random number generated by T;

r_R: Random number generated by R;

$\oplus$: Bitwise XOR operation;

&: Bitwise sum operation;

$h(X,Y)$: The modified hash function, X, Y are two encryption parameters. When the Hamming weight value X is large, it will encrypt Y; otherwise, it will encrypt X;

ASK: Start session command;

B, D, E, F, M: Communication message.

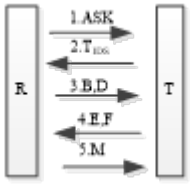


Figure 1: NFC Algorithm Steps

3.2 Steps of the NFC Authentication Algorithm

The proposed algorithm can be divided into two different stages [18], the first stage is the initialization stage, and the second stage is the authentication stage. The purpose of the first stage is to complete the initialization of the R and T information. After the initialization, the R end stores the information as $K, K_{old}, K_{new}, T_{IDS}, T_{ID}$, and $K_{old} = K_{new} = K$; the T end stores the information as K, T_{IDS}, T_{ID}.

The steps of proposed algorithm can be seen in Figure 1. The specific steps are described as follows.

Step 1. Starts the algorithm from the R end, and R sends a message ASK to T.

Step 2. After receiving the message, T sends its own pseudonym T_{IDS} to r as a response.

Explanation: T sends a pseudonym T_{IDS} without sending the real identifier information T_{ID}, which can ensure the security of T privacy information; at the same time, the pseudonym T_{IDS} will be updated after each communication, so as to avoid the attacker launching a location tracking attack on T.

Step 3. After R receiving the message, searches in the database to see if the data is equal to the received T_{IDS}? No, the algorithm stops. If there is, R will generate a random number r_R , and attain the message B, D according to the calculation rule, and finally send B, D to T.

Among them, $B = r_R \oplus T_{ID}, D = h(r_R, T_{ID})$.

Explanation: if R is not found in the database, it indicates that T is likely to be counterfeited by the attacker. Due to this step operation, the redundant steps can be avoided in the follow-up R. If found, R can retrieve other information related to the tag according to T_{IDS}, for example T_{ID}, to facilitate subsequent message calculation.

Step 4. After receiving the message, T will deform the received message B to get the random number r_R, and then use the same algorithm to calculate D by combing r_R with itself T_{ID}. At the same time, it will judge the relationship between D and D.

If the relation is unequal, the algorithm stops.

If the relation is equal, it means $r_R = r_R, D = D$, and it also means that R passes the verification of T. At this time, T generates a random number r_T, calculates the value of message E, F in turn according to the agreed rules, and finally sends message E, F to R. where message $E = (r_R \& T_{ID}) \oplus r_T, F = h(r_T \oplus K, K), D = h(r_R, T_{ID}) = h(B \oplus T_{ID}, T_{ID})$; random number $r_R = B \oplus T_{ID}$.

Explanation: the main function of the message B is to get the random number generated by R, and the main function of the message D is to judge the authenticity of R.

Step 5. After R receiving the message, R will deform the received message E to get the random number r_T, and then use the same algorithm to get F by combing r_T with itself K_*. At the same time, it will judge the relationship between F and F.

If the relation is unequal, the algorithm stops.

If the relation is equal, it indicates that $r_T = r_R$, and T is verified by R. At this point, R starts to calculate the message M, then updates the information, and finally sends M to T.

In the above, when $* = old$, R updates the information in the following way: $K_{new} = h(K_{old}, r_R \& r_T), T_{IDS}^{new} = h(T_{IDS}, r_R \& r_T)$.

In the above, when $* = new$, R updates the information in the following way:

$$\begin{aligned} K_{old} &= K_{new}, \\ K_{new} &= h(K_{new}, r_R \& r_T), \\ T_{IDS}^{new} &= h(T_{IDS}, r_R \& r_T). \end{aligned}$$

where message $M = h(r_R, r_T)$, $F = h(r_T \oplus K_{new}, K_{new})$ or $F = h(r_T \oplus K_{old}, K_{old})$; random number $r_T = E \oplus (r_R \& T_{ID})$.

Explanation: R use K_{new} to calculate F first, and only when the verification T fails, R will use K_{old} again to calculate another F and verify T again. The two verifications can resist the desynchronization attack initiated by the attacker.

Step 6. After T receiving the message, obtains M‘ by combining with the random number of the previous calculation according to the agreed algorithm, and judges the relationship M‘ with M.

If the relation is unequal, the algorithm stops.

If the relation is equal, it indicates that M‘ $= M$, and it also indicates that R passes verification by T. T start updating information:

$$\begin{aligned} K &= h(K, r_R \& r_T), \\ T_{IDS} &= h(T_{IDS}, r_R \& r_T). \end{aligned}$$

After T completes the information update, the algorithm ends.

Explanation: In the process of calculating messages M', we need to use a random number r_R, which has been calculated in Step 4, so it can be directly used here.

4 Security Analysis for NFC Algorithm Protocol

Mutual Authentication.
The proposed algorithm can provide authentication between the two parties in each communication. Specifically, in Step 3, R verifies T through information T_{IDS} for the first time; in Step 5, R verifies T through information E, F for the second time. The verification of R by T is realized in Step 4 and Step 6. Specifically, in Step 4, T verifies R through information B, D for the first time; in Step 6, T verifies R through information M for the second time. So, the proposed algorithm can provide mutual authentication.

Forward Security.
In the encryption process, random numbers are added into session message B, D, E, F, M. Random numbers are randomly generated by random number generator, which are mutually different and unpredictable. It is not feasible to analyze the random number used in the next session from the eavesdropping message for the attacker, so the attacker cannot pass the verification. Therefore, the algorithm has forward security.

Backward Security.
During the encryption process, the session messages B, D, E, M keep the fresh by random numbers r_R, while the session messages E, F, M keep the fresh by random numbers r_T. Random numbers are randomly generated, and the random numbers used in the previous two rounds of conversation have no correlation. The attacker can't deduce the previous random number from the current random number, so, the attacker cannot analyze the useful privacy information. Therefore, the proposed algorithm has backward security.

Replay Attack.
In order to pass a session entity verification?the attacker replays the message obtained from the previous round of eavesdropping in the next round session, so as to obtain other privacy information. The proposed algorithm adds random number to all message encryption process in order to solve the replay attack initiated by the attacker. When the attacker replays the message of the previous round, the random value used in the next round session has changed, so that the calculated value of the current round message is also different, and the replay of the previous round message can only fail to verify. Therefore, the algorithm can resist replay attack.

Location Attack.
In the proposed algorithm, the mobile device identifier information is hidden deliberately, and the pseudonym is introduced. Pseudonym can make the attacker unable to know the real mobile device identifier information. At the same time, pseudonym also uses the update mechanism after each information exchange, which makes the pseudonym information used in each round different, so that the attacker can't locate the specific location of the mobile device. Therefore, the proposed algorithm can resist location attack.

Fake Attack.
The premise of successful fake attack is that the attacker needs to have the privacy information owned by the real session device, and in the algorithm, no matter what means the attacker uses, he can't know the privacy information of any session device in advance; at the same time, in the communication, all the information is sent after encrypted, so that the attacker can eavesdrop on the message in plaintext and cannot know the privacy information. Therefore, the proposed algorithm can resist fake attack.

Asynchronous Attack.
The attacker can destroy some information of the server or mobile device in the session, so that the consistency between them will be lost and the normal communication will not be achieved. In the proposed algorithm, the share key of two rounds sessions is stored at one server end. In Step 5, the server will verify the two mobile devices, so that the consistency between the two can be restored. Therefore, the algorithm can resist asynchronous attack.

5 Performance Analysis of NFC Algorithm

In this section, the comparative analysis between the proposed algorithm and other classical algorithms is given from the calculation cost and the interaction number in mobile devices. The analysis results are shown in Table 1. Notes: $\surd$ means can resist, $\times$ means cannot resist.

In Table 1, the symbol P represents the bitwise operation (such as and operations, join operations, XOR operations), the symbol r represents the computation cost of generating random number, the symbol h represents the computation cost of hash functions (or modified hash functions), the symbol e represents the computation amount of elliptic curve encryption, and the symbol f represents the operation of physically unclonable functions. The symbol pr indicates the computation amount of pseudo-random number function. The symbol l represents the length of each session message, and the symbol

Table 1: Performance and Security Comparison of Different Algorithms

Attack type	[13]	[16]	[10]	[4]	[9]	**Our protocol**
Calculation amount	$6p+1r+8h$	$2p+2r+3h+4e$	$2p+1r+6h$	$1p+1r+4h+6f$	$1p+1r+4h+3pr$	$3p+1r+5h$
Traffic	$7l+1bit$	$6l+2bit$	$6l$	$8l+2bit$	$7l$	$6l+1bit$
Mutual authentication	√	√	√	√	×	√
Forward security	×	√	√	×	√	√
Backward security	√	√	√	√	√	√
Replay attack	√	√	√	√	√	√
Location attack	√	×	√	√	√	√
Fake attack	√	√	×	√	×	√
Asynchronous attack	×	√	√	×	√	√

Notes: √ means can resist, × means cannot resist.

bit represents a bit length. The symbol √ means that it can resist the attack; the symbol × means that it cannot resist the attack.

According to the analysis in Table 1, the computation cost of the proposed algorithm is similar to that of the algorithm in [10, 13] on the mobile device end, but the computation amount of the proposed algorithm is still slightly small on the mobile device end, because the number of encryption times of hash function is less than the two other algorithms. The proposed algorithm is different from the algorithm in [4,9,16] in terms of the computation amount at the mobile device end. Because the algorithm in [4, 9, 16] not only uses hash function encryption, but also uses other encryption methods to encrypt information, which increases the computation amount to a certain extent. At the same time, the total number of gates at the mobile device side will also increase in the implementation process, resulting in an increase of mobile devices. From the perspective of interactive information number in a complete session, the proposed algorithm basically maintains a considerable level compared with other algorithms.

In the proposed algorithm, bit operation will be used for the first time when calculating random number r_R, and bit operation will be used for the second and third time when calculating message E. Therefore, in the whole algorithm, bit operation is used for three times on the mobile device end. The mobile device side will generate a random number r_T, so in the whole algorithm, the random number generation is used on the mobile device side. The mobile device side uses hash function encryption for the first time when calculating messages D, and will use hash function encryption for the second time, the third time, the fourth time and the fifth time when calculating messages F, message M, updating shared key K and updating pseudonym T_{IDS}. Therefore, hash function encryption will be used on the mobile device side for five times in the whole algorithm. Based on the above, the total computation cost at the mobile device side is $3p+1r+5h$.

Based on the analysis of Table 1, the proposed algorithm can reduce the computation cost at the mobile device side. In a whole session, this algorithm does not increase the number of interactive information, meanwhile, the proposed algorithm has a greater improvement in the security aspect compared with other algorithms. It can give the common types attacks, provide the better security requirements to users, and ensure the security of users' privacy information.

6 Formal Reasoning Based on GNY Logic

The formal reasoning method based on GNY logic is used to prove the algorithm.

Formal Model.

In order to analyze the proposed algorithm formally with GNY logic, it is necessary to model the communication process in the proposed algorithm formally. Here, symbol R is used to represent server and symbol T is used to represent the mobile device:

$Msg1 : R \rightarrow T : ASK$

$Msg2 : T \rightarrow R : T_{IDS}$

$Msg3 : R \rightarrow T : B, D$

$Msg4 : T \rightarrow R : E, F$

$Msg5 : R \rightarrow T : M$

The model is further formulated as follows:

$Msg1 : T \triangleleft *ASK \sim | \rightarrow R| \equiv \#ASK$

$Msg2 : R \triangleleft *T_{IDS} \sim | \rightarrow T| \equiv \#T_{IDS}$

$Msg3 : T \triangleleft * (B, D) \sim | \rightarrow R| \equiv \# (B, D)$

$Msg4 : R \triangleleft * (E, F) \sim | \rightarrow T| \equiv \# (E, F)$

$Msg5 : T \triangleleft *M \sim | \rightarrow R| \equiv \#M$

Initialization Hypothesis.

$A1 : R \ni T_{ID}$

$A2 : R \ni K$

$A3 : R \ni T_{IDS}$

$A4 : T \ni T_{IDS}$

$A5 : T \ni T_{ID}$

$A6 : T \ni K$

$A7 : R| \equiv \#(r_T)$

$A8 : T| \equiv \#(r_R)$

$A9 : R| \equiv R \overset{T_{ID}}{\longleftrightarrow} T$

$A10 : R| \equiv R \overset{T_{IDS}}{\longleftrightarrow} T$

$A11 : R| \equiv R \overset{K}{\longleftrightarrow} T$

$A12 : T| \equiv T \overset{K}{\longleftrightarrow} R$

$A13 : T| \equiv T \overset{T_{ID}}{\longleftrightarrow} R$

$A14 : T| \equiv T \overset{T_{IDS}}{\longleftrightarrow} R$

Initialization hypothesizes are as follows: $A1, A2, A3$ is owned by server R, $A4, A5, A6$ is owned by mobile device T, $A7$ is server R's belief in the freshness of information, $A8$ is server T's belief in the freshness of information, $A9, A10, A11$ is the share information trusted between the mobile device T and server R, $A12, A13, A14$ is the share information trusted between the server R and mobile device T.

Proving Goals.

Based on GNY logic formal analysis, in the proposed algorithm?five goals needs to be proved:

$G1 : R| \equiv T| \sim \#(F)$

$G2 : R| \equiv T| \sim \#(E)$

$G3 : T| \equiv R| \sim \#(B)$

$G4 : T| \equiv R| \sim \#(D)$

$G5 : T| \equiv R| \sim \#(M)$

Reasoning Proof.

Because the reasoning proof process of the five proof goals is similar, here, only the proof of $G1$ is selected as an example for reasoning proof. The reasoning of proof goal is as follows:

First of all, from the initialization assumption $A7 : R| \equiv \#(r_T)$: and the freshness rule: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y),P|\equiv\#(F(X))}$ we can know that $R| \equiv \#(r_T, K)$.

In $Msg4, R \triangleleft * r_T$, that is $R \ni r_T$, combining the initialization assumptions $A1, A2, A3$, and rules $P2$, we can know that $R \ni (r_T, K)$.

Then, according to $R| \equiv \#(r_T, K)$, $R \ni (r_T, K)$ and the rule of freshness $F10 : \frac{P|\equiv\#(X),PX}{P|\equiv\#(H(X,Y))}$, we can know that $R| \equiv \#(F)$, that is $R| \equiv \#(h(r_T \oplus K, K))$.

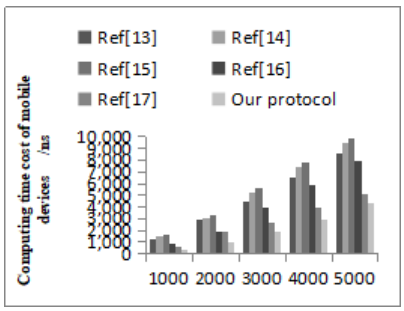


Figure 2: Comparison of Computing Time Cost of Mobile Devices with Different Algorithms

Finally, according to $Msg4, A11, R \ni (r_T, K), R| \equiv \#(h(r_T \oplus K, K))$ and message parsing rule $I3$, we can get: $R| \equiv T| \sim (F)$, that is $R| \equiv T| \sim (h(r_T \oplus K, K))$.

From the definition of freshness, we can deduce the proof goal $G1 : R| \equiv T| \sim (F)$, that is $G1 : R| \equiv T| \sim (h(r_T \oplus K, K))$.

7 Simulation Experiment

In this section, simulation experiments are carried out for the computing time cost of mobile devices in different NFC algorithms. The computing time cost of the mobile device not only includes the computing time at the mobile device side, but also includes the waiting time in the whole message interaction process. Therefore, the result is related to the computation amount and the communication amount.

The simulation environment is as follows: win 8 operating system (64 bit operating system), 4GB ram and Intel Core i5-3230m CPU@ 60GHz. Small and portable MySQL is used as the database for data storage, MATLAB software is used for simulation, part of the simulation program is based on C language programming, and the data storage is realized by linked list in data structure.

In the simulation experiment, in order to avoid the interference of random factors on the accuracy of simulation experiment, no less than 200 simulation experiments are carried out in each simulation experiment. There is only one server, and gradually increase the number of mobile devices that have a session with the server. When the number of mobile devices in the session is 1000, 2000, 3000, 4000 and 5000, we record each computing time cost at the mobile device side, calculate the average value of experiment data, and take the average value as the final result. The computing time cost of different algorithms at the mobile device side is shown in Figure 2.

As can be seen from Figure 2, when the number of mobile devices is small, the computing time overhead of the mobile devices is close among different algorithms. When the number of mobile devices interacting with the server

increases gradually, the computing time cost of the algorithms in [4, 9, 16] increases obviously. The main reason is that the three algorithms not only use hash function, but also use other encryption algorithms, which makes the overall computing time cost increase obviously. The computing time cost of mobile devices between [10, 13] and our algorithm is not very large. The main reason is that the three algorithms only use hash function to encrypt information, which can effectively reduce the computing time cost. However, it is obvious that the computing time cost of our algorithm is better than that of the other two algorithms. The reason is that the number of times using hash function encryption is slightly less than other algorithms. Therefore, overall, the total communication cost of the proposed algorithm is better than other algorithms.

8 Conclusions

In this paper, a lightweight NFC authentication algorithm is proposed. In the proposed algorithm, we firstly present a modified hash function encryption algorithm, which encrypts the communication information to ensure the information security. The modified hash function makes full use of the Hamming weight parameter carried by the encryption parameter itself, which can reduce the introduction of new parameters, decrease the storage space, meanwhile, increase the difficulty of attacker's cracking capacity. The analysis results show that the proposed algorithm has higher security performance and meets the user's security needs. Simulation experiment results show that the comprehensive cost of the proposed algorithm is better than other NFC algorithms.

Acknowledgments

This paper is supported by the Exploration on curriculum system reform of excellent network engineer training under the background of "collaborative education"(the second batch of industry university collaborative education project of Higher Education Department of the Ministry of education in 2018) (201802068001).

References

[1] X. Chen, K. Choi, K. Chae, "A secure and efficient key authentication using bilinear pairing for NFC mobile payment service," *Wireless Personal Communications*, vol. 92, no. 1, pp. 1–17, 2017.

[2] S. Y. Chiou, "An efficient RFID authentication protocol using dynamic identity," *International Journal of Network Security*, vol. 21, no. 5, pp. 728–734, 2019.

[3] Y. P. Duan, "Lightweight RFID group tag generation protocol," *Control Engineering of China*, vol. 27, no. 4, pp. 751–757, 2020.

[4] P. Gope, J. Lee, T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[5] Y. J. Li, S. B. Wang, X. T. Yang, *et al.*, "Lightweight NFC security authentication scheme based on mobile terminal," *Computer Engineering and Applications*, vol. 56, no. 16, pp. 84–89, 2020.

[6] J. Ling, Y. Wang, W. F. Chen, "An improved privacy protection security protocol based on NFC," *International Journal of Network Security*, vol. 19, no. 1, pp. 39–46, 2017.

[7] D. W. Liu, J. Ling, "Improved RFID authentication protocol with backward privacy," *Computer Science*, vol. 43, no. 8, pp. 128–130, 2016.

[8] Y. L. Liu, X. C. Yin, Y. Q. Dong, *et al.*, "Lightweight authentication scheme with inverse operation on passive RFID tags," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 74–79, 2019.

[9] Z. H. Liu, C. J. Huang, H. Suo, "Modified mobile RFID bidirectional authentication protocol against counterfeiting attack," *Computer Applications and Software*, vol. 37, no. 6, pp. 309–315, 2020.

[10] Y. N. Ma, "NFC communications-based mutual authentication scheme for the internet of things," *International Journal of Network Security*, vol. 19, no. 4, pp. 631–638, 2017.

[11] S. Q. Mei, X. R. Deng, "Mobile RFID bidirectional authentication protocol based on shared private key and bitwise operation," *Computer Applications and Software*, vol. 37, no. 7, pp. 302–308, 2020.

[12] F. Tan, "An improved RFID mutual authentication security hardening protocol," *Control Engineering of China*, vol. 26, no. 4, pp. 783–789, 2019.

[13] J. Q. Wang, Y. F. Zhang, D. W. Liu, "Provable secure for the ultra-lightweight RFID tag ownership transfer protocol in the context of iot commerce," *International Journal of Network Security*, vol. 22, no. 1, pp. 12–23, 2020.

[14] P. Wang, Z. P. Zhou, J. Li, "Improved serverless RFID security authentication protocol," *Journal of Frontiers of Computer Science and Technology*, vol. 12, no. 7, pp. 1117–1125, 2018.

[15] Y. S. Wei, J. H. Chen, "Tripartite authentication protocol RFID/NFC based on ECC," *International Journal of Network Security*, vol. 22, no. 4, pp. 664–671, 2020.

[16] R. Xie, J. Ling, D. W. Liu, "Wireless key generation algorithm for RFID system based on bit operation," *International Journal of Network Security*, vol. 20, no. 5, pp. 938–949, 2018.

[17] H. Xu, J. Ding, P. Li, et al, "A lightweight RFID mutual authentication protocol based on physical unclonable function," *Sensors*, vol. 18, no. 3, pp. 760–780, 2018.

[18] B. Yuan, J. Liu, "A universally composable secure grouping proof protocol for RFID tags," *International Journal of Network Security*, vol. 28, no. 6, pp. 1872–1883, 2016.

Biography

Fang-ming Cao graduated from South China University of technology with a master's degree in 2016. Now working in Guangdong Peizheng University, he is a full-time teacher of computer major, and also a lecturer. At present, the research direction is mainly in the field of information security, etc.

Dao-wei Liu received a master's degree in School of Computers from Guangdong University of Technology (China) in June 2016. He is a teacher in department of computer science and engineering, Guangzhou College of Technology and Business. His current research interest fields include information security.

On the Linear Complexity of Binary *Half-ℓ-Sequences*

Zhihua Niu[1,2] and Yuqi Sang[1]
(Corresponding author: Zhihua Niu)
School of Computer Engineering and Science, Shanghai University[1]
Shanghai 200444, China
Email: zhniu@shu.edu.cn
Key Laboratory of Applied Mathematics (Putian University), Fujian Province University[2]
Fujian Putian, 351100, China
(Received Apr. 6, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 23, 2022)

Abstract

Binary *half-ℓ-sequences* are $\varphi(q)/2$-periodic sequences generated by a Feedback with Carry Shift Register(FCSR) with connection integer q. In this paper, we focus on the linear complexity of binary *half-ℓ-sequences*. We give some upper and lower bounds of their linear complexity. The numerical experiment shows that for most binary *half-ℓ-sequences* the linear complexity is close to the upper bound.

Keywords: Binary Sequence; Feedback with Carry Shift Register; Half-ℓ-Sequence; Linear Complexity

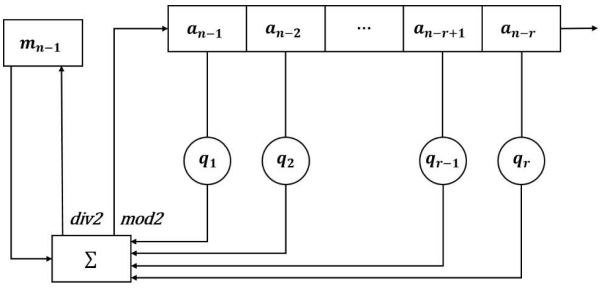


Figure 1: Feedback with carry shift register

1 Introduction

Linear Feedback Shift Registers(LFSRs) are widely used in information theory, coding theory, and cryptography. Klapper and Goresky [10] proposed Feedback with Carry Shift Registers(FCSRs), a new type of feedback shift registers as an alternative to LFSRs. The main idea of FCSR is to add a memory to LFSR. Figure 1 shows the structure of FCSR with connection integer $q = -1 + q_1 2^1 + q_2 2^2 + \ldots + q_r 2^r$, where $q_i \in \{0, 1\}$ and $r = \lceil \log_2(q+1) \rceil$ is the length of the FCSR. $\sum$ represents integer addition and $m_n \in \mathbb{Z}$.

The operation of the shift register is defined as follows:

1) Compute the sum $\sigma = \sum_{i=1}^{r} q_i a_{n-i} + m_{n-1}$;
2) Shift the contents one step to the right, outputting the right almost bit a_{n-r};
3) Place $a_n = \sigma_n \pmod 2$ into the leftmost shift register;
4) Replace the memory integer m_{n-1} with $m_n = (\sigma_n - a_{n+r})/2 = \lfloor \sigma_n/2 \rfloor$.

Klapper and Goresky discussed some basic properties of sequences produced by FCSRs [10]. To obtain stream ciphers with better performance, some researchers tried to combine LFSRs with FCSRs [6, 19]. Some researchers proposed shift registers base on modified FCSRs, such as ring FCSR [3, 11], F-FCSR [1] and X-FCSR [2].

For a (binary) sequence $s^\infty = s_0, s_1, \ldots$ generated by an FCSR of the shortest length with connection integer q, we denote

$$\Phi_2(s^\infty) = \lceil \log_2(q+1) \rceil,$$

called the *2-adic complexity* of s^∞. And s^∞ is periodic with period $T = \mathrm{ord}_q(2)$, where $\mathrm{ord}_q(2)$ is the multiplicative order of 2 modulo q. It is clear, if $T = \varphi(q)$, where $\varphi(-)$ is the Euler function, then s^∞ reaches its maximum period. Such sequence is referred to as the *ℓ-sequence* [10]. If $T = \varphi(q)/2$, s^∞ is called the *half-ℓ-sequence* in [8, 18], which will be discussed in this work. In this case, the connection integer q is prime and $q \equiv \pm 1 \pmod 8$. For details on FCSRs, the reader is referred to the classic books [7, 9].

An LFSR or an FCSR can generate any binary periodic sequence s. The length of the shortest LFSR (resp. FCSR) capable of producing s is called the linear complexity (resp. *2-adic complexity*) of s. In cryptography, as candidates of keys in stream cipher systems, binary sequences must have large "complexity".

We should remark that it seems that there is no relationship between the linear complexity and the *2-adic complexity* of a sequence. For example, any m-sequence of period 2^n-1 has the maximal *2-adic complexity* $\log_2(2^{2^n-1}-1)$ (see [17]) but its linear complexity is n. So it is necessary to consider the linear complexity for sequences generated by an FCSR.

Indeed, the linear complexity of *ℓ-sequences* has been widely investigated. C. Seo and S. Lee [15] discussed the linear complexity of *ℓ-sequences* when connection integer q is 2-prime or strong 2-prime. Q. C. Wang and H. Xu [13] deduced the linear complexity of *ℓ-sequences* when q is of form p^e with any prime p. L. Tan and Q. C. Wang [16] studied the stability of the linear complexity of *ℓ-sequences*. A. Arshad [4] described the behavior of frequency distribution of various patterns in binary *ℓ-sequences*.

In this paper, we study the linear complexity of binary *half-ℓ-sequences*, which has not been touched on in the literature. In Section 2, we introduce some related notions and lemmas. In Sections 3, we give some bounds for the linear complexity of binary *half-ℓ-sequences* generated by an FCSR with a prime connection integer $q \equiv 1 \pmod 8$. In Section 4, we give some bounds for sequences with $q \equiv 7 \pmod 8$. Finally, we summarize the work in Section 5.

2 Preliminaries

For our discussion, we need the exponential representation of FCSR sequences proposed by Klapper [10].

Definition 1. *[10] Let s^∞ be a periodic binary sequence generated by an FCSR with connection integer q. Then there exists $A \in \mathbb{Z}_q$ such that for all $i = 0, 1, 2, \ldots$ we have*

$$s_i = A \cdot 2^{-i} \pmod q \pmod 2. \tag{1}$$

Then, we introduce some definitions and lemmas about characteristic polynomial, generating function, cyclotomic polynomial, and order of the polynomial, which are important in our proof.

Definition 2. *[5] Let s^∞ be a T-period sequence over $\mathbb{F}_2$. A polynomial of the form*

$$f(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_r x^r \in \mathbb{F}_2[x]$$

is called the characteristic polynomial of s^∞ if

$$s_i = c_1 s_{i-1} + c_2 s_{i-2} + \ldots + c_r s_{i-r}, \forall i \geq r.$$

The characteristic polynomial with the lowest degree is called the minimal polynomial, denoted by $m(x)$. The linear complexity of s^∞ is defined as the degree of $m(x)$, denoted as $LC(s^\infty)$.

Definition 3. *[5] Let s^∞ be a T-periodic sequence over $\mathbb{F}_2$, the polynomial of the form*

$$S(x) = s_0 + s_1 x + s_2 x^2 + \ldots \in \mathbb{F}_2[x] \tag{2}$$

is called the generating function of s^∞.

Lemma 1. *[5] Let s^∞ be a T-periodic sequence with generating polynomial $S(x)$ defined by Equation (2). Then the linear complexity of s^∞ is*

$$LC(s^\infty) = T - \deg(gcd(x^T - 1, S(x))).$$

Definition 4. *[14] Let $g(x) \in \mathbb{F}_2[x]$ be a nonzero polynomial. If $g(0) \neq 0$, then the least positive integer m for which $g(x)$ divides $1 + x^m$ is called the order of $g(x)$ and denoted by $ord(g(x))$.*

The order of a polynomial is also called the period of it.

Lemma 2. *[14] Let $m(x)$ be the minimal polynomial of s^∞ of the least period T, then $ord(m(x)) = T$.*

Lemma 3. *[14] Let $h(x) = g_1(x)^{n_1} g_2(x)^{n_2} \ldots g_k(x)^{n_k}$, where $g_1(x), g_2(x), \ldots, g_k(x)$ are pairwise relatively prime nonzero polynomials and $n_1, n_2, \ldots, n_k \in \mathbb{N}$. Then $ord(h(x)) = 2^\xi m$, where ξ is the least positive integer such that $2^\xi \geq \max\{n_1, n_2, \ldots, n_k\}$ and m is $lcm(ord(g_1(x)), ord(g_2(x)), \ldots, ord(g_k(x))$.*

Definition 5. *[14] Let n be a positive integer with $p \nmid n$, and e be an n-th root of unity over $\mathbb{F}_2$, then*

$$Q_n(x) = \prod_{\substack{i=1, \\ gcd(i,n)=1}}^{n} (x - e^i) \tag{3}$$

is the n-th cyclotomic polynomial over $\mathbb{F}_2$.

According to the theory of cyclotomic polynomial [14], we have

$$1 + x^n = \prod_{d|n} Q_d(x) \tag{4}$$

and

$$Q_d(x) = \prod_{i=1}^{\varphi(d)/\deg(r_i(x))} r_i(x), \tag{5}$$

where $r_i(x)$ is an irreducible polynomial of degree $ord_d(2)$.

3 Bounds on Linear Complexity of Binary *half-ℓ-sequences* with Prime Connection Integer $q \equiv 1 \pmod 8$

In this section, we discuss the linear complexity of binary *half-ℓ-sequences* generated by FCSR with a prime connection integer $q \equiv 1 \pmod 8$.

Lemma 4. *[8] Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then s^∞ is balanced, and the first half of s^∞ is the bit-wise complement of its second half.*

Lemma 4 deduces the following lemma.

Lemma 5. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then $f(x) = 1 + x + x^{(q-1)/4} + x^{(q-1)/4+1}$ is a characteristic polynomial of s^∞.*

From the above lemma, we immediately get a general upper bound for linear complexity.

Theorem 1. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Then we have*

$$LC(s^\infty) \le (q-1)/4 + 1.$$

Proof. By Lemma 5, we have $LC(s^\infty) \le \deg(f(x)) = (q-1)/4 + 1$. □

Below we give two lower bounds. The first (Theorem 3) is obtained by analyzing the characteristic polynomial of binary *half-ℓ-sequences*. The second lower bound (Theorem 4) is from the exponential representation of binary FCSR sequences.

Theorem 2. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Write*

$$\frac{q-1}{2} = 4 \cdot 2^{e_0} p_1^{e_1}$$

with odd prime p_1 and $e_i \in \mathbb{N}$ for $i \in \{0, 1\}$. Then we have

$$LC(s^\infty) \ge 1 + 2^{e_0+1} + ord_{p_1^{e_1}}(2).$$

Proof. Let I_d be the set of all the factors of d, for example, $I_{12} = \{1, 2, 3, 4, 6, 12\}$. By Lemma 5, we see that

$$f(x) = (1+x)(1 + x^{p_1^{e_1}})^{2^{e_0+1}}$$

is a characteristic polynomial of s^∞. According to Equactions (4) and (5),

$$\begin{aligned} f(x) =& (1+x)^{1+2^{e_0+1}} \prod_{d | p_1^{e_1}} Q_d(x)^{2^{e_0+1}} \\ =& (1+x)^{1+2^{e_0+1}} \prod_{d | p_1^{e_1}} \Big(\prod_{i=1}^{\varphi(d)/\deg(r_{i_d}(x))} r_{i_d}(x) \Big)^{2^{e_0+1}}. \end{aligned}$$

Since the minimal polynomial $m(x) \mid f(x)$, then

$$m(x) = (1+x)^a \prod_{j=1}^{k} \Big(\prod_{i=1}^{c_j} r_{i_{d_j}}(x) \Big)^{b_j}$$

where $d_j \mid p_1^{e_1}$, $1 \le k \le \#I_{p_1^{e_1}}$, $1 \le b_j \le 2^{e_0+1}$, $0 \le a \le 1 + 2^{e_0+1}$, and $1 \le c_j \le \varphi(d_j)/\deg(r_{i_{d_j}}(x))$.

From Lemma 3,

$$ord(m(x)) = 2^\xi \cdot lcm(d_1, d_2, \ldots, d_k),$$

where ξ is the least positive integer such that $2^\xi \ge \max\{a, b_1, \ldots, b_k\}$. From Lemma 2, $ord(m(x)) = (q-1)/2 = 2^{e_0+2} p_1^{e_1}$. Hence,

$$2^\xi = 2^{e_0+2}, lcm(d_1, d_2, \ldots, d_k) = p_1^{e_1}.$$

Clearly, $1 + 2^{e_0+1}$ is the least positive integer such that $2^\xi \ge 2^{e_0+2}$. For $d_j \mid p_1^{e_1}$, we have $\deg(r_{i_j}(x)) > 1$. So the degree of $m(x)$

$$\begin{aligned} \deg(m(x)) \ge& \deg((1+x)^{1+2^{e_0+1}} \prod_{j=1}^{k} r_{i_{d_j}}(x)) \\ \ge& 1 + 2^{e_0+1} + \sum_{j=1}^{k} ord_{d_j}(2). \end{aligned}$$

Since $d_j \mid p_1^{e_1}$ and $lcm(d_1, d_2, \ldots, d_k) = p_1^{e_1}$, there must exist some $1 \le k \le \#I_{p_1^{e_1}}$ such that $p_1^{e_1} \in \bigcup_{j=1}^{k} I_{d_j}$. So we have

$$\sum_{j=1}^{k} ord_{d_j}(2) > ord_{p_1^{e_1}}(2)$$

and

$$LC(s^\infty) = \deg(m(x)) \ge 1 + 2^{e_0+1} + ord_{p_1^{e_1}}(2).$$

□

Based on Theorem 2, we give a more general result.

Theorem 3. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer $q \equiv 1 \pmod 8$. Write*

$$\frac{q-1}{2} = 4 \cdot 2^{e_0} p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$$

with odd primes p_i, $e_0 \in \mathbb{N} \cup \{0\}$ and $e_i \in \mathbb{N}$ for $1 \le i \le t$. Then we have

$$LC(s^\infty) \ge 1 + 2^{e_0+1} + \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}.$$

Proof. Similar to Theorem 2,

$$f(x) = (1+x)^{1+2^{e_0+1}} \prod_{\substack{d>1, \\ d | \prod_{i=1}^{t} p_i^{e_i}}} \Big(\prod_{i=1}^{\varphi(d)/\deg(r_{i_d}(x))} r_{i_d}(x) \Big)^{2^{e_0+1}}$$

is a characteristic polynomial of s^∞. Let $m(x)$ be the minimal polynomial of s^∞, then

$$m(x) = (1+x)^a \prod_{j=1}^{k} \Big(\prod_{i=1}^{c_j} r_{i_{d_j}}(x) \Big)^{b_j},$$

where $d_j \mid \prod_{i=1}^{t} p_i^{e_i}$, $1 \le k \le \#I_{\prod_{i=1}^{t} p_i^{e_i}}$, $1 \le b_j \le 2^{e_0+1}$, $0 \le a \le 1 + 2^{e_0+1}$, and $1 \le c_j \le \varphi(d_j)/\deg(r_{i_{d_j}}(x))$. According to Lemma 3, we have $ord(m(x)) = 2^\xi \cdot lcm(d_1, d_2, \ldots, d_k)$, then $2^\xi = 2^{e_0+2}$ and $lcm(d_1, d_2, \ldots, d_k) = \prod_{i=1}^{t} p_i^{e_i}$.

Similar to Theorem 2,

$$\deg(m(x)) \geq 1 + 2^{e_0+1} + \sum_{j=1}^{k} ord_{d_j}(2).$$

Since $d_j \mid p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ and $lcm(d_1, \dots, d_k) = \prod_{i=1}^{t} p_i^{e_i}$, there must exist some $1 \leq k \leq \#I_{p_1^{e_1} \dots p_t^{e_t}}$ such that $\{p_1^{e_1}, \dots, p_t^{e_t}\} \subset \bigcup_{j=1}^{k} I_{d_j}$. For $\gcd(a, b) = 1$, $ord_{ab}(2) = lcm(ord_a(2), ord_b(2)) \geq \max\{ord_a(2), ord_b(2)\}$. We can deduce

$$\sum_{j=1}^{k} ord_{d_j}(2) \geq \max\{ord_{p_1^{e_1}}(2), \dots, ord_{p_t^{e_t}}(2)\}$$

and

$$LC(s^\infty) \geq 1 + 2^{e_0+1} + \max\{ord_{p_1^{e_1}}(2), \dots, ord_{p_t^{e_t}}(2)\}.$$

□

Next, by Definition 1, we give a lower bound in Theorem 4.

Theorem 4. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with prime connection integer q. Then we have*

$$LC(s^\infty) \geq 1 + \lfloor \log_2(q) \rfloor.$$

Proof. From Definition 2, the generating function of sequence s^∞ is

$$S(x) = \sum_{i=0}^{\infty} A \cdot 2^{-i} \pmod q \pmod 2 x^i \tag{6}$$

Let β be the prime such that $2^\beta < q$ and $2^{\beta+1} > q$, from Definition 1, we have

$$s_{T-1-\beta} = 2^{-T+(\beta+1)} \equiv 1 \pmod q \pmod 2$$

and

$$s_{T-1-i} = 2^{-T+1+i} \equiv 0 \pmod q \pmod 2,$$

where $0 \leq i \leq \beta - 1$. Let $A = 1$ in Equation (6), then

$$S(x) = \sum_{i=0}^{T-1-(\beta+1)} s_i x^i + x^{T-1-\beta},$$

and

$$\deg(S(x)) \leq T - 1 - \lfloor \log_2(q) \rfloor.$$

From Lemma 1,

$$LC(s^\infty) = T - \deg(\gcd(x^T - 1, S(x))) \geq 1 + \lfloor log_2(q) \rfloor.$$

□

Remark 1. *The result in Theorem 4 holds for either $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$.*

For all binary *half-ℓ-sequences* with prime $q \equiv 1 \pmod 8$ and $q < 5000$, by the BM algorithm [12] and the results in the above theorems, we can check that about 82% of binary *half-ℓ-sequences* whose linear complexity achieves the upper bound in Theorem 1.

Example 1. *Let us consider the FCSR with connection integer $q = 41 = 2^0 \times 5 \times 8 + 1$, the period is $(q-1)/2 = 20$. With the constant $A = 1$, binary half-ℓ-sequence s^∞ is given by*

$$s_i = 21^i \pmod{41} \pmod 2 \tag{7}$$

where $i = 0, 1, 2, \dots$, then the first period of s^∞ is

$$s^{20} = 11100111110001100000$$

From Theorem 1, $LC(s^\infty) \leq (q-1)/4 + 1 = 11$. From Theorem 3, $LC(s^\infty) \geq 1 + 2^{0+1} + ord_5(2) = 7$. And from Theorem 4, $LC(s^\infty) \geq 1 + \lfloor log_2(41) \rfloor = 6$. By the BM algorithm, the linear complexity $LC(s^\infty) = 11$.

4 Bounds on Linear Complexity of Binary *half-ℓ-sequences* with Prime Connection Integer $q \equiv 7 \pmod 8$

In this section, we discuss the linear complexity of binary *half-ℓ-sequences* with prime $q \equiv 7 \pmod 8$. We give an upper bound in Theorem 5 and a lower bound in Theorem 6, respectively.

For a T-periodic binary sequence s^∞, let $W_H(s^\infty)$ denote the Hamming weight of the first period of s^∞, i.e. the number of 1's in one period of s.

Theorem 5. *Let s^∞ be a binary half-ℓ-sequence s^∞ generated by an FCSR with prime $q \equiv 7 \pmod 8$. If $W_H(s^\infty)$ is odd, then $LC(s^\infty) \leq (q-1)/2$. And if $W_H(s^\infty)$ is even, then $LC(s^\infty) \leq (q-1)/2 - 1$.*

Proof. Let $W_H(s^\infty)$ be even, then $(1 + x) \mid S(x)$. By Lemma 1, we have

$$\deg(\gcd(x^T - 1, S(x))) \geq \deg(1 + x)$$

and hence

$$LC(s^\infty) \leq (q-1)/2 - 1.$$

Let $W_H(s^\infty)$ be odd, we know that $(1 + x) \nmid S^T(x)$. Similarly,

$$LC(s^\infty) \leq (q-1)/2.$$

□

Theorem 6. *Let s^∞ be a binary half-ℓ-sequence generated by an FCSR with $q \equiv 7 \pmod 8$. Write*

$$\frac{q-1}{2} = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$$

with odd primes p_i and $e_i \in \mathbb{N}$ for $1 \leq i \leq t$. Then we have

$$LC(s^\infty) \geq \max\{ord_{p_1^{e_1}}(2), ord_{p_2^{e_2}}(2), \dots, ord_{p_t}^{e_t}(2)\}.$$

Proof. Let $m(x)$ be the minimal polynomial of s^∞. From Definition 4, we can deduce $m(x)|(1+x^{(q-1)/2})$.

Let $(q-1)/2 = \prod_{i=1}^{t} p_i^{e_i}$, then we have

$$ord(m(x)) = (q-1)/2 = \prod_{i=1}^{t} p_i^{e_i}.$$

Similar to Theorem 3,

$$1 + x^{(q-1)/2} = (1+x) \prod_{\substack{d>1, \\ d|p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}}} Q_d(x).$$

Suppose $m(x) = \prod_{j=1, b_j \geq 1}^{k} Q_{d_j}(x)^{b_j}$, where $d_j \mid \prod_{j=1}^{k} p_j^{e_j}$, $d_j > 1, b_j \geq 1$. From Lemma 3, we have

$$ord(m(x)) = 2^{\xi} \cdot lcm(d_1, d_2, \ldots, d_k),$$

where ξ is the least integer such that $2^{\xi} \geq \max\{b_1, b_2, \ldots, b_k\}$.

According to Lemma 2, $ord(m(x)) = \prod_{i=1}^{t} p_i^{e_i}$, we have

$$2^{\xi} = 1, lcm(d_1, d_2, \ldots d_k) = \prod_{i=1}^{t} p_i^{e_i}.$$

By Theorem 3, $LC(s^\infty) \geq \max\{ord_{p_1^{e_1}}(2), \ldots, ord_{p_t^{e_t}}(2)\}$. □

The result in Theorem 4 is also suitable for the case $q \equiv 7 \pmod 8$.

For prime $q < 5000$ with $q \equiv 7 \pmod 8$, we can check that about 86% of binary *half-ℓ-sequences* whose linear complexity achieves the upper bound.

Example 2. *Let us consider a binary half-ℓ-sequence s^∞ with $q = 47 = 5 \times 8 + 7$, and the period of s^∞ is $(q-1)/2 = 23$. With the constant $A = 1$, the sequence is given by*

$$s_i = 24^i \pmod{47} \pmod 2 \tag{8}$$

where $i = 0, 1, 2, \ldots$. Then the first period of s^∞

$$s^{23} = 10001100100111010100000$$

From Theorem 3, $LC(s^\infty) \leq (q-1)/2 - 1 = 23$. From Theorem 4, $LC(s^\infty) \geq ord_{23}(2) = 11$. From 6 $LC(s^\infty) \geq 1 + \lfloor log_2(47) \rfloor = 7$. By the BM algorithm, the linear complexity is $LC(s^\infty) = 23$.

5 Conclusions

In this paper, we have discussed the linear complexity of binary *half-ℓ-sequences* generated by FCSRs. Based on the theory of FCSR and cyclotomic polynomial, we give some bounds of linear complexity and some examples. The numerical experiment shows that the linear complexity of most binary *half-ℓ-sequences* achieves the upper bound.

Acknowledgments

This work was partially supported by the National Key Research and Development Program of China(2018YFB0704400), Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) (NO. SX202102), the National Nature Science Foundation of Shanghai (Grant No. 19ZR1417700), the Research and Development Program in Key Areas of Guangdong Province(Grant No.2018B010113001), the State Key Program of National Nature Science Foundation of China (Grant No. 61936001).

References

[1] F. Arnault and T. Berger, "F-FCSR: Design of a new class of stream ciphers," in *International Workshop on Fast Software Encryption, Lecture Notes in Computer Science*, vol. 3557, pp. 83–97, 2005.

[2] F. Arnault and T. Berger, "X-FCSR – A new software oriented stream cipher based upon FCSRs," in *Progress in Cryptology – INDOCRYPT 2007, Lecture Notes in Computer Science*, vol. 4859, pp. 341–350, Springer, 2007.

[3] F. Arnault and T. Berger, "A new approach for FCSRs," in *Selected Areas in Cryptography*, pp. 433–448, Springer, 2009. .

[4] A. Arshad, "Feedback with carry shift registers and (in-depth) security of ciphers based on this primitive," in *15th International Bhurban Conference on Applied Sciences and Technology (IBCAST'18)*, pp. 431–438, Pakistan, 2018.

[5] T. W. Cusick and C. Ding, *Stream ciphers and number theory*. Elsevier, 1998. ISBN: 9780444516312.

[6] L. Dong and J. Wang, "Novel analysis of stream cipher combing LFSR and FCSR," in *International Conference on Frontiers in Cyber Security*, vol. 879, pp. 23–38, 2018.

[7] M. Goresky and A. Klapper, *Algebraic shift register sequences*. Cambridge: Cambridge University Press, 2012. ISBN: 9781107014992.

[8] T. Gu and A. Klapper, "Distribution properties of half-ℓ-sequence," in *Sequences and Their Applications - SETA 2014, Lecture Notes in Computer Science*, vol. 8865, pp. 234–245, Cham, 2014.

[9] M. S. Hwang and I. C. Lin, *Introduction to Information and Network security (6ed, in Chinese)*. Taiwan: Mc Graw Hill, 2017.

[10] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *Journal of Cryptology*, vol. 10, no. 2, pp. 111–147, 1997.

[11] Z. Lin, D. Pei, and D. Lin, "Fast construction of binary ring FCSRs for hardware stream ciphers," *Designs, Codes and Cryptography*, vol. 86, no. 4, pp. 939–953, 2018.

[12] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.
[13] W. Qi and H. Xu, "On the linear complexity of FCSR sequences," *Applied mathematics-A journal of Chinese universities*, vol. 18, no. 3, pp. 318–324, 2003.
[14] L. Rudolf and N. Harald, *Introduction to finite fields and their applications*. Cambridge: Cambridge university press, 1994. ISBN: 9780521460941.
[15] C. Seo, S. Lee, and Y. Sung, "A lower bound on the linear span of an FCSR," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 691–693, 2000.
[16] L. Tan and W. Qi, "On the k-error linear complexity of l-sequences," *Finite Fields and Their Applications*, vol. 16, no. 6, pp. 420–435, 2010.
[17] T. Tian and W. Qi, "2-adic complexity of binary m-sequences," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 450–454, 2009.
[18] Q. C. Wang and C. H. Tan, "New bounds on the imbalance of a half-l-sequence," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2688–2691, 2015.
[19] N. Yerukala and V. Nalla, "Alternating step generator using FCSR and LFSRs: A new stream cipher," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 5, pp. 130–138, 2019.

Biography

Zhihua Niu was born in 1976 in Shanxi, China. She received the B.S. degree in Mathematics Education from Huaibei Normal University in 1998, and the M.S. degree in Computational Mathematics from Xi'an Jiaotong University in 2002, and the Ph.D. degree in Cryptography from Xidian University in 2005. She is now with the School of Computer Engineering and Science, Shanghai University, China. She worked as a visiting scholar supervised by Prof. Andrew Klapper in University of Kentucky(Lexington) during 2013-2014. Her research interests include pseudo-random sequences, cryptography and information security.

Yuqi Sang was born in 1996 in Henan, China. He was received the B.E. degree in Materials Science from Henan University of Science and Technology. He is now studying for a master's degree at the School of Computer Engineering and Science in Shanghai University.

An Overview on Network Security Situation Awareness in Internet

Wei Wu[1] and Cheng-Ying Yang[2]
(Corresponding author: Cheng-Ying Yang)
Wuhan Digital Engineering Institute[1]
Wuhan, Hubei, China
Department of Computer Science, University of Taipei[2]
Email: cyang@utaipei.edu.tw
(Received Dec. 21, 2021; Revised and Accepted Apr. 24, 2022; First Online Apr. 30, 2022)

Abstract

Network Security Situation Awareness is one of the most concerned research in the field of network security. According to the progressive relationship of the subject, it could be divided into three stages, the situation awareness, the situation evaluation and the situation prediction. With the accurately prediction of network security status in advance, the performance of internet service could be fundamentally improved and the evolution from the passive defense to the active defense could be realized. Therefore, the prediction of network security situation has become a popular research topic. This work summarizes and sorts out the meaning, situation awareness element extraction and the application with network security situation awareness to provide a reference for the relevant researchers in the security field.

Keywords: (2) Access Control; Network Security; Situation Awareness

1 Introduction

The infrastructure of internet has been continuously developing and the novel application with internet has been growing up and extending the networking scale. The topology and structure of internet becomes much complicate and leads the security concerns. Although the various schemes have been adopted for the secure protection, they could independently work for the isolated problem. Without integrating those problems existing in internet, the difficulties could not be systematically found. Network Security Situation Awareness (NSSA) [3] is a concept to integrate all available information and evaluates the security situation of the network. It could provide some security analyses to minimize the risks and to reduce the losses because of the unsafe factors. Upon the respects of monitoring capabilities and emergency response, NSSA benefits and contributes within the internet.

Internet has the characters of openness, interactivity and distribution. It makes human beings with the gratification in life including the information sharing, the openness and flexibility. However, many security issues are coming because of the convenience with internet. For example, the information leakage, the information pollution, the information uncontrollable, the information destruction, and the information infringement are fulfilling within our diary life. These unsafe concerns threaten the legitimate rights. In general, the network security could include two parts, the information security and the security control. The information security includes the integrity of information, the availability of information system, the confidentiality of information and the reliability of information [13]. On the other hand, the security control refers to the identity authentication, the non-repudiation, the authorization and the access control.

The following issues are the current network security problems [15].

1) The computer systems are infected and damaged because of virus.
   There were 73% of computers infected with viruses in 2001. The percentage went up to 83% in the first half of 2003. Among these infected computers, 59% of computers had more than 3 experiences of infection. There were 14% of data are destroyed because of virus, and 57% of data are partially damaged.

2) Hacker activities become an important threat for all computers.
   It makes the computers with fatal fragility and vulnerability. Up to date, almost of the network management centers connected to the internet have been attacked or invaded by hackers.

3) There exists challenges of network security to the information infrastructures.
   The network security system has many weaknesses in the ability of prediction, reaction, prevention and recovering. This situation belongs to the lowest abil-

ity of protection. The illegal activities in internet are increasing with a rate of 30% each year.

The internet is a dynamic system. With the changing of network structure and application, the principle of security police may fail. Corresponding to the real situation, the adjustments have been made in time. Some of the important network services are given in the following.

1) Communication Authentication:
The role of the communication authentication is to determine the identity of the users to prevent others from the interfering during the communication process. There are two authentication schemes, one is unilateral authentication where the user's identification is checked, and the other is mutual authentication to each other.

2) Access Control:
The access control service is to ensure that only authorized users can access the network and utilize resources. The principle of access control is to check user IDs, passwords, and limit the scope and extent of their use of resources according to the permissions granted.

3) Confidentiality:
The purpose of privacy services is to prevent the data to be read by unauthorized persons. The privacy includes both data in the storage and data in the transition. Security checks are applied on the specific files, the communication links, and the specified fields in the file.

4) Traffic Flow Analysis and Protection:
The role of the traffic flow analysis protection is to prevent the features of the flow, information length, and information source and destination information from being obtained by analyzing these characters.

5) Integrity:
The function of integrity protection is to protect the data in the storage and the transmission from being deleted, changed, inserted and duplicated, and the service could also include the recovery functions.

6) Signature:
The signature confirms as the receipt to certify and the acknowledge that the information is sent or received by the signatory. The purpose of signature is to avoid disputing between the communicating parties over the information source.

According to the specific goals of network security prediction, the relative researches could be divided to the following four categories [24].

1) Attack prediction – prediction for the next possible actions with the current occurring event.

2) Intention identification – prejudgment for the attacker's final intention after the occurrence of threat event.

3) Attack/intrusion warning—prediction the possible damage to the target network before the threat event occurring. It includes the types of attacks, the possible time and the specific location corresponding to the attacks.

4) Prediction of security situation – Prediction the trend of evolution of overall security state within the target network.

In general, the first two problems are hold in the processing of the occurrence of a threat event. After observing some certain behaviors of the threat event, the schemes predict the subsequent development with two different ways. They are two earliest concerns in network security situation prediction. The methods used with many similarities could be replaced by each other in some scenarios. The third question is to desire to move away from the threat event. It requires to warn for the threat event before it actually happens. The last question focuses on the macro security situation of the entire networks. It is no longer limited to the specific threat event or the local network area. The researches on the above four issues are described in the detail below. Due to the similarity of the first two issues, the following is given with a unified introduction.

The concept of attack behavior prediction and attack intent identification could be referred to 2001. Geib and Goldman [9] regarded the attack behavior prediction as an extension of the attack intent identification. They proposed for some prerequisites and existence of the problem. For example, the preceding activity of the threat event may not be directly observable, or multiple threat events may occur simultaneously. Then, the specific method for the attack behavior prediction and the attack intent identification were proposed. Beginning with that moment, the related researches became attractive. In this paper, it illustrates the idea of network security situation awareness in section 2. Section 3 gives the issue on the process of network security situation awareness. Especially, it points out the difficulty with big data in section 4. Section 5 gives the application of NSSA in the internet. Conclusions and the suggestions for the future research are given in the final.

2 Network Security Situation Awareness

Although there have been more and more studies on Situation Awareness (SA) in the recent years, it is still in the exploratory stage [14]. For the definition of SA, it not only with psychological, environmental and systemic explanations, but also with individual, perspective of groups descriptions. SA is still not yet formed a unified cognition. Endsley proposed the concept of SA in 1988, "under a certain time and space, recognize and understand environmental factors, and predict the future development

trend", and a three-component model consisting of situational element extraction, situational understanding and situational prediction [7]. This concept comes from the factors on the aerospace flight research. It mainly aimed at the individual SA. However, due to the characteristics of task dependence and collaborative communication among all members in the group, people began to study SA in the human being. Wellens proposed the concept of group SA [20], which was defined as "the common view of group members about current environmental events." However, there is still no unified definition of group SA. However, the group SA models proposed by Endsley *et al.*, Salas *et al.* [16] and Shu *et al.* [19] are widely used.

Based on the distributed cognition theory, Amman *et al.* [2] discussed SA from the system level and called it system-level SA. As the methods of system SA, the distributed SA is used to study for the group SA from the perspective of the system [17]. Initiation of knowledge related to the specific tasks, SA is the emergent feature from the interaction of various agents in the system. In addition to the above illustration, other researchers have proposed for their own understanding of SA, e.g. Uugerty [11] considered SA as a kind of knowledge and defines it as "a continuously updated, meaningful knowledge of unpredictable, multifaceted situations that the operators can use to made a decision when they participate in an instant multitasking." Unlike Endsley's opinion, it could argue that SA is a broader concept that should include both the focal and more automated environmental processes.

Dong *et al.* [6] believed that the situation is the synthesis of the state of things in a system which is complete and global status. Awareness is a cognitive mapping which bases on the data fusion and integration, the risk evaluation, the visualization and other related technologies. SA is a comprehensive understanding of environmental factors in the both time and space to predict the state after a period of time in the future and to achieve a reasonable decision-making process.

NSSA was inspired by the SA of aero-traffic control and applied the concept of SA to the field of network security. Batsell [4] and Shifflet [18] proposed the intrusion detection framework to SA. Since Bass proposed the concept of NSSA, many scholars have carried out the researches on NSSA in the further [3]. Jian Gong *et al.* systematically illustrated the definition of NSSA and the understanding of basic concepts [10].

Yan Li *et al.* [14] introduced the basic operating mechanism of NSSA and expounded the role of each link in the process of NSSA. Two fundamental models, the conceptual model of SA proposed by Endsley and the functional model and data fusion model proposed by Bass, led a foundation for the researches on NSSA. With concerning the increasingly complex internet, it is necessary to innovatively improve the NSSA model to realize the intelligent perception.

3 Process of Network Security Situation Awareness

The process of NSSA usually involves several different stages. According to the practical, some scholars use the method of classification in the engineering to process. Some scholars categorize the process with the conceptual level and some scholars sort the process base on the chain of data value. According to the logical analysis framework of SA, this paper introduces the three aspects of NSSA. It includes the network situation element extraction, the situation evaluation and situation prediction.

The extraction of network security situation elements is the basis on the network security situation research. In the element acquisition stage, security-related data should be obtained as effectively as possible. The extracted elements should be analyzed in a comprehensive manner. The main task of this stage is to obtain the data and to make a pre-process. The purpose of data preprocessing is to delete the redundant data, to extract more important situational elements, and to standardize the original data to provide a basis for situational evaluation and situational prediction [22].

Essentially, the acquisition of situational elements is used to classify the data in the network, and to determine whether each data is abnormal and to determine what kind of abnormality it belongs to if the abnormal data is found. The general classification algorithms include the decision tree, Bayesian rule, the artificial neural network, the support vector machine and the association rule-based classification.

The advantage of the principal component analysis in the network security situation feature element extraction is that the character of correlation among samples could be eliminated at the second stage. The compression of the original sample dimension could be realized. The independent component analysis method is a high-level process. It also plays an important role for the feature extraction. The principal component analysis and the feature extraction method function with their own advantages. However, the obtained low-dimensional feature data are lack of the identification information. They are not the most helpful data for classification. Recently, feature extraction with cluster analysis has also been widely studied in the detection for human intrusion. By dividing the data set into the different categories, the normal/ abnormal behaviors could be distinguished.

Network security situation evaluation is mainly to obtain the various monitoring data in the network. Network administrator could make decisions and prepare for protection according to the domain knowledge and the historical data with the network security feature and the comprehensive evaluation for network security status with the help of mathematical models. The core link of the NSSA is to correlate the extracted massive data related to the network security with a series of mathematical models and algorithms and to analyze the information of network se-

curity. Network security situation prediction refers to the forecast of network security situation change trend in the network environment in the future based on the current network security situation evaluation and the existing historical data. Situation prediction could provide the basis for the decision to the network managers. It could timely detect the security problems in the network and take the corresponding measures [8].

4 Network Security Situation Awareness with Big Data

Big data employs a network to collect, to store, to analyze, to calculate, to share and use the huge data. It is a huge nonlinear complex system. The complexity of big data is mainly reflected in the big number of nodes, the diversity of nodes, the diversity of connections, and the diversity of information. Because the network is with the characters of dynamic complexity, complex and changeable structure and multi-complexity fusion, the network with the big data has to face more security risks.

Big data has the characters of many sensing nodes, different types, diverse connections, and dynamic information. The most of the previous NSSA models belong to single-source mode or multi-source mode homogeneous models. Without the understanding of complex networks with big data, the models of NSSA are built up [5]. The existing NSSA models still exist shortcomings such as the heavy load, the large response delay, the poor integrity, the stability and the accuracy. The data comes from a variety sources and the types and formats of data are different. Also, because there are a lot of errors and the redundancy in the massive historical data, these data are not suitable for the analysis of NSSA directly. The dealt process of the amount of data with big data is more complicated. This complexity will affect the immediacy of the data fusion and the correlation analysis.

With big data, the factors that affect the network security are complex and diverse. There exist the correlations among the various security feature elements. The feature of the network security is with the mutual influence and the timely changing. It is very difficult to integrate and to process. The feature data extraction may be incomplete with fusing a large amount of network security data. The effect of feature dimensionality reduction might be difficult to evaluate and it might lead an inaccurate information. The correlation analysis and the process of huge security data are relatively complex. The efficiency of cloud-based distributed computing has to be improved.

The data of network security situation contain a large amount of uncertain information with big data [21]. They are incomplete, inaccurate and contradictory to a certain extent. The uncertain information in the process of situation evaluation needs to be solved. Recently, the researches on network security situation indicators are often aimed at a specific application, and there is no indexing and standard to describe the overall network security situation evaluation. The existence of many uncertain factors increases the complexity of network security measurement. The measurement of some indicators cannot be quantified directly but some can be quantified. However, these indicators could not be measured in detail. Therefore, it is necessary to construct a good index measurement to meet the feasibility of quantitative calculation of network security situation.

It is impossible to verify whether the network security situation indicators cover all the security evaluation with big data, and there is a lack of effective verification for the indicators. With big data, the massive security data change rapidly, and the selection of network security evaluations needs to reflect the network security situation timely and accurately. However, it could not be practical to obtain a real-time and accurate prediction of network security situation under the condition of exile dynamic model. The existing network security situation prediction relies on the data preprocessing and the manual intervention. Conversely, the data process is lack of the wisdom of learning of historical experience and knowledge. Network security prediction needs to be advanced studied in the future to improve the learning efficiency, the convergence speed, and the accuracy. With big data, the existing network security situation prediction is difficult to predict the time, the node location and the attack type. Also, it could not effectively support the accurate decision-making of network security active defense.

Recently, with the advent of big data, the researches on NSSA has been highly valued. These researches on the technology could enhance the efficiency of NSSA and improve the timeliness and accuracy of network security evaluation and prediction. Moreover, it could be better to ensure the network security with big data. In the future, with big data, the researches on the NSSA technology could be found as the following.

1) Research on the Network Security Situation Awareness model that is systematized, standardized, and valid to the different applications. Also, research on the self-adjusting, highly scalable and highly stable NSSA system, and find the key technologies for the security situation extraction, situation evaluation and situation prediction.

2) With big data, set up a set of effective, complete and measurable network security situation evaluation index with a standard system. Objectively, describe the comprehensive and accurate network security situation and provide a scientific basis for the situation evaluation and prediction.

3) Study deeply the characteristics of security with big data. Analyze the relationship of the feature elements of security among the huge data. Research on the extraction and analysis of the feature elements for the multi-source dynamic heterogeneous security with big data.

4) With big data, research on the measurement models and methods of network security. It includes the measurement functions, the analytical models and the decision criteria. Also, it needs the deep and comprehensive understanding of network security measurement system.

5) Learn from the various disciplines, including new methods and new ideas for quantitative evaluation of network security situation with big data, and research on the comprehensive, efficient and accurate thee network security situation evaluation with the characters of massive security data.

6) Research on the network security situation prediction technology based on the new generation of artificial intelligence science and technology. Apply these technologies to meet the security requirements of a large amount of data, dynamic change, high immediacy and high degree of coordination to supports the accurate decision-making in network security management and to provide the guidance for the active and dynamic defense of network security.

5 Internet Application

Due to the ubiquity and easy operation of internet, SA has a wide range of applications. With using the capability of powerful global monitoring to grasp the running status of the real-time network and take the corresponding security measures to ensure the network security. In internet, the situation information is extracted by using the firewall logs, the intrusion detection logs, the virus logs, the network scanning and other methods. Jirsik *et al.* [12] proposed the concept of network-wide Cyber SA as the specific domain of network SA. It focuses on the SA of computer networks and the factors considered are the network devices such as the switches and the routers. Its goal is to provide a deep understanding and to make the decision for the dynamic computer network. Alcaraz *et al.* [1] postulated a wide-area SA for the protection of critical infrastructure. With the wide-area SA approach for the dynamic protection, it monitors the performance of the critical infrastructure and takes the corresponding services. The framework proposed for the wide-area SA is based on the context awareness and the hybrid perspectives.

For the problems existing in the SA in the social network, Xiao Haidong *et al.* [23] proposed a method of intelligent SA. This method could effectively reduce the interference of the historical false alarm data and realize the automatic collection of SA data. It makes the SA more suitable for the small network and has the characteristics of the situation visualization.

Although a great progress has been made in the development of NSSA, the research is still in its infancy, and there are still many problems needed to be improved and solved. Regarding the future development, the followings are given for reference.

1) Expansion of Application:
In addition to the traditional threats such as viruses and malware, with the development of IoT, blockchain technology and digital currency, some emerging threats are developing rapidly. NSSA should not be limited to the traditional applications.

2) Combination with Big Data:
Adopt a variety of technologies based on big data such as the association merging, the fusion analysis and the deep mining. Combining with the hierarchical detection such as the agreement reduction identification, the static feature matching, the dynamic behavior analysis, and the abnormal behavior mining, the potential security threats could be detected from the discrete and isolated data.

3) Visualization Display:
Visualization technology could intuitively display the massive heterogeneous data and the processed results by NSSA. However, how to quickly, accurately, completely and effectively communicate with the security situation to the decision makers is still a very challenging problem.

6 Conclusion

This work describes the related work of NSSA, and introduces the origin, the existing definitions and the system models of the SA and the NSSA. The researches and the applications in the fields of NSSA are classified and summarized. The trend of development and the application prospects of NSSA are expected and some problems that still need to be solved and may be faced in the future.

1) The scope of application continues to expand.
Traditional network SA usually focuses on the conventional applications. Currently, with the ubiquity of network computing, the applications of network SA will be deeply extended to the mobile computing, the edge computing, the social computing, the opportunistic networks, the interplanetary networks and the other aspects.

2) The integration with new technologies.
Artificial intelligence, machine learning, etc., have become the important methods of SA because of their own advantages and characteristics. Big data, cloud computing, and IoT, etc. also provide new ideas for SA and become the application scenarios of SA. It will become an inevitable trend to apply technologies, such as blockchain and honeypots, to the SA. The combination of SA and other technologies will definitely bring a novel vitality to the field and provide new methods and inspirations for solving the problems in the SA. In general, the researches on NSSA

is still in its infancy. There are still many problems needed to be improved and solved. With the continuous improvement in the related researches, NSSA will definitely get greater development and give full play to its own advantages and characteristics to provide a strong guarantee for the internet security.

Acknowledgments

This work was partially supported by the Ministry Of Science and Technology, Taiwan (ROC), under contract no.: MOST 107-2221-E-845 -002 -MY3 and MOST 110-2221-E-845 -002.

References

[1] C. Alcaraz, L. Javier, "Wide-area situational awareness for critical infrastructure protection," *Computer*, vol. 46, no. 4, pp. 30-37, 2013.

[2] A. Anzanpour, I. Azimi, M. Götzinger, A. M. Rahmani, N. TaheriNejad, P. Liljeberg, "Self-awareness in remote health monitoring systems using wearable electronics," in *Proceedings of IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE'17)*, 2017.

[3] T. Bass, D. J. Gruber, "A glimpse into the future of ID," *The Magazine of USENIX & SAGE*, vol. 24, no. 3, pp. 40-49, 1999.

[4] S. G. Batsell, N. S. Rao, M. Shankar, "Distributed intrusion detection and attack containment for organizational cyber security," *Cyber and Information Security Research*, 2005.

[5] E. Bou-Harb, M. Husák, M. Debbabi, C. Assi, "Big data sanitization and cyber situational awareness: a network telescope perspective," *IEEE Transactions on Big Data*, vol. 5, no. 4, pp. 439-453, 2017.

[6] Z. Dong, T. Xu, Y. Li, P. Feng, X. Gao, X. Zhang, "Review and application of situation awareness key technologies for smart grid," in *Proceedings of 2017 IEEE Conference on Energy Internet and Energy System Integration*, pp. 1-6, 2017.

[7] M. R. Endsley, S. J. Selcon, T. D. Hardiman, D. G. Croft, "A comparative analysis of SAGAT and SART for evaluations of situation awareness," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 42. no. 1, 1998.

[8] L. I. Fangwei, L. I. Qi, Z. H. U. Jiang, "Improved method of situation assessment method based on hidden Markov model," *Journal of Computer Applications*, vol. 37, no. 5, pp. 1331, 2017.

[9] C. W. Geib, R. P. Goldman, "Plan recognition in intrusion detection systems," in *Proceedings DARPA Information Survivability Conference and Exposition II (DISCEX'01)*, IEEE, vol. 1, pp. 46-55, 2001.

[10] J. Gong, X. Jain, Q. Su, "Overview of network security situational awareness," *Journal of Software*, vol. 28, no. 4, pp. 1010-1026, 2017.

[11] L. Gugerty, "Situation awareness in driving," *Handbook for Driving Simulation in Engineering, Medicine and Psychology*, pp. 265-272, 2011.

[12] T. Jirsik, C. Pavel, "Toward real-time network-wide cyber situational awareness," in *Proceedings of IEEE/IFIP Network Operations and Management Symposium*, 2018.

[13] K. Lai, Y. Wang, "Research on the application of neural networks to the security and risk assessment of information," *International Journal of Digital Content Technology and Its Applications*, vol. 6, no. 9, pp. 132-140, 2012.

[14] Y. Li, G. Q. Huang, C. Z. Wang, Y. C. Li, "Analysis framework of network security situational awareness and comparison of implementation methods," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1-32, 2019.

[15] G. Lu, D. Feng, "Situational awareness modeling of industrial control network based on particle filter," *Chinese Journal of Automation*, vol. 44, no. 8, pp. 1405-1412, 2018.

[16] E. Salas, C. Prince, D. P. Baker, L. Shrestha, "Situation awareness in team performance: Implications for measurement and training," *Human Factors*, vol. 37, no. 1, pp. 123-136, 1995.

[17] P. M. Salmon, N. A. Stanton, G. H. Walker, D. P. Jenkins, *Distributed Situation Awareness: Theory, Measurement and Application to Teamwork*, Taylor & Francis eBooks, 2017.

[18] J. Shifflet, "A technique independent fusion model for network intrusion detection," in *Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mat hematics*, vol. 3, no. 1, pp. 1-3, 2005.

[19] Y. Shu, F. Kazuo, "An inference method of team situation awareness based on mutual awareness," *Cognition, Technology & Work*, vol. 7, no. 4, pp. 272-287, 2005.

[20] A. R. Wellens, "Group situation awareness and distributed decision making: From military to civilian applications," *Individual and Group Decision Making: Current Issues*, pp. 267-291, 1993.

[21] J. Wu, K. Ota, M. Dong, J. Li, H. Wang, "Big data analysis-based security situational awareness for smart grid," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 408-417, 2016.

[22] J. Wu, L. Yin, Y. Guo, "Cyber attacks prediction model based on Bayesian network," in *Proceedings of IEEE 18th International Conference on Parallel and Distributed Systems*, 2012.

[23] H. Xiao, N. Chen, "Analysis of smart situational awareness of mobile social information," *Science in China (Information Science)*, vol. 45, no. 6, pp. 783-795, 2015.

[24] S. Zhang, Y. Shen, G. Zhang, "Network security situation prediction model based on multi-swarm chaotic particle optimization and optimized grey

neural network," in *IEEE 9th International Conference on Software Engineering and Service Science (ICSESS'18)*, pp. 426-429, 2018.

Biography

Wei Wu studied at Chung Buk National University from 2008 to 2011, majored in Political Diplomacy, and obtained a master's degree. In 2011, entre Wuhan Digital Engineering Institute. The title is an engineer.

Cheng-Ying Yang received an M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and a Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of the IEEE Satellite & Space Communication Society. Currently, he is employed as a Professor at the Department of Computer Science, University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing, and computer security.

Fine-grained Access Control Scheme Supporting Cloud-assisted Write Permission Control in Cloud-aided E-Health System

Kai He[1,3], Ziqi Wang[1,3], Jiaoli Shi[2], Anyuan Deng[2], and Shunlin Lv[2]
(Corresponding author: Jiaoli Shi)
School of Computer Science and Artificial Intelligence, Wuhan Textile University[1]
School of Computer and Big Data Science, Jiujiang University[2]
407081693@qq.com
3 Hubei Clothing Information Engineering Technology Research Center, China[3]
(Received July 30, 2021; Revised and Accepted Jan. 28, 2022; First Online Apr. 2, 2022)

Abstract

We consider a multi-reader-multi-writer scene in cloud-aided E-Health systems. Data is produced on all kinds of medical devices and encrypted to ciphertexts for security. These pieces of ciphertext would be aggregated as an electronic medical records file on controllers and uploaded onto the cloud. Doctors then download and decrypt the encrypted file, make diagnoses and treatment plans, and write them in the encrypted file. Nurses implement real-time treatment plans and record progress in the same file. This paper proposes a Fine-grained Access Control Scheme supporting Cloud-assisted Write Permission Control. In this scheme, multiple authorized users can read the same file but cannot write files until they are appropriate. We represent Users' statuses as a matrix and use a Viète formula to match them with a write access policy on the cloud to judge whether the user can modify the file or not.

Keywords: Attribute-based Encryption; Fine-grained Access Control; Write Permission Control

1 Introduction

With the fast development of cloud services, cloud-based PHR (personal health record) systems becomes popular more and more, such as Google Health and Microsoft HealthVault. In these PHR systems, lightweight medical devices and controllers are deployed gradually in hospital or home, and users can access PHR services anytime and anywhere. In the scene, most security issues stem from the plaintext transmission of data. Thus, the data need to be encrypted to be ciphertext before being sent to the controller.

These pieces of ciphertext then would be aggregated as an electronic medical records file on controllers and uploaded onto the cloud. Doctors then download and decrypt the encrypted file, make diagnoses and treatment plans, and write them in the encrypted file. Accordingly, nurses implement real-time treatment plans and record progress in the same file. This scenario is called Multi-Reader-Multi-Writer by us.

It is troublesome to carry out access control over a wide variety of data generated by all kinds of devices. Fortunately, ABE (Attribute-Based Encryption) may be the most suitable method. When the ABE method is adopted, the judgment of reading permission is in the user, while the control of write permission is generally migrated to the cloud server by the owners. On the one hand, owners want a cloud server to realize aggregating privilege control. However, on the other hand, the cloud server cannot get out anything about the ciphertext.

Our contributions can be summarized as follows.

1) We propose a fine-grained access control scheme supporting multiple authorized users to write the same encrypted medical record file. In this scheme, the encrypted file can be read by multiple users who have authorized read rights and can be modified by some doctors or nurses who has authorized write rights and be in an appropriate status (such as at work).

2) We present a representation and matching method of users' statuses. Users' statuses represent as a Matrix and match on the cloud by using the Viète formula to judge whether the user can modify the file or not.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 gives the system architecture. Section 4 demonstrates the construction. Section 5 presents all kinds of analyses. Section 6 demonstrates the efficiency of our proposed scheme. Finally, Section 7 concludes the paper. This paper concretizes the application scenario of our scheme, stores a medical records file using blockchain, and extends several parts over its earlier version [2]. These extended parts include

security model and formal proof, correctness analysis, performance analysis, *et al.* What is more, and we adjusted simulation.

2 Related Works

Fugkeaw *et al.* [4] presented a write access enforcement mechanism based on the proxy re-encryption method, in which users may have permission to update files stored on the cloud. Despite the data owner freeing from encrypting files to be updated and loading back to the cloud, the cloud servers asked the user to enter the passphrase to decrypt and re-encryption file.

Dong *et al.* [3] designed a SECO (Secure and scalable data collaboration services) scheme in cloud computing, in which the latest version of written data was decided by early in early write principle. Ruj *et al.* [15] compelled that data is written by a single user at a time using Claim Policy. Li *et al.* [13] only considered the Create-Writing situation. They divided time into slices and controlled write permission using Hash chain and signature.

Jahan *et al.* [7] extended the CP-ABE scheme to support write operation with coarse-grained write access. Fugkeaw *et al.* [5] represented read and write access privilege as an attribute of a user. Jahan *et al.* [9] provided authorized users with fine-grained read/write access without altering access policies specified by data owners.

Lee *et al.* [11] used attribute-based encryption as Self-updatable encryption (SUE) and presented revocable-storage attribute-based encryption (RS-ABE) by combining user revocation and ciphertext updating functionalities. Yang *et al.* [19] allow patients' vital signs to be measured and aggregated on medical devices and uploaded on a cloud for storage and healthcare workers access. They mainly focused on the lightweight break-glass access control system and did not investigate the aggregating privilege control. Wang *et al.* [17] proposed an RWAC (read and write access control) scheme, in which the write control was done on a user using the CP-ABE method. Jahan *et al.* [8] also agreed on a drawback of CP-ABE. Users can modify the access policy specified by the data owner if write operations are incorporated in the scheme. However, their scheme enabled the users to perform write operations without altering the access policy. Their write control was still done on a user. Alam [1] mentions five platforms to develop IoT systems using blockchain technology. They are IOTA, IOTIFY, Exec, Xage and SONM. IOTA solves various performance limitations of blockchains. IOTIFY provides an online web solution. Exec helps users' applications to the benefits of the cloud used. Xage is a secure IoT blockchain platform for adding automation. SONM is a medium-sized fog computing platform.

Many Cloud Service Providers (CollateBox, Microsoft Azure, Windows Azure, Google docs, Amazon S3, etc.) also allow multiple writers in one file, although most of them use role-based access control (RBAC), which is a centralized method to control the access of shared documents.

3 System Architecture

3.1 System Model

As shown in Figure 1, there are six entities in the system: AA (attribute authorities), Server (cloud servers), Medical devices, Controller (the data controller), Reader (data readers, such as patients or their families), and Writer (data modifier, such as doctors or nurses). We assume that: a) AA and Controller are trusted. b) Cloud is semi-trusted, which will execute all tasks correctly but is curious about ciphertexts' content. c) Unauthorized readers cannot read an out-sourced ciphertext, and unauthorized writers cannot write a ciphertext. Readers can read the ciphertext but cannot write it. Writers can read or write it.

AA (Trusted Attribute Authorities). They generate a public parameter set, and then generate, issue, revoke and update three keys (a global private key GSK_{u_t}, a global public key GPK_{u_t}, and a private attribute key SK_{u_t}) for each user called u_t in this paper. With GSK_{u_t}, users can make a digital signature to ensure data integrity. Using the private key SK_{u_t}, Readers can read out-sourced ciphertext if his/her attributes meet the read policy defined in the ciphertext. With SK_{u_t}, Writers can read and modify out-sourced ciphertext if his/her attributes meet the write policy defined in the ciphertext.

Medical Devices. They monitor the body's various parameters data (called M by us) and encrypt them to be Cm by running a certain symmetric encryption algorithm with a content key $Key_{content}$. The symmetric key $Key_{content}$ was negotiated in advance between the medical devices and their controllers.

Controller. It receives Cm from medical devices and encrypts the content key to Cp by running a CP-ABE encryption algorithm with a read policy defined by himself/herself. Next, Controllers defines a write policy (X, Y) and encrypts it with a part of Cp to Ct. As a result, the encrypted electronic health record file ($Cm||Cp||Ct$) is constructed and uploaded on Server.

Reader of an Out-Sourced Data. Anyone can download an encrypted electronic health record file from a cloud server and tries to read it by matching his/her private key SK_{u_t} to the read policy in Cp. If the match succeeds, he/she can get the content key and decrypt the encrypted electronic health record file to the plaintext data M.

Writer of an Out-Sourced Data. Any writer can download and read a ciphertext if his SK_{u_t} matches

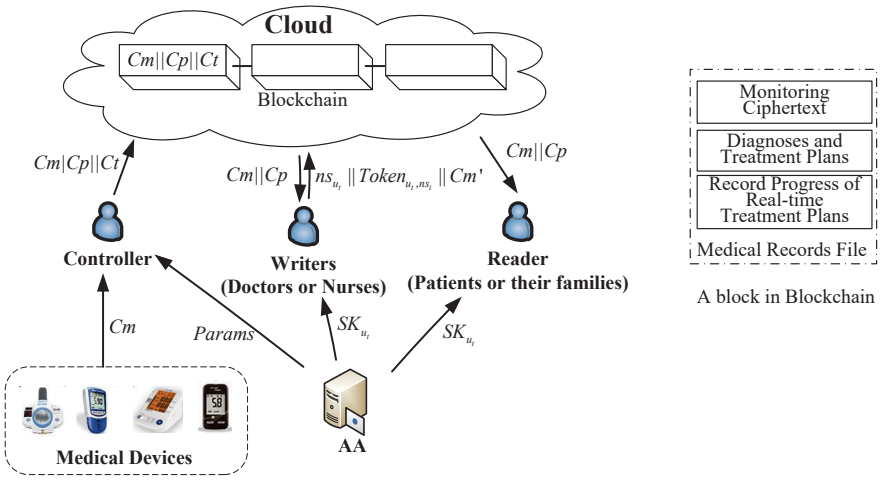


Figure 1: System Model

successfully to the read policy in Cp. Next, he/she may modify the plaintext data M and encrypts it to Cm' with the content key. Then he/she signs his/her write credential $ns_{u_t}||Token_{u_t,ns_i}$ with his/her global private key GSK_{u_t} and uploads the result and Cm' on Server.

Server. The semi-trusted cloud server in cloud-aided E-health system is always online, stores all encrypted electronic health record files submitted by controllers, and provides data access services anytime and anywhere. Let ns_{u_t} denotes the user's status of written data, ns_i the status vector of users' access,$Token_{u_t,ns_i}$ the write credential. When Writer uploads a writing request $ns_{u_t}||Token_{u_t,ns_i}||Cm'$, Server stores the user's status ns_{u_t}, and tries to match Ct with $ns_{u_t}||Token_{u_t,ns_i}$ and other users' statuses saved before. Suppose the match succeeds (means that the write policy is satisfied), Server updates Cm with Cm'. Otherwise, Server records the user's status ns_{u_t} and ignores the request. What is more, Server can be realized by a cluster of multiple servers not to make a bottleneck or a single point of failure in the system.

3.2 Security Requirements

Data Confidentiality. Unauthorized users or cloud servers (which are semi-trusted) should be prevented from accessing the plaintext of the data. This is because that they do not have enough attributes to satisfy the read access policy.

Collusion Resistance. Multiple users cannot improve the ability to decrypt a ciphertext by combining their attributes. It is assumed that doctors or nurses will not share their write credentials with others for their good.

Semi-Hiding and Unpredictability. Cloud servers will complete the match of the writing policy faithfully without knowing the details of write policies or write credentials. They also cannot predict whether or not a user's request writing data is accepted.

3.3 Security Model

We define the security for our scheme in terms of a game as follows:

Setup.

The challenger runs the algorithm $Setup$ to generate public parameters $params$ and a master secret key MSK. Then, he publishes the $params$ to an adversary Λ.

Phase 1.

The adversary Λ can submit a challenge (X^*, Y^*) to the challenger, and construct his/her $Token_{u_t,ns_i}$. When Λ queries User u_t on State ns_i, the challenger signs $Token_{u_t,ns_i}$ using GSK_{u_i}, and issues them to Λ.

Challenge.

The adversary Λ gives a challenge (X, Y), which must be satisfied with $X^* \cup X - X^* \cap X \geq 2$ *or* $Y^* \cup Y - Y^* \cap Y \geq 2$. Ct is constructed and sent to Λ, and then matched with $Token_{u_t,ns_i}$.

Phase 2.

Λ can query and construct more $Token_{u_t,ns_i}$, as long as they do not violate the constraints on the challenge (X^*, Y^*).

Guess.

Λ outputs a guess (X^*, Y^*) of (X, Y).

The advantage of an adversary Λ in this game is defined as:

$$Pr[X^* = X \wedge Y^* = Y] = 0.5$$

This completes the security game.

4 Proposed Scheme

4.1 Overview

When CP-ABE is used to control the access to medical record files in E-Health systems, the data generated by monitor devices should be uploaded onto the cloud immediately after being encrypted. The encrypted data is sent to a controller to be aggregated into a medical record file. The file is bound with a read policy and a write policy, uploaded on the cloud, and stored in blockchain. Then doctors or nurses can download the encrypted medical record file to make diagnoses and treatment plans or record the progress of real-time treatment plans remotely. These plans or progress are also uploaded onto the cloud and stored in the medical record file.

In the above scene, monitor devices, controllers, doctors, or nurses cannot always be online or restore massive data. Due to their limited storage ability or may only carry a lightweight mobile terminal,these data are usually uploaded on the cloud and downloaded when read or written by users. Then Server can process the written data by two methods:

1) *According to the content of data* (the first method). The data owner verifies and decides the latest version of written data submitted by multiple users according to the data content. Based on this method, we construct two collaborative access control schemes (see the previous research [10]).

2) *According to the write access policy of data* (the second method). Server decides the latest version of written data according to the write policy defined by Owner. In addition, Owner can specify an arbitrary on-demand policy to ensure data consistency. Based on the second method, this work constructs a new Access Control Scheme supporting Ciphertext Writing Privilege Management in Cloud-aided E-Health System.

In our scheme, the writer (doctors or nurses) can read the monitoring record file, make diagnoses and treatment plans, and write them in the medical records file. In contrast, nurses implement real-time treatment plans and record progress in the same medical records file. These writers can write these data to the medical records file and form an updated file M'. Then they encrypt M' to Cm' by symmetric encryption and upload the Cm' on the cloud along with their write access credentials $ns_{u_t}||Token_{u_t,ns_i}$. To prevent imitate attack, these writers sign $ns_{u_t}||Token_{u_t,ns_i}||Cm'$ with their global private key GSK_{u_t}. Subsequently, $Sign(ns_{u_t}||Token_{u_t,ns_i}||Cm')_{GSK_{u_t}}$ is sent to the cloud as a writing request.

When the writing request arrives in Server, Server firstly verifies the signature using the user's global public key GPK_{u_t} and then matches $ns_{u_t}||Token_{u_t,ns_i}$ to Ct. If the match is successful, Server covers Cm with Cm'. Otherwise, Server ignores the writing request. For convenience, we put aside the realization of concurrent mechanisms. Each write success triggers a blockchain transaction event so that the write operation can be recorded on blockchain and cannot be tampered with.

To facilitate the research, let us focus on the write privilege control and make a quick summary. To control the collaborative writing on a single file by multiple writers, Controller defines a write policy, constructs Ct by associating the policy with the ciphertext, and sends Ct and the ciphertext onto Server together. Server then aids Controller to match the collaborative write policy with the writer's write credential when a writer submits a writing request.

Our scheme addresses two issues:

1) Designing the structure of Ct and the writer's write credential.

2) Judging whether or not the writer's write credential is satisfied with Ct (that is, match of Ct).

4.2 Structure of Ct

Inspired by [14], we design a new access structure of Ct, wherein writers' statuses may be input manually or generated automatically.

Let $u_c s_d|u_a s_b$ indicate the relationship between a device u_c and Status s_d when another device u_a accesses data in the status s_b. Let $u_c s_d|u_a s_b = \{-1, +1, ^*\}$. $u_c s_d|u_a s_b = -1$ indicates that the device u_a can access data in the status s_b only if u_c has ever been in the status s_d.$u_c s_d|u_a s_b = +1$ indicates that u_a can access data in the status s_b only if u_c is being in the status s_d. s_d.$u_c s_d|u_a s_b = *$ indicates that there is not any constraint in $u_c s_d$ when the user u_a accesses data in the status s_b.

Let Nu denotes the number of writers, Ns the number of statuses, and $N = Nu \cdot Ns$. The access structure can be described by a matrix Ms (shown in Figure 2).

When the writer u_a writes data in the status s_b, the access structure, expressed as a line of Matrix Ms, must be satisfied by other writers' statuses. Therefore, we extract all of the elements of the line of Ms, and construct a vector $\overrightarrow{m}_{line_{a,b}}$, wherein $line_{a,b} = (a-1) * Ns + b$.

For instance, let $Nu = 3$, and $Ns = 4$. The vector $\overrightarrow{m}_1$ (the first line of Ms) is assumed as: $\overrightarrow{m}_1 = (1, *, *, *, *, *, *, *, *, *, *)$. It denotes that User u_1 can write the data in Status s_1 with independence of other writers or their statuses. The vector $\overrightarrow{m}_{12}$ (the latest line of Ms) is assumed as: $\overrightarrow{m}_{12} = (-1, *, -1, 1, *, *, *, *, *, *, -1, 1)$. It denotes that the writer u_1 has ever been in the status s_1 and the status s_3, the writer u_3 has ever been in the status s_3, while both u_1 and u_3 are being in the status s_4, when the writer u_3 writes the data in the status s_4.

According to different values of $\overrightarrow{m}_{line}$, we construct three sets: X, Y and P, wherein, the elements of

$$\begin{bmatrix} u_1s_1 \,|\, u_1s_1 & \cdots & u_1s_{Ns} \,|\, u_1s_1 & u_2s_1 \,|\, u_1s_1 & \cdots & u_{Nu}s_{Ns} \,|\, u_1s_1 \\ u_1s_1 \,|\, u_1s_2 & \cdots & u_1s_{Ns} \,|\, u_1s_2 & u_2s_1 \,|\, u_1s_2 & \cdots & u_{Nu}s_{Ns} \,|\, u_1s_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ u_1s_1 \,|\, u_{Nu}s_{Ns} & \cdots & u_1s_{Ns} \,|\, u_{Nu}s_{Ns} & u_2s_1 \,|\, u_{Nu}s_{Ns} & \cdots & u_{Nu}s_{Nm} \,|\, u_{Nu}s_{Ns} \end{bmatrix}$$

Figure 2: Access Structure of User Status Constraints

$X = \{x_i\}$ and $P = \{p_k\}$ are respectively the positions of +1, -1 and * in $\overrightarrow{m}_{line}$. For example, when $\overrightarrow{m}_{12} = (-1, *, -1, 1, *, *, *, *, *, *, -1, 1)$,$X = \{4, 12\}$,$Y = \{1, 3, 11\}$, and $P = \{2, 5, 6, 7, 8, 9, 10\}$.

4.3 Structure of the Write Credential

The write credential is designed as a monitor vector of a writer status consists with multiple elements of $u_a s_b$. $u_a s_b = +1$ denotes that the writer u_a is being in the status s_b, $u_a s_b = -1$ denotes that the writer u_a has ever been in the status s_b, and $u_a s_b = 0$ denotes that the writer u_a hasn't ever been in the status s_b.

Let $\vec{r}_a = (u_a s_1, u_a s_2, \cdots u_a s_{Ns})$, and $\vec{r} = (\vec{r}_1, \vec{r}_1, \cdots \vec{r}_N)$ can be described as follows.

$$\vec{r} = (u_1s_1, u_1s_2, \cdots u_1s_{Ns}, u_2s_1, u_2s_2, \cdots u_2s_{Ns}, \cdots u_{Ns}s_1, u_{Ns}s_2, \cdots u_{Ns}s_{Ns})$$

The number of elements of $\vec{r}$ is N:$|\vec{r}| = N$.

For example, $\vec{r} = (-1, -1, 0, 1, -1, 0, 0, 1, 0, -1, -1, 1)$. $\vec{r}_1 = (-1, -1, 0, 1)$ denotes that the writer u_1 has ever been in the status s_1 and s_2, and is being in the status s_4 now.

According to the values of different elements of $\vec{r}$, two sets can be constructed as: X' and Y'. The elements of $X' = \{x_i\}$ are positions of +1 in $\vec{r}$, and those of $Y' = \{y_i\}$ are positions of -1 in $\vec{r}$. For instance, $\vec{r} = (-1, -1, 0, 1, -1, 0, 0, 1, 0, -1, -1, 1)$, $X' = \{4, 8, 12\}$ and $Y' = \{1, 2, 5, 10, 11\}$.

4.4 Intuition of Matching Ct

Whether $\vec{r}$ is satisfied to $\vec{m}_{line}$ is the same as whether $X \subseteq X' \wedge Y \subseteq Y'$ is valid, wherein, $X \subseteq X'$ is equivalent to $X = X' - P$, and $Y \subseteq Y'$ to $Y = Y' - P$. In the above example, $X' - P = \{4, 12\}$, $Y' - P = \{1, 11\}$.

Inspired by [14], we use Viète formula on the wildcard set P to construct a proper coefficient a_j in Formula (1).

$$\prod_{p_\tau \in P} (x - p_\tau) = \sum_{l=0}^{n_p} (a_l \cdot x^l) \tag{1}$$

where, $p_\tau, a_l \in Z$, n_p denotes the number of elements in P, and $n_p \leq N$.

The coefficient a_l can be constructed by Viète Formula (2) as follows.

$$a_{n-t} = (-1)^t \sum_{1 \leq k_1 < k_2 < \ldots < k_t \leq n} p_{i_1} p_{i_2} \cdots p_{i_t} \tag{2}$$

We can get Formula (3) when replacing x of the above Formula (1) with $i = 1, 2, 3..., n_X$ and cast them up.

$$\sum_{i=1,2,3...,n_X} \prod_{p_\tau \in P} (i - p_\tau) = \sum_{i=0}^{n_p} (a_l \cdot \sum_{i=1,2,3...,n_X} i^l) \tag{3}$$

Based on Formula (3), we construct our scheme.

4.5 Sketch of Scheme

Our scheme includes three parts and four algorithms, which are described in Figure 3. To keep things simple, we focus on the write privilege control, especially matching a write credential to a write policy Ct.

Initialization. AA calls the algorithm *Setup* to generate a global public parameter set (*params* called by us) and a master private key MSK, and publishes it. Then AA generates three keys for each user: a global private key GSK_{u_t}, a global public key GPK_{u_t} and a private attribute key SK_{u_t}. AA sends GSK_{u_t} and SK_{u_t} to User by a key exchange protocol. SK_{u_t} is not marked in Figure 3, because that it was irrelevant with the write privilege access control.

Write Policy Definition. Owner defines a collaborative write policy, calls the algorithm *EncryptCt* to construct Ct, and uploads it onto Server. Server attaches Ct behind $Cm||Cp$, and then $Cm||Cp||Ct$ is stored.

Data Write. When a user writes data, he/she signs $ns_{u_t}||Token_{u_t,ns_i}||Cm'$ with his/her global private key GSK_{u_t}, and submits it onto Server. Then Server verifies $ns_{u_t}||Token_{u_t,ns_i}||Cm'$ with the user's global public key GPK_{u_t}, and runs the algorithm $MatchCt$ to match Ct. If the match succeeds, Server accepts the written data, and updates Cm to Cm'.

4.6 Construction of Our Scheme

In this section, we describe in detail our scheme. As introduced in Section above, our scheme has four algorithms: Setup, *EncryptCt*, *TokenGen* and *MatchCt*.

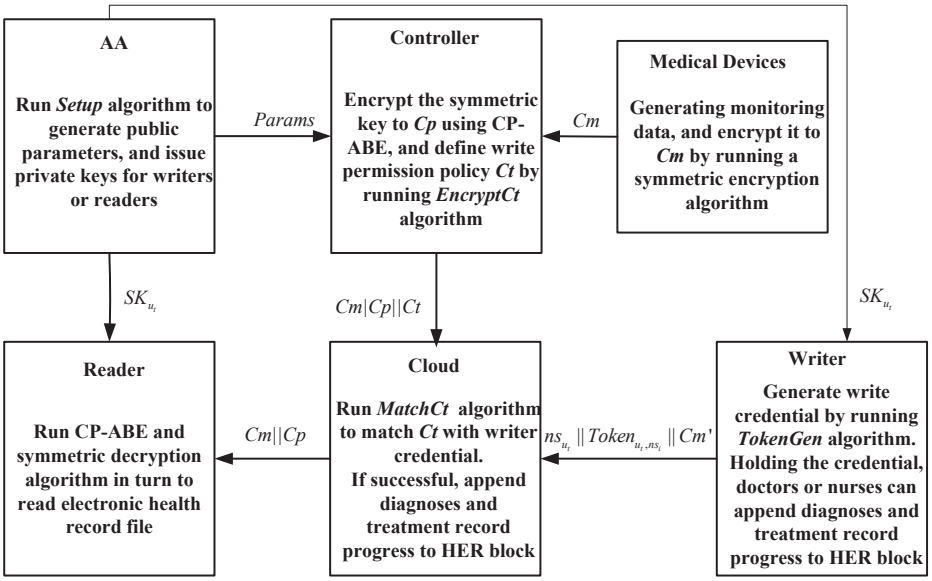


Figure 3: Sketch of our scheme

4.6.1 Setup

The algorithm *Setup* runs on AA. It chooses two group elements: $h_0, g \in G_q$ wherein G_q is a group with a prime order q. It also chooses $N+4$ random numbers: $\alpha_1, \beta_1, \beta_2, \delta, \delta_1, \delta_2, ..., \delta_N \in Z_q^*$, and computes:

$$\Omega_1 = e(g, h_0)^{\alpha_1 \beta_1},$$
$$\Omega_2 = e(g, h_0)^{\alpha_1 \beta_2},$$
$$\{h_w = h_0^{\delta_w}\}_{w=1}^{N}, \{\tilde{x}_w = g^{\delta^{x_w}}\}_{w=1}^{N}, \{\tilde{y}_w = g^{\delta^{y_w}}\}_{w=1}^{N}.$$

Then AA publishes public parameters and stores the master secret key MSK as follows:

$$params = (\{h_w, \tilde{x}_w, \tilde{y}_w\}_{w=0}^{N}, g^{\alpha_1}, \Omega_1, \Omega_2, q, G, e(.,.), g^{\delta}),$$
$$MSK = (\alpha_1, \beta_1, \beta_2, \delta, \delta_1, \delta_2, ..., \delta_N)$$

4.6.2 EncryptCt

The algorithm *EncryptCt* runs on a controller to construct *User Status Constraints*, the write policy Ct. The controller chooses two random numbers $\mu_1, \mu_2 \in Z_q^*$, and constructs Ct as follows.

$$\begin{aligned}
Ct &= (Ct_0, \{Ct_{1,w}\}_{w=0}^{n_P}, \{Ct_{2,w}\}_{w=0}^{n_P}, Ct', Ct''),\\
Ct_0 &= \Omega_1{}^{\mu_1} \Omega_2{}^{\mu_2},\\
Ct_{1,w} &= (h_w \cdot \prod_{i=1, x_w \in X}^{n_X} g^{i^w \cdot \delta^{x_w}})^{a_w \cdot (\mu_1 + \mu_2)},\\
Ct_{2,w} &= (h_w \cdot \prod_{i=1, y_w \in Y}^{n_Y} g^{i^w \cdot \delta^{y_w}})^{a_w \cdot (\mu_1 + \mu_2)},\\
Ct' &= g^{\alpha_1, \mu_1},\\
Ct'' &= g^{\mu_2}
\end{aligned}$$

Wherein, $\{a_w\}$ is computed by (2). Then the controller sends Ct onto the cloud, and stores it on the cloud.

4.6.3 TokenGen

The algorithm *TokenGen* runs on a writer (a doctor or nurse) to generate a write access credential.

We encrypt the set P concatenating with the content key $Key_{content}$:

$$\hat{C} = (Key_{content} || P) \cdot e(g, g)^{\alpha \cdot s}$$

We assume that these writers who possess reading permission can get the set P by decrypting $policy_{read}$. It is a reasonable assumption because that if writers can get the plaintext M, they will know which users or statuses the plaintext M it is related to.

When a writer makes a writing request, he/she computes $\theta = \sum_{w=0}^{n_P} \delta_w \cdot a_w$ based on P and Viète formula, chooses a random number $s \in Z_q^*$, and constructs $Token_{u_t, ns_t}$:

$$\begin{aligned}
Token_{u_t, ns_t} &= \left(\tilde{S}_0, \tilde{S}_1, \tilde{S}_2, \tilde{S}_3, \tilde{S}_4, P\right),\\
\tilde{S}_0 &= g^{\frac{\alpha_1 \cdot s}{\theta}},\\
\tilde{S}_1 &= h_0^{s_1} \cdot \prod_{\substack{i=1,2,\cdots,n_X \\ x_i \in X' - P}} g^{\frac{s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{x_i},\\
\tilde{S}_2 &= h_0^{\alpha_1 s_2} \cdot \prod_{\substack{i=1,2,\cdots,n_X \\ x_i \in X' - P}} g^{\frac{\alpha_1 \cdot s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{x_i},\\
\tilde{S}_2 &= h_0^{\alpha_1 s_2} \cdot \prod_{\substack{i=1,2,\cdots,n_X \\ x_i \in X' - P}} g^{\frac{\alpha_1 \cdot s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{x_i},\\
\tilde{S}_4 &= h_0^{\alpha_1 \cdot s_2} \prod_{\substack{i=1,2,\cdots,n_Y \\ y_i \in Y' - P}} g^{\frac{\alpha_1 \cdot s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{y_i}.
\end{aligned}$$

4.6.4 MatchCt

The algorithm $MatchCt$ runs on Server (any of cloud servers) to match Ct. Server calculates ρ based on P by the Viète formula: $\rho = \{a_w\}_{w=0}^{n_p}$, and computes M_1 and M_2 as below.

$$M_1 = Ct_0 \frac{e(\tilde{S}_0, \prod_{w=0}^{n_P} (Ct_{1,w})^{a_w})}{e(\tilde{S}_1, Ct') \cdot e(\tilde{S}_2, Ct'')},$$
$$M_2 = Ct_0 \frac{e(\tilde{S}_0, \prod_{w=0}^{n_P} (Ct_{2,w})^{a_w})}{e(\tilde{S}_3, Ct') \cdot e(\tilde{S}_4, Ct'')}$$

If M_1 and M_2 are both 1 ($M_1 = M_2 = 1$), the writing policy is satisfied. Otherwise, the cloud server ignores the writing request.

In our scheme, AA and Server must be online all the time, but others don't need to be.

5 Analysis

5.1 Correctness Analysis

The detail analysis is presented as below.

$$\begin{aligned}
M_1 =& Ct_0 \frac{e(\tilde{S}_0, \prod_{w=0}^{n_P} (Ct_{1,w})^{a_w})}{e(\tilde{S}_1, Ct') \cdot e(\tilde{S}_2, Ct'')}, \\
part1 \stackrel{def}{=}& e(\tilde{S}_0, \prod_{w=0}^{n_P} (Ct_{1,w})^{a_w}) \\
=& e\left(g^{\frac{a_1 \times s}{q}}, \left(h_0^q \times g^{\sum_{w=1}^{n_P} \left(\sum_{i=1}^{n_X} i^w \times d^{x_i} \times a_w\right)}\right)^{m_1+m_2}\right) \\
=& e(g, h_0)^{\alpha_1 \cdot s \cdot (\mu_1+\mu_2)} \\
& \cdot e(g, g)^{\frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1+\mu_2) \cdot \sum_{w=1}^{n_P} \left(\sum_{i=1}^{n_X} i^w \cdot \delta^{x_i} \cdot a_w\right)}, \\
part2 \stackrel{def}{=}& e(\tilde{S}_1, Ct') \\
=& e\left(h_0^{(s+\beta_1)} \cdot g^{\sum_{i=1}^{n_X} \left(\frac{s}{\theta} \cdot \prod_{\tau=1}^{n_P} (i-p_\tau)\right) \cdot \delta^{x_i}}, g^{\alpha_1 \mu_1}\right) \\
=& e(g, h_0)^{\alpha_1 \mu_1 \beta_1} \cdot e(g, h_0)^{s \cdot \alpha_1 \mu_1} \\
& \cdot e(g, g)^{\frac{\alpha_1 \mu_1 \cdot s}{\theta} \cdot \sum_{i=1}^{n_X} \left(\prod_{\tau=1}^{n_P} (i-p_\tau) \cdot \delta^{x_i}\right)}, \\
part3 \stackrel{def}{=}& e(\tilde{S}_2, Ct'') \\
=& e\left(h_0^{\alpha_1(s+\beta_2)} \cdot g^{\sum_{i=1}^{n_X} \left(\frac{\alpha_1 s}{\theta} \cdot \prod_{\tau=1}^{n_P} (i-p_\tau)\right) \cdot \delta^{x_i}}, g^{\mu_2}\right) \\
=& e(g, h_0)^{\alpha_1 \mu_2 \beta_2} \cdot e(g, h_0)^{s \cdot \alpha_1 \mu_2} \\
& \cdot e(g, g)^{\frac{\alpha_1 \mu_2 \cdot s}{\theta} \cdot \sum_{i=1}^{n_X} \left(\prod_{\tau=1}^{n_P} (i-p_\tau) \cdot \delta^{x_i}\right)}, \\
Ct_0 =& e(g, h_0)^{\alpha_1 \beta_1 \mu_1 + \alpha_1 \beta_2 \mu_2}, \\
M_1 =& e(g, h_0)^{\alpha_1 \beta_1 \mu_1 + \alpha_1 \beta_2 \mu_2} \cdot \\
& \frac{e(g, h_0)^{\alpha_1 \cdot s \cdot (\mu_1+\mu_2)}}{e(g, h_0)^{\alpha_1 \beta_1 \mu_1 + \alpha_1 \mu_2 \beta_2} \cdot e(g, h_0)^{s \cdot \alpha_1 \cdot (\mu_1+\mu_2)}} \cdot \\
& \frac{e(g, g)^{\frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1+\mu_2) \cdot \sum_{w=1}^{n_P} \left(\sum_{i=1}^{n_X} i^w \cdot \delta^{x_i} \cdot a_w\right)}}{e(g, g)^{\frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1+\mu_2) \cdot \sum_{i=1}^{n_X} \left(\prod_{\tau=1}^{n_P} (i-p_\tau) \cdot \delta^{x_i}\right)}} = 1.
\end{aligned}$$

The correctness analysis of our scheme has been finished.

5.2 Security Proof

Decisional q-parallel BDHE Assumption. Decisional q-parallel Bilinear Diffie-Hellman Exponent Assumption problem (q-parallel BDHE, for short) can be recalled as follows.

Choose a group G of prime order p, two random numbers $a, s \in Z_p$ and a random element $g \in G$. If an adversary is given y:

$$\begin{aligned}
y =& (g, g^s, g^a, ..., g^{a^q}, g^{a^{q+2}}, ..., g^{a^{2q}}, \\
\forall_{1 \le j \le q}& \left(g^{s \cdot b_j}, g^{\frac{a}{b_j}}, ..., g^{\frac{q}{b_j}}, g^{\frac{q+1}{b_j}}, ..., g^{\frac{2q}{b_j}}\right), \\
\forall_{1 \le j,k \le q, k \ne j}& \left(g^{\frac{a \cdot s \cdot b_k}{b_j}}, ..., g^{\frac{a^q \cdot s \cdot b_k}{b_j}}\right))
\end{aligned}$$

It is hard to distinguish a valid tuple $e(g, g^{a^{q+1} \cdot s}) \in G_T$ from a random element R in G_T.

An algorithm $\mathbb{B}$ that outputs $z \in \{0, 1\}$ has advantage ε in solving Decisional q-parallel BDHE problem if

$$\begin{aligned}
|Pr\left[\mathbb{B}\left(y, T = e(g, g)^{a^{q+1} \cdot s}\right) = 0\right] \\
- Pr\left[\mathbb{B}\left(y, T = R\right) = 0\right]| \varepsilon.
\end{aligned}$$

Theorem 1. *Suppose that an adversary Λ can find a polynomial time algorithm $\hat{A}$ that can success the game with the advantage ε.*

Proof. Permissions on out-sourced ciphertext should be read or written for the owner and writers, read for the readers, neither read nor written for all others. We need to prove that a reader cannot write the ciphertext. Thus, we assume that the adversary Λ can read a ciphertext, but cannot write the ciphertext.

We assume that the adversary Λ chooses a challenge (X^*,Y^*), and the (X^*,Y^*) is compared to (X,Y) with

two different elements at least. For simplicity, we assume that $X^* - X = \{\tilde{x}\}$ and $X - X^* = \{\hat{x}\}$.Our goal is to prove that the adversary Λ cannot distinguish X^* and X.

Setup. The challenger issues public parameters params to $\hat{A}$. $params = (\{h_w\}_{w=0}^{N}, \{g_w\}_{w=1}^{N}, g^{\alpha_1}, \Omega_1, \Omega_2, q, G, e(\cdot,\cdot), g^{\delta})$

Phase 1. $\hat{A}$ computes $\theta = \sum_{w=0}^{N} \delta_w \cdot a_w$, and chooses $s \in Z_q^*$, and constructs $Token_{u_t,ns_t}$:

$$Token_{u_t,ns_t} = \left(\tilde{S}_0, \tilde{S}_1, \tilde{S}_2, \tilde{S}_3, \tilde{S}_4, P\right),$$

$$\tilde{S}_0 = g^{\frac{\alpha_1 \cdot s}{\theta}},$$

$$\tilde{S}_1 = h_0^{s_1} \cdot \prod_{\substack{i=1,2,\cdots,n_{X^*} \\ x_i \in X^{*'} - P}} g^{\frac{s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{x_i},$$

$$\tilde{S}_2 = h_0^{\alpha_1 \cdot s_2} \prod_{\substack{i=1,2,\cdots,n_{X^*} \\ x_i \in X^{*'} - P}} g^{\frac{\alpha_1 \cdot s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{x_i},$$

$$\tilde{S}_3 = h_0^{s_1} \cdot \prod_{\substack{i=1,2,\cdots,n_{Y^*} \\ y_i \in Y^{*'} - P}} g^{\frac{s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{y_i},$$

$$\tilde{S}_4 = h_0^{\alpha_1 \cdot s_2} \prod_{\substack{i=1,2,\cdots,n_{Y^*} \\ y_i \in Y^{*'} - P}} g^{\frac{\alpha_1 \cdot s}{\theta}} \prod_{\tau=1}^{n_P} (i - p_\tau) \cdot \delta^{y_i}$$

Challenge. The challenger constructs and retains a table to record (X^*,Y^*). When the challenge (X^*,Y^*) exists in the table, the challenger reconstructs and returns Ct, otherwise, he/she returns the same Ct as before.

Ct is matched as follows.

$$\begin{aligned} M_1 &= e(g,g)^{\frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1+\mu_2)\left(\sum_{w=1}^{n_P} i^w \cdot \widehat{\delta^x} \cdot a_w - \prod_{\tau=1}^{n_P} (i-p_\tau) \cdot \delta^{\tilde{x}}\right)} \\ &= e(g,g)^{\frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1+\mu_2)\left(\sum_{w=1}^{n_P} i^w \cdot a_w\right) \cdot \left(\widehat{\delta^x} - \delta^{\tilde{x}}\right)} \end{aligned}$$

Phase 2. Same as **Phase 1**.

Guess. Let $\tilde{a}$ be defined as follows.

$$\tilde{a} \overset{def}{=} \frac{\alpha_1 \cdot s}{\theta} \cdot (\mu_1 + \mu_2) \left(\sum_{w=1}^{n_P} i^w \cdot a_w\right)$$

We then have: $M_1 = e(g,g)^{\tilde{a} \cdot \left(\widehat{\delta^x} - \delta^{\tilde{x}}\right)}$.

According to Decisional q-parallel DBHE problem, the adversary Λ cannot distinguish $e(g,g)^{\widehat{\delta^x}}$,$e(g,g)^{\delta^{\tilde{x}}}$, or a random element R. Correspondingly, he/she cannot distinguish X^* or X. □

5.3 Features of Matching Ct

The write policy is semi-hidden in our scheme. Firstly, it consists of five parts: three group elements (Ct_0, Ct', Ct'') and two sets $(\{Ct_{1,w}\}_{w=0}^{n_P}, \{Ct_{2,w}\}_{w=0}^{n_P})$. These five parts cannot derive out the corresponding write policy. Secondly, the algorithm $MatchCt$ can't leak out a write policy in the process of matching Ct either. The adversary can only get the set P. The write policy then holds a $semi-hidden$ feature.

What's more, the way of matching holds a noteworthy feature: $re-usability$. It is observed that the construction of Ct is independent of the random numbers μ_1 and μ_2. Therefore, we can reuse the writing access structure by refreshing Ct with different μ_1 and μ_2 after each successful match: Cloud server chooses a random number $\psi \in Z_q^*$, and computes: $Ct_{1,w} \leftarrow (Ct_{1,w})^{\psi}$,$Ct_{2,w} \leftarrow (Ct_{2,w})^{\psi}$, $Ct' \leftarrow (Ct')^{\psi}$,$Ct'' \leftarrow (Ct'')^{\psi}$.

As a result, the write policy holds two features: $semi-hidden$ and $reusability$. With these two features, our scheme holds $unpredictability$. That is to say, a server can help data owners with writing permission control, but cannot predict or determine the subsequent writing request.

5.4 Performance Analysis

In this section, we compare storage and computation costs to other two classic schemes (DAC-MACS [18] and Hur's [6]) on each entity and complete simulations of core algorithms in our scheme.

5.4.1 Storage Cost Comparison

Table 1 shows the comparison of storage costs. We ignore the storage cost of random integers like the other two schemes (DAC-MACS [18] and Hur's [6]).

Wherein, $|p|$: Storage cost of an elemental of groups; $n_{a,k}$: Number of attributes managed by AA_k; N_A: Number of AAs in the scheme; n_{a,k,u_t}: Number of attributes distributed by AA_k to u_i; $n_{u_t,k}$: Number of users managed by AA_k; t_r : Number attributes of the access tree $Tree_{Read}$ assigned by each owner; n_p: Number of wildcards in a vector of constraint of access structure; N: Number of elements in the constraint access structure.

In our scheme, AA_k stores $\{h_w\}_{w=0}^{N}$, $\{g_w\}_{w=1}^{N}$, g^{α_1}, Ω_1, Ω_2, which equals $N|p|$, $N|p|$, $|p|$, $|p|$ and $|p|$ respectively. The storage costs on both owner and user are the same as that of our previous work [10]. The storage cost of Ct on cloud is Ct_0, $\{Ct_{1,w}\}_{w=0}^{n_p}$, $\{Ct_{2,w}\}_{w=0}^{n_p}$, Ct' and Ct'', which equals $|p|$, $n_P|p|$,$n_P|p|$, $|p|$ and $|p|$ respectively. Compared to existing schemes, our scheme spends less storage cost on each user. But that on AA_k and cloud is the most because we have taken multi-writer access control into account, while they did not.

Table 1: Comparison of storage cost ($|p|$)

	DAC-MACS	Hur's	Our previous work	Our Scheme
AA_k	$n_{a,k}+3$	$n_{a,k}+3$	$(1+\sum_{k=1}^{N_A} n_{a,k})\,\|p\|$	4+2N
Owner	$3N_A+1+\sum_{k=1}^{N_A} n_{a,k}$	$2N_A+\sum_{k=1}^{N_A} n_{a,k}$	$(3+2\sum_{k=1}^{N_A} n_{a,k,u_t})\,\|p\|$	$1+\sum_{k=1}^{N_A}(n_{a,k})$
User	$1+2\sum_{k=1}^{N_A} n_{a,k,u_t}$	$3N_A+1+\sum_{k=1}^{N_A} n_{a,k,u_t}$	$(n_{a,k}+3+n_{u_t,k})\,\|p\|$	$1+\sum_{k=1}^{N_A} n_{a,k,u_t}$
Cloud	$3+3t_r$	$3+3t_r$	$(3+2t)\,\|p\|$	$5+2t_r+2n_P$

5.4.2 Computation Cost Comparison

Table 2 gives out the computation cost comparison of the core algorithms. We ignore the computation cost of multiplying and dividing like the other two schemes (DAC-MACS [18] and Hur's [6]).

$|E|$: Exponent arithmetic; $|Pe|$: An $e(g,g)$ bilinear mapping operation; k: Number of attributes of a user's private key; I_{A_k}: Attribute set in a ciphertext issued by AA_k; n_P: Number of elements in a wildcard set P; n_X: Number of elements in a status set X; n_Y: Number of elements in a status set Y.

As shown in Table 2, the running time of the algorithm Setup is proportional to M (the number of statuses). The algorithm $EncryptCt$ runs on each owner to construct Ct, which need $(6+n_X+n_Y)|E|$. Algorithm $MatchCt$ runs on Server to match Ct, which needs $(2n_P)|E|+6|Pe|$. It is related with N (the number of users). Compared to the other two schemes, our scheme works for multi-writer access control, but those of DAC-MACS [18] and Hur's [6] for a single user is an extra cost.

We can replace users' identities with an attribute set to reduce delay time if the number of attribute sets is lesser than the number of users' identities. This replacement can extend our scheme to a larger scale.

6 Simulation

We complete the simulation on Ubuntu system with an Intel Core i7 10^{th} Gen CPU. The Pairing-Based Cryptography library is installed onto Ubuntu to simulate all of the algorithms. The elliptic curve is chosen as, the order of all groups as 160 bit, and the field size as 512bit. Times are the mean of 10 trials to avoid the results of accidents.

Figure 4 (a) gives out the computational time comparison between Hur's [6], Li's [12], Teng's [16], and ours. It shows that the encrypting time spent on a controller is similar to these two schemes, Hur's [6] and Li's [12]. We have joined the data sharing and aggregating scheme by writing privilege permission control with a negligible performance impact. Figure 4(b), (c) and (d) show that the computational costs spent on each entity are remarkably correlated linearly with n_P without depend on n_X or n_Y. It is worth knowing that the write policy and token can be generated on a controller and a writer separately ahead of time. The computational delay spent on token matching are almost 50 ms, which falls within the user acceptable dealing tolerance range. This simulation gives the feasibility of this scheme.

7 Conclusion

This paper analyzes the control requirements when multiple doctors or nurses collaboratively write the same encrypted data in Cloud-aided E-Health scene. In response to these requirements, we propose an Access Control Scheme supporting Ciphertext Writing Privilege Management in Cloud-aided E-Health System by expressing a write access control policy as Matrix. Our scheme has two noteworthy features:

1) Fine-grained write privilege control. Authorized doctors or nurses can write data legally only when his/her write credential satisfies the write policy defined by the data's controller, while unauthorized users cannot.

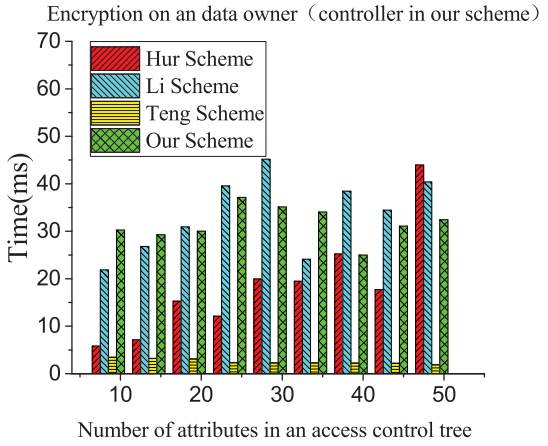
2) Data-binding-policy access control method. The outsourced data is bound to a collaborative write policy before being stored on the cloud. The policy can be on-demand now that it is defined by the data owner, bringing flexibility to our scheme.

Acknowledgments

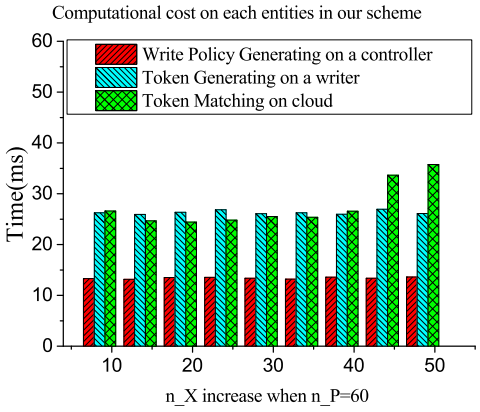
This work is supported by the National Science Foundation of China (No. 62062045), the Science and Technology Research Project of Jiangxi Provincial of Education

Table 2: Computational cost comparison

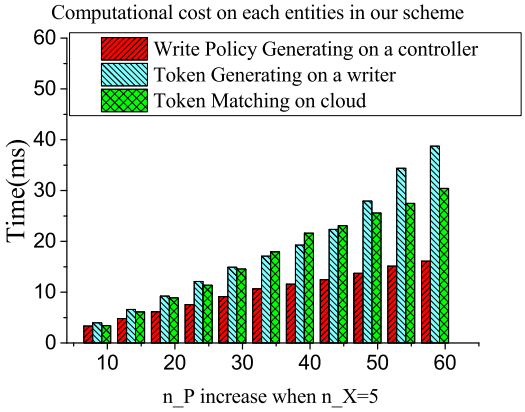
	EncryptData on controller	**DecryptData** on User	**DecryptData** on Cloud	**EncryptCt** on controller	**MatchCt** on Server
DAC-MACS	$(3+6t_r)\|E\|$	$\|E\|$	$N_A \times ((\sum_{k=1}^{I_{A_k}} (3\|Pe\|+\|E\|)) +2\|Pe\|$	-	-
Hur's	$(2+2t_r)\|E\|$	$(k+logt_r)\|E\| +(2k+1)\|Pe\|$	0	-	-
Our previous work	$(2+2t_r)\|E\|$	$\|E\|+\|P\|$	$(k+logt_r)\|E\|+(2k)\|Pe\|$	-	-
Our Scheme				$(6+n_X+n_Y)\|E\|$	$(2n_P)\|E\|+6\|Pe\|$



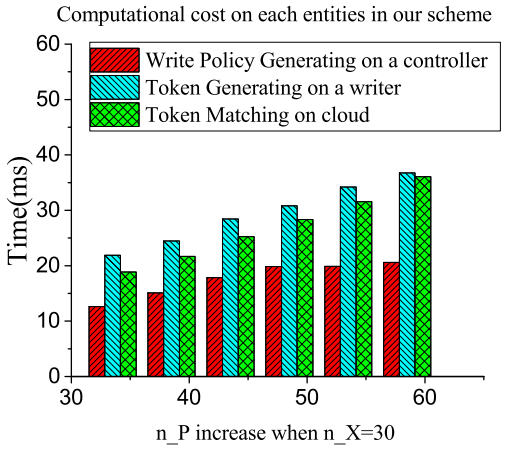
(a)Compare with other schemes



(b)n_X is changing when n_P=60



(c) n_P is changing when n_X=5



(d) n_P is changing when n_X=30

Figure 4: Simulation of Computational Cost

Department (No.GJJ180905), and the MOE (Ministry of Education in China) Project of Humanities and Social Sciences (No.20YJAZH112).

References

[1] T. Alam, "A survey on the use of blockchain for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 13, no. 3, pp. 119–130, 2021.

[2] A. Deng, J. Shi, and K. He, "Acs-wam: an access control scheme supporting write authority management in cloud-assisted cyber-physical systems," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, pp. 747–752, 2019.

[3] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *Computers & security*, vol. 42, pp. 151–164, 2014.

[4] S. Fugkeaw and H. Sato, "Enforcing hidden access policy for supporting write access in cloud storage systems.," in *CLOSER*, pp. 530–536, 2017.

[5] S. Fugkeaw and H. Sato, "An extended cp-abe based access control model for data outsourced in the cloud," in *2015 IEEE 39th Annual Computer Software and Applications Conference*, vol. 3, pp. 73–78, 2015.

[6] J. Hur and K. Kang, "Secure data retrieval for decentralized disruption-tolerant military networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 16–26, 2012.

[7] M. Jahan, M. Rezvani, A. Seneviratne, and S. Jha, "Method for providing secure and private fine-grained access to outsourced data," in *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, pp. 406–409, 2015.

[8] M. Jahan, M. Rezvani, Q. Zhao, P.S. Roy, K. Sakurai, A. Seneviratne, and S. Jha, "Light weight write mechanism for cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 5, pp. 1131–1146, 2017.

[9] M. Jahan, P.S. Roy, K. Sakurai, A. Seneviratne, and S. Jha, "Secure and light weight fine-grained access mechanism for outsourced data," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 201–209, 2017.

[10] S. Jiaoli, H. Chuanhe, W. Jing, Q. Kuangyu, and H. Kai, "Multi-user collaborative access control scheme in cloud storage [j]," *Journal on Communications*, vol. 37, no. 1, pp. 88–99, 2016.

[11] K Lee, D.H. Lee, J.H. Park, M. Yung, and Y. Mu, "Cca security for self-updatable encryption: Protecting cloud data when clients read/write ciphertexts," *The Computer Journal*, vol. 62, no. 4, pp. 545–562, 2019.

[12] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785–796, 2016.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2012.

[14] T.V.X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE transactions on information forensics and security*, vol. 11, no. 1, pp. 35–45, 2015.

[15] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 384–394, 2013.

[16] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute-based access control with constant-size ciphertext in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 4, pp. 617–627, 2015.

[17] J. Wang, B. Lang, and R. Zhu, "Rwac: A self-contained read and write access control scheme for group collaboration," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, pp. 97–103, 2018.

[18] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dacmacs: effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

[19] Y. Yang, X. Liu, and R.H. Deng, "Lightweight break-glass access control system for healthcare internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610–3617, 2017.

Biography

Kai He received the B.S. degree in computer science from Wuhan Textile University, Wuhan, China, in 2010, and the Ph.D. degree from Wuhan University, Wuhan, China, in 2016. Since 2016, He has been a Lecturer at the School of Mathematics and Computer, Wuhan Textile University, Wuhan, Hubei, China. From Jan. to June 2015, he was a visiting Student at the University of Calgary. His research interest includes the Cloud security, auction, *et al.*

Ziqi Wang received the B.S. in computer science from Wuhan Textile University, Wuhan, Hubei, China in 2020. He is currently pursuing the master degree in Wuhan Textile University. His research interests include cloud security and data security, blockchain.

Jiaoli Shi received the Ph.D. degree from the School of Computing, Wuhan University, in 2017. Since 2012, she has been an Assistant Professor at the school of computer and big data science, Jiujiang University. Her research

interests include Cloud security, ICN security, SDN and CDN. Dr. Jiaoli twice won the third prize of Doctoral Forum of School of Computer Science, Wuhan University for Excellence in 2014 and 2015.

Anyuan Deng received the B.Sc. degree in computer science from Jiangxi Normal University, Nanchang, China, in 1995, M.Sc. degree in computer science from Huazhong University of Science and Technology, Wuhan, China, in 2006. Since 2003, He has been a professor at the school of computer and big data science, Jiujiang University, Jiujiang, China. His research interests include Cloud security, ICN security, Software Engineering and CDN.

Shunlin Lv is an undergraduate student in the school of computer and big data science, Jiujiang University. His research interests include Cloud security, Privacy protection.

Comparative Attribute Access Control Scheme Based on Spatio-temporal Constraints in Cloud

Junling Zhang, Ze Wang, Ping Zhao, Minghua Gao, and Shimin Sun
(Corresponding author: Ze Wang)

School of Computer Science and Technology, Tiangong University
399 Binshui W Rd, Xiqing, Tianjin, China
Email: wangze@tiangong.edu.cn

(Received July 15, 2021; Revised and Accepted Mar. 2, 2022; First Online Apr. 9, 2022)

Abstract

Cloud computing provides an extensible, high-performance solution by entrusting computational tasks and storage to clouds, effectively addressing resource constraints in data storage, data sharing, and computing for users. Attribute-based encryption (ABE) is considered the most potent encryption primitive for achieving fine-grained access control and solves the problem of one-to-many encrypted data sharing. However, as applications evolve, the ABE scheme may not handle particular scenarios such as access policies related to the user's time and space range. In addition, end-users should protect their identity and the associated privacy from attacks by malicious authorized institutions and providers. Attribute encryption scheme based on ciphertext policy (CP-ABE) encrypts ciphertext according to user attribute set, which uses policies and constraints defined by the data owner to provide safe and reliable fine-grained access control. To solve the Spatio-temporal constraints more effectively, this paper introduces the comparison relationship in the comparative attribute encryption (CBE) scheme into the process of attribute-based encryption and realizes that the two attributes of time and location satisfy various constraints on the integer set. Thus, data users can flexibly access data at a multi-dimensional level. Furthermore, our solution is proven secure and efficient through security and performance analysis.

Keywords: Comparison Attribute Encryption; Dynamic Access Control; Spatio-temporal Constraints

1 Introduction

Cloud storage provides us with a new data information storage model, which enables economies of scale and elastic scaling, reducing operating cost and avoiding waste of resources. Therefore, many enterprises are migrating their business to one or more cloud platforms. However, this model of cloud storage poses entirely new challenges to privacy and security, because data is no longer stored in users' trusted domains, but stored in remote cloud servers. In addition, cloud service providers may try to learn user's sensitive data, resulting in privacy leakage. Therefore, achieving access control while ensuring data security is a great challenge.

To implement secure data access control on untrusted cloud servers, traditional solutions encrypt data before storing it in cloud servers, but the encryption results in higher key management overhead and increases the complexity of the system. Attribute-based encryption (ABE) is the most promising solution to private data access control through reasonable configuration of sharing policies. Since [19] was proposed in 2005, the ABE has attracted wide attention from the government, enterprises and academia. The ABE is an extension of identity-based encryption, which implements broadcast encryption for a group of users and provides fine-grained encrypted access control for data down to the attribute level. [10] proposes Key-Policy ABE (KP-ABE), which embeds policies into user keys and embeds attributes into ciphertexts. The design of the KP-ABE has its application in scenarios such as paid video sites, log encryption management, etc. Different from the KP-ABE, [3] proposes Ciphertext-Policy ABE (CP-ABE), which embeds policies into ciphertexts and embeds attributes into user keys. The CP-ABE can be used in many applications including cloud environments, hospitals, government and smart factories.

Due to the high flexibility and scalability of cloud computing, many enterprises and individuals have used cloud servers to store and calculate their data. However, some occasions require high confidentiality, where users' access rights depend not only on their attributes, but also on dynamic factors, such as change of time and location. Taking a PHR system as an example, patients can develop access policies to encrypt their personal medical records and upload them to the cloud server, allowing relevant medical staff to view the patients' medical records under certain conditions and make diagnosis. Assume that in the PHR system only doctors and pharmacists are al-

lowed to view the medical records and examine patients' health status, where doctors can visit the documents at any time and any place, but pharmacists can only visit the documents in the office building of their hospital during working hours (8:00 a.m.-18:00 p.m.). In this case, the fine-grained access control is applied, which considers access time, location and identity attributes, and achieves rapid retrieval and sharing of medical data.

The above case needs to consider both time and space, but the traditional CP-ABE scheme rarely combines dynamic changes of time and space to solve access control problems in cloud storage. In 2014, Androulaki *et al.* [1] described in detail the framework of the LoTAC, which enables spatio-temporal access control of cloud stored data by integrating the cloud provider's operations and infrastructure. According to literature [20], in 2014 Shao *et al.* provided location privacy protection by encrypting the anonymity attribute of ciphertext policy to ensure the confidentiality of service data and access policies for locations. According to literature [22,29,30], in 2013-2014 Zhu *et al.* constructed an encryption scheme based on specific temporal predicates by comparing secure integers. There are some common problems in the existing schemes:

1) Computational cost is fairly high for data owners to enhance access policies and encrypt data for each user;
2) It is easy for malicious users to publish false information and illegally access data and services;
3) When rough locations are not dense enough, it causes the privacy leakage of mobile users' locations.

A malicious location service provider (LSP) may retain the current location, and provide users with previous traveling records and other information. The LSP also can monitor the user's life trajectory, preferences, health status and other aspects of his private life based on the user's spatial and temporal information. Or it may simply use the user ' s spatio-temporal information to identify users. In [5], the singleness test experiment shows that four points with specific time and location are sufficient to correctly identify an individual user with a probability of 95%. The combination of location and time reveals individual characteristics of a user, which is known as the user's standard identifier. Therefore, guaranteeing anonymity of users and protecting their identity requires protection of their spatial and temporal information and their identity. In [17], a new access control scheme based on temporal and spatial constraints is proposed. The TSC-ABAC scheme uses multi-dimensional range derivation function (MRDF) to compare tand uses the token generation algorithm to determine the location. This is the first scheme to handle time and location at the same time, bbut the scheme cannot effectively support continuous location range constraint information in the location dimension.

Therefore, this paper re-designs the ABE encryption scheme based on bilinear mapping to solve the above problems, and adds the two attributes of time and location into the scheme. A user key is associated with static properties, time range and location range. If the user's attributes satisfies given requirements and the temporal and spatial ranges match the access policy, the trapdoor can be released and the ciphertext can be decrypted successfully. The contributions of this paper are as follows:

1) We propose the first CP-ABE scheme that can effectively deal with constraints of both time range and location range;
2) We apply the proxy re-encryption scheme in the proposed scheme, and associate the temporal and spatial attributes owned by the user with the current access time of the user to make the scheme more flexible and efficient;
3) Security analysis and theoretical performance analysis show that the proposed solution is secure and effective.

2 Related Work

At present, there are several ABE schemes to deal with the temporal and spatial factor. However, most schemes consider only one of the factors. Scheme in literature [1] combines both aspects, but ignores the fine-grained access control for users. To overcome the drawbacks of the above schemes, this paper designs a data access control scheme that considers both temporal and spatial ranges. In this paper, by integrating the constraints of user's spatio-temporal attributes into access control, a complete and effective scheme is designed, and the comparative attribute-based encryption and decryption is adopted to define user access rights, thus achieving more flexible fine-grained access control. At present, only a few access control schemes consider dynamic and static attributes, and the computational cost is huge. Considering location-based access control from the perspective of spatio-temporal constraints, and combining common part shared by access control mechanism and location verification, we design the access control scheme that can resist spatio-temporal attacks.

2.1 Encryption Schemes Associated with Time Attributes

In the development process of the ABE scheme, some work has studied the constraint of time. For example, in literature [21], Bethencourt *et al.* proposed a scheme by utilizing the access policy tree which assigns 0 / 1 to the branches of the access policy tree to realize the comparison of integers. However, actual application process faces the problem of low efficiency. Therefore, Hong [11] *et al.* proposed a concept of timed release to encrypt the access policy tree of the CP-ABE, which cannot accurately know user's access time, so it cannot work well when the user make access within a certain time. Through

the forward/backward derivation function, Zhu *et al.* [29] first proposed a comparative attribute-based encryption scheme, which performs well in comparing the time range. In literature [28], Zhu *et al.* discussed how to use a mechanism from the proxy re-encryption scheme to control the constraint of time range, but they only presented a general idea without specific solutions to the above problems. In literature [27], Yang *et al.* proposed an access control scheme taking time into consideration, which slices time, refreshes the key in initialization of each time slot and sends that key to the user who meets the policy requirements. However, this scheme needs to update the key and publish it at each time slot, which leads to increased encryption and decryption overhead and reduced efficiency. In literature [23], Wang *et al.* proposed a scheme that handles the constraint of time range with a multidimensional range derivation function, but the range of attributes handled is small and the scheme is not suitable for large scale generalization.In literature [6,18], TRE technology is combined with encryption scheme, and a CP-ABE scheme based on time-release encryption is proposed. TRE relies on a time server to publish trap gates at a specified time, and only when the receiver gets the trap gates can it be decrypted.However, this scheme does not support dynamic change of time range and has poor flexibility.

2.2 Encryption Schemes Associated with Location Attributes

Some ABE schemes are combined with the LBS, as mentioned in literature [14, 25]. However, these schemes only consider the location of users, and use privacy protection technology to achieve access control. Actually, dynamic location can be treated as a common attribute of the ABE scheme. In literature [7], Denisow *et al.* encrypt user's location by the Geohash algorithm, and integrate the location into the ABE scheme. In literature [26], Xue *et al.* improved the CP-ABE scheme by applying the trapdoor mechanism to the access control scheme. In literature [8], the scheme proposed by Ghafghazi *et al.* integrates broadcast encryption with the CP-ABE to handle location attributes.In literature [16], in order to protect user location privacy, combined with OT and CP-ABE schemes, a privacy-protecting LBS query scheme is proposed to protect the privacy of LBS suppliers and vehicles.

3 Preliminaries and Defintions

3.1 Composite Order Bilinear Map

Let $p, q, p^{'}, q^{'}, s_1, s_2$ be large prime numbers, N = pq is a public RSA model,$s = s_1 s_2$, $n^{'} = p^{'} q^{'}$ and $n = sn^{'}$ be secret,G and G_T be two cyclic bilinear groups of composite order $n = sn^{'}$, α,β be two random exponents in Z, and $e : G \times G \rightarrow G_T$ be a bilinear map with the following properties:

1) Bilinearity: for any $\forall g_1, g_2 \in G$ and $\forall a, b \in Z$,$e\left(g_1{}^a, g_2{}^b\right) = e\left(g_1, g_2\right)^{ab}$;

2) Non-degeneracy: g_1 and g_2 are the generators of group, $e\left(g_1, g_2\right) \neq 1$;

3) Computability: for $g_1, g_2 \in G$,there exists a valid algorithm to compute $e\left(g_1, g_2\right)$.

3.2 Trapdoor Structure

The access policy tree consists of trapdoors and nodes associated with time and location ranges. Location and time trapdoors can be embedded in any node of the access policy tree, and the access rights of certain users are restricted by the trapdoor TD. We define that a trapdoor has two states, exposed and not exposed.

Not exposed: a user is not allowed to pass through the trapdoor in order to access the corresponding secret.

Exposed: a user can pass through the trapdoor to access the corresponding secret and the trapdoor is exposed.

A user needs to have certain attributes required by the access policy and initiate the access within corresponding temporal and spatial ranges to release the trap door.

With the trapdoor independent of user's set of attributes, the user does not have a private key associated with the time and location. As a result, the trapdoor decreases the workload of revoking and re-distributing private keys. The scheme in this paper allows different access policies to set trapdoors and a ciphertext can be associated with different trapdoors of different spatio-temporal constraints. Therefore, the spatio-temporal information can be flexibly combined with other user attributes, and users have to meet the access policy and release the trapdoor to access the secret data.

3.3 Access Policy Tree

In the process of data encryption, traditional ABE schemes perform access control through the structure of an access policy tree. We optimized the tree by embedding spatio-temporal constraints into the structure, adopting a multi-dimensional distance derivation function, and using trapdoors to help determine the legitimacy of users. The structure of the access policy tree is shown in Figure 1 below:

This paper implements the fine-grained access requirements through an access policy tree, where each leaf node represents a attribute At owned by the user. Non-leaf nodes represent logic gates (AND,OR) and trapdoors (Threshold).num_x represents the number of children of non-leaf node x, and k_x denotes the threshold value. $\text{parent}\,(x)$ denotes the parent node of node x. $\text{attr}\,(x)$ indicates that the leaf node x is associated with the attribute.

In Figure 1, we consider embedding the spatio-temporal constraints into the non-leaf nodes of the access policy tree,and define $\text{TD}^x_{\{t_a,t_b\}}$ to represent the constraint of time range associated with node x and $\text{LD}^x_{\{l_a,l_b\}}$

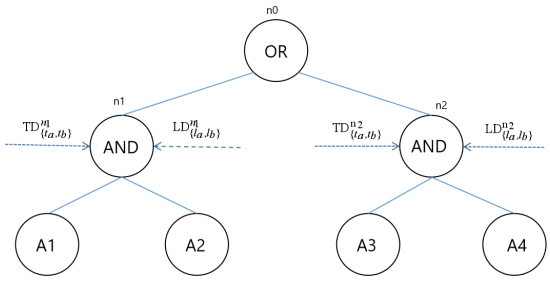


Figure 1: Access policy tree structure

to represent the constraint of location range associated with node x. In the access policy tree as shown above, the sub-access policy applied to node n1 needs to satisfy $A_1 \wedge A_2$,and the sub-access policy applied to node n2 needs to satisfy $A_3 \wedge A_4$. The user needs to satisfy the requirement of $(A_1 \wedge A_2) \vee (A_3 \wedge A_4)$, and the access time and location should be within the range of $[t_a, t_b], [l_a, l_b]$ in order to successfully access resources from the cloud.

3.4 Introduction of the Multidimensional Range Derivation Function

The MRDF utilizes the "one-way" property to represent the total ordering relation of integers. We choose the MDRF to select the lower-bound and upper-bound integer values $(l_{i,j}, l_{i,k})$,and $\psi \to U$ is a cryptographic mapping regarding the user's U-preserving order, mapping each attribute to a value $v\{l_{i,j}, l_{i,k}\}_{A_i \in A}$ that reflects a cryptographic bound.

We define this mapping function $\psi(\cdot)$ as follows:

$$\begin{aligned} \mathrm{v}\{l_{i,j}, l_{i,k}\}_{\mathrm{A}_i \in \mathrm{A}} &\leftarrow \psi\left(\{l_{i,j}, l_{i,k}\}_{\mathrm{A}_i \in \mathrm{A}}\right) \\ &= \left(\varphi^{\prod_{\mathrm{A}_i \in \mathrm{A}} \lambda_1^{l_{i,j}} \mu_i^{z-l_{i,k}}}\right) \in G_{n'}. \end{aligned}$$

Given a function F: $V \to v$ based on a set, it is called the multi-dimensional range derivation function when it satisfies the requirements below:

1) Easy to compute: the function F can be computed in the PPT algorithm, if $l_{i,j} \leq l'_{i,j}, l_{i,k} \geq l'_{i,k}$,we have: $\forall A_i \in A$,

$$\mathrm{v}\{l'_{i,j}, l'_{i,k}\} \leftarrow \mathrm{F}\{l_{i,j} \leq l'_{i,j}, l_{i,k} \geq l'_{i,j}\}(\mathrm{v}\{l_{i,j}, l_{i,k}\}).$$

2) Hard to invert: For an attribute $A_i \in A$, it is difficult for any PPT algorithm to derive $\mathrm{v}\left\{l'_{i,j}, l'_{i,k}\right\}$,if $l_{i,j} > l'_{i,j}$ or $l_{i,k} < l'_{i,k}$.

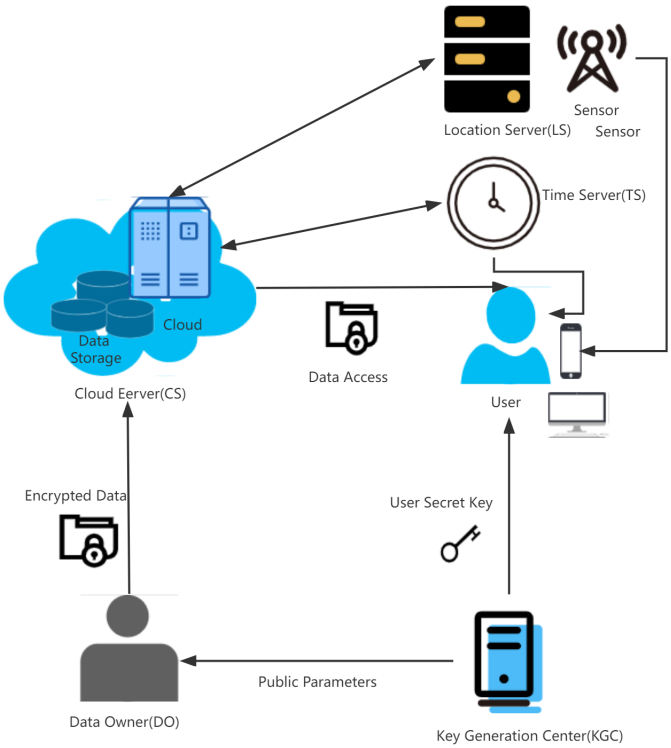


Figure 2: System model diagram

The function F(.) has the following form:

$$\begin{aligned} \mathrm{v}\{l'_{i,j}, l'_{i,k}\} &\leftarrow \mathrm{F}\{l_{i,j} \leq l'_{i,j}, l_{i,k} \geq l'_{i,j}\}(\mathrm{v}\{l_{i,j}, l_{i,k}\}) \\ &= (v\{l_{i,j}, l_{i,k}\}_{A_i \in A})^{\prod_{A_i \in A} \lambda_i^{l'_{i,j}-l_{i,j}} \mu_i^{l'_{i,k}-l_{i,k}}} \\ &= (\phi^{\prod_{A_i \in A} \lambda_i^{l_{i,j}} \mu_i^{z-l_{i,k}}})^{\prod_{A_i \in A} \lambda_i^{l'_{i,j}-l_{i,j}} \mu_i^{l'_{i,k}-l_{i,k}}} \\ &= \phi^{\prod_{A_i \in A} \lambda_i^{l'_{i,j}} \mu_i^{z-l'_{i,k}}} \in G_{n'}. \end{aligned}$$

4 TSC-CABE Scheme

4.1 System Model

Our system mainly contains six entities, Cloud Service Provider (CSP), Key Generation Center (KGC), Location Server (LS), Time Server (TS), Data Owner (DO), Data User (DU), as Figure 2.

Key Generation Center (KGC). The KGC initializes public parameters and distributes keys to users based on their attribute sets. In this system, it is assumed that the KGC is a fully trusted institution.

Cloud service provider (CSP). The cloud service provider stores data and provides access to data for users. Using its powerful computing power to provide data re-encryption services, the cloud

service provider is considered to be honest and semi-trustworthy.

Data owner (DO). The data owner specifies the policy for accessing the ciphertext and associates a set of attributes with resources to be accessed. Assume that the data owner is honest and trustworthy.

Data user (DU). Each user has a unique identifier and the KGC issues keys to users based on their attributes. A user, if considered dishonest, wants to decrypt the data without being authorized. It is likely that unauthorized users collude together to obtain more information.

Time Server (TS). The time server is to provide safe and reliable time services including time synchronization. Let F_t represent the time format in the system.

Location Server (LS). The location servers are distributed in some specific areas, which can perform computational operations. For example, the location server for trapdoor decryption can find out the location of the user with the help of sensors. Let F_{loc} represent the location format in the system.

4.2 Framework of TSC-CABE Scheme

The TSC-CABE proposed in this paper mainly includes five phases: system initialization, key generation, encryption, re-encryption, and decryption. Below is introduced the implementation of each phase.

- System initialization $(\kappa) \rightarrow (PKP, MK)$

  The initialization algorithm is operated by the KGC, and the algorithm outputs the public key parameter PKP and the master key MK by entering a security parameter κ.

- Key generation $(PKP, MK, \mathrm{gid}, S_{gid}, T_{gid}, L_{gid}) \rightarrow SK_{gid}$

  Operated by the KGC, the key generation algorithm generates user's private key SK_{gid} by entering the public key parameter PKP, the master key MK, the user global identity gid, the set of attributes of the user, and the time and location constraints $T_{gid} = [t_a, t_b], L_{gid} = [l_a, l_b]$.All elements in $T_{\mathrm{gid}}, L_{\mathrm{gid}}$ are related by specific integers to guarantee the full order like $0 \leq t_a \leq ... \leq t_b$.

- Encryption $(m, \Gamma, PKP) \rightarrow (\mathrm{CT})$

  The data owner operates the encryption algorithm.The algorithm receives the message M, accesses the tree structure and the public key parameter PKP, and final outputs the ciphertext CT with time and location constraints embedded in the ciphertext as defined by the data owner.

- Re-encryption $(PKP, CT, t_c, l_c) \rightarrow (\mathrm{RC})$

  The re-encryption algorithm is run by the CSP. Input the public key PKP, ciphertext CT, current time t_c and current location l_c of user access into the algorithm and the re-encrypted ciphertext RC is output.

- Decryption $(PKP, RC, SK_{gid}) \rightarrow (\mathrm{m}/\perp)$

  The user operates the decryption algorithm by inputting the public key parameter PKP, the ciphertex RC, and the user's private key $\mathrm{SK}_{\mathrm{gid}}$.If the attribute of time is within the current time range and the location is within the current location range, the decryption can be done successfully, otherwise the decryption shall fail.

5 Algorithms in the TSC-CABE Scheme

- Algorithm 1. System initialization algorithm

  First of all, the key generation center selects a bilinear mapping system $S_N = \{N = pq, G, G_T, e\}$ with the composite order as $n = s^{'}n^{'}$, and then selects G_s,$\mathrm{G}_{n'}$, two subgroups of G. What follows is that the KGC selects random generators $g \in G_s, \phi \in G_{n'}, \omega \in G$, and two random numbers $\lambda, \mu \in Z_{n'}^*$,where $e(g, \phi) = 1$ but $e(g, \omega) \neq 1$.Next, operate the three hash functions, $H_0, H_1 : \{0,1\}^* \rightarrow G_{S'}, H_2 : G_T \rightarrow Z_n^*$.Select any two indices $\alpha, \beta \in Z_n^*$ and generate $h = \omega^{\beta}, \eta = g^{1/\beta}, \varsigma = e(g, \omega)^{\alpha}$ In the end, the public key is generated as follows:

$$\mathrm{MK} = \left(p, q, n^{'}, \alpha, \beta\right).$$

- Algorithm 2. key generation algorithm

  Each user has a set of attributes S_{gid}.The key generation center KGC selects $u_j \in Z_n^*$ and a random value $r_i \in Z_n^*$ for each attribute $i \in S_{gid}$, and then computes the corresponding attribute key as follows:

$$\mathrm{SK}_{\mathrm{attr}} = \Big\{ \mathrm{D} = \mathrm{g}^{\frac{\alpha + u_j}{\beta}} H_0(\mathrm{gid})^{\frac{u_j}{\beta}}, \mathrm{D}' = \omega^{\mathrm{u_j}} \\ \forall \mathrm{i} \in \mathrm{S_{gid}} : \mathrm{D_i} = (\mathrm{g}H_0(\mathrm{gid}))^{u_j} \mathrm{H_1(i)^{r_i}}, \mathrm{D}_{\mathrm{i}}' = \omega^{\bar{r}_i} \Big) \Big\}.$$

To achieve access control under the constraint of time, we assume that the user is assigned the temporal and spatial access rights $[t_a, t_b], [l_a, l_b]$, where F_t, F_{loc} respectively represent the temporal and spatial formats in the system. $[t_a, t_b], [l_a, l_b]$ represent the boundary values of time and location in the system respectively, and all elements are discrete integers with total ordering. The KGC selects a $r_t \in Z_n^*$ for each temporal attribute and generates a time key as

$$\mathrm{DK}_{[t_a, t_b]} = \{ D_t = (gH_0(gid)^{u_j}) \cdot H_1(F_t)^{r_t}, D_t' = \omega^{r_t} \\ D_t'' = \left(v_{\{t_a, t_b\}}\right)^{r_t} = \varphi^{r_t \lambda^{t_a} \mu^{z - t_b}} \Big\}.$$

Also, the KGC select a $r_l \in Z_n^*$ for each spatial attribute and generate a location key as

$$\mathrm{DK}_{[l_a,l_b]} = \{D_l = (gH_0(gid)^{u_j}) \cdot H_1(F_l)^{r_l}, D_l' = \omega^{r_l} \; D_l'' = \left(v_{\{l_a,l_b\}}\right)^{r_l} = \varphi^{r_l \lambda^{l_a} \mu^{z-l_b}}\}.$$

Final the user key is generated as

$$\mathrm{SK_{gid}} = \left\{\mathrm{SK_{Attr}}, \mathrm{DK}_{[t_a,t_b]}, \mathrm{DK}_{[l_a,l_b]}\right\}.$$

- Algorithm 3. encryption algorithm

The data owner first encrypts the message by a symmetric key ek, and then encrypts ek according to an access policy defined by himself. Later the DO uploads the whole encrypted data to the cloud server. A ciphertext is generated by the algorithm below.

The algorithm starts by visiting the root node of the tree and generates a polynomial q_x for each node from the top down, and for each node x, set $d_x = k_x - 1$. Beginning with the root node, the algorithm selects a random number $s \in Z_n^*$ and sets $q_R^0 = s$.Each node x has two values q_x^0, q_x^1. If a time trapdoor or a location trapdoor is associated with node x, node x is associated with $t_x^0 \in Z_n^*$ and $l_x^0 \in Z_n^*$. For node x, the value of q_x^1 value is calculated as follows:

$$\begin{cases} q_{\mathrm{x}}^1 = q_x^0 - l_x^0 - t_x^0 & \text{x is associated with both} \\ q_{\mathrm{x}}^1 = q_x^0 - l_x^0 & \text{x is associated with location} \\ q_{\mathrm{x}}^1 = q_x^0 - t_x^0 & \text{x is associated with time} \\ q_{\mathrm{x}}^1 = q_x^0 & \text{There is other cases} \end{cases}$$

For a non-leaf node x, the polynomial q_x can be chosen arbitrarily, provided that $q_x(0) = q_x^1$ and $d_x = k_x - 1$ are satisfied. For any node x except the root node, $q_x^0 = q_{paraent(x)}(index(x))$. Let χ be the set of leaf nodes in the access policy tree, γ represent the set of attributes associated with the time range $[t_a, t_b]$, and Z represent the set of attributes associated with the location range $[l_a, l_b]$. The ciphertext CT is as follows:

$$\begin{aligned} CT = \Big\{ & \mathrm{T}, \tilde{C} = \mathrm{Enc}(\kappa, m), C = \kappa e(g,\omega)^{\alpha s}, C' = h^s \\ & \forall x \in \chi, C_x = \omega^{q_x^1}, C_x' = H_1(att(x))^{q_x^1} \\ & \forall y \in \gamma, C_y = \omega^{t_y^0}, C_y' = H_1(A_t)^{t_y^0} \\ & C_y'' = \left(v_{\{t_i,t_j\}}\right)^{t_y^0} = \varphi^{t_y^0 \lambda^{t^i} \mu^{z-t_j}} \\ & \forall z \in Z, C_z = \omega^{l_z^0}, C_z' = H_1(A_l)^{l_z^0} \\ & C_z'' = \left(v_{\{l_i,l_j\}}\right)^{l_z^0} = \varphi^{l_z^0 \lambda^{l^i} \mu^{z-l_j}} \Big\}. \end{aligned}$$

- Algorithm 4. Re-encryption algorithm

When a user requests access to the cloud server, the cloud server operates a re-encryption algorithm to convert the ciphertext CT to RC, which effectively ensures that the re-encrypted ciphertext is ultimately dependent on location and time. In particular, for each node $y \in \gamma, z \in Z$, the cloud server will examine whether time t_c and location l_c of the node satisfy the constraint of time range $[t_a, t_b]$ and the constraint of position range $[l_a, l_b]$. If not, label $\widetilde{C_y''}, \widetilde{C_z''}$ as the special symbol $\perp$; if the constraints are satisfied, the calculation below is operated:

$$\begin{aligned} \tilde{\mathrm{C}}_y'' &= \mathrm{C}_y \cdot F_{\{t_i \le t_c, t_j \ge t_c\}}(C_y'') \\ &= \mathrm{C}_y \cdot F_{\{t_i \le t_c, t_j \ge t_c\}} \left(v_{\{t_i,t_j\}}\right)^{t_y^t} \\ &= \mathrm{C}_y \cdot \left(\varphi^{t_y^0 \lambda^{t^i} \mu^{z-t_j}}\right)^{\lambda^{t_c - t_i} \mu^{t_j - t_c}} \\ &= \omega^{t_y^0} \cdot \left(v_{\{t_c,t_c\}}\right)^{t_y^0} \\ &= \left(v_{\{t_c,t_c\}} \omega\right)^{t_y^0}. \end{aligned}$$

$$\begin{aligned} \tilde{\mathrm{C}}_{\mathrm{z}}'' &= \mathrm{C}_z \cdot F_{\{l_i \le l_c, l_j \ge l_c\}}(C_z'') \\ &= \mathrm{C}_z \cdot F_{\{l_i \le l_c, l_j \ge l_c\}} \left(v_{\{l_i,l_j\}}\right)^{l_z^0} \\ &= \mathrm{C}_z \cdot \left(\varphi^{l_y^0 \lambda^{l_i} \mu^{z-l_j}}\right)^{\lambda^{l_c - l_i} \mu^{l_j - l_c}} \\ &= \omega^{l_z^0} \cdot \left(v_{\{l_c,l_c\}}\right)^{l_z^0} \\ &= \left(v_{\{l_c,l_c\}} \omega\right)^{l_z^0}. \end{aligned}$$

Thus the final re-encrypted ciphertext is

$$RC = \Big\{\mathrm{T}, C, C', \tilde{C}, \{\mathrm{C_x}, \mathrm{C_x'}\}_{\forall \mathrm{x} \in \chi}, \{\mathrm{C_y}, \mathrm{C_y''}\}_{\forall \mathrm{y} \in \gamma}, \{\mathrm{C}_z, \mathrm{C}_z''\}_{\forall z \in \mathrm{Z}}\Big\}.$$

The cloud server sends the encrypted ciphertext CT' to the user, as well as the current time t_c and current location l_c.

- Algorithm 5. Decryption algorithm

In the decryption phase, the user uses the private key to decrypt data. First define a recursive algorithm $DecrytNode(RT, SK_{gid}, x)$. Input ciphertext RC, private key $\mathrm{SK_{gid}}$, and node x.

If x is a leaf node, then let $i = attr(x)$.

If $i \in S_{gid}$, we have

$$\begin{aligned} F_x^{\mathrm{attr}} &= \mathrm{Decryt}\,No\,\mathrm{de}(RC, SK_{gid}, x) \\ &= \frac{e(D_i, C_x)}{e(D_i', C_x')} \\ &= \frac{e\left((gH_0(gid))^{u_j} H_1(i)^{r_i}, \omega^{q_x^1}\right)}{e\left(\omega^{r_i}, H_1(\mathrm{att}(x))^{q_x^1}\right)} \\ &= e(gH_0(gid), \omega)^{u_j q_x^1}. \end{aligned}$$

If $i \notin S_{gid}$, define $DecrytNode\left(CT', SK_{gid}, x\right) = \perp$.

Next we consider nodes $\forall y \in \gamma$, which include leaf and non-leaf nodes and require $t_c \in [t_i, t_j]$ and $t_c \in$

$[t_a, t_b]$ while ensuring secure access control within a valid time range. $A_t\,[t_i, t_j]$ is the access policy for node y in the access policy tree, and $A_t\,[t_a, t_b]$ is the time range when the user is given access right. When the access time is valid, it is calculated as follows:

$$\begin{aligned}\tilde{\mathrm{D}}_t'' &= F_{\{t_a \le t_c, t_b \ge t_c\}}\left(\mathrm{D}_{\mathrm{t}}''\right) \\ &= F_{\{t_a \le t_c, t_b \ge t_c\}}\left(v\,\{t_a, t_b\}\right)^{r_t} \\ &= \left(v_{\{t_c, t_c\}}\right)^{r_t}.\end{aligned}$$

$$\begin{aligned}F_{\mathrm{y}}^{\mathrm{time}} &= \frac{e\left(D_t, \tilde{C}_y''\right)}{e\left(D_t'\tilde{\mathrm{D}}_t'', C_y'\right)} \\ &= \frac{e\left(\left(gH_0(gid)\right)^{u_j} H_1\left(A_t\right)^{r_t}, \left(v_{\{t_c,t_c\}}\omega\right)^{t_y^0}\right)}{e\left(\omega^{r_t}\left(v_{\{t_c,t_c\}}\right)^{r_t}, H_1\left(A_t\right)^{t_y^0}\right)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j t_y^0} \cdot e\left(gH_0(gid), v_{\{t_c,t_c\}}\right)^{u_j t_y^0} \\ &= e\left(gH_0(gid), \omega\right)^{u_j t_y^0}.\end{aligned}$$

Similarly, we consider nodes$\forall z \in Z$ in the access policy tree, which include leaf and non-leaf nodes. Requirel $l_c \in [l_i, l_j]$ and $l_c \in [l_a, l_b]$ while ensuring secure access control within a valid time range. $A_l\,[t_l, t_l]$ is the access policy for node z, and $A_l\,[l_a, l_b]$ is the location range where a user is given access rights. When the access location is valid, then the calculation is as follows:

$$\begin{aligned}\tilde{\mathrm{D}}_l'' &= F_{\{l_a \le l_c, l_b \ge l_c\}}\left(\mathrm{D}_l''\right) \\ &= F_{\{l_a \le l_c, l_b \ge l_c\}}\left(v\,\{l_a, l_b\}\right)^{r_l} \\ &= \left(v_{\{l_c, l_c\}}\right)^{r_l}.\end{aligned}$$

$$\begin{aligned}F_{\mathrm{z}}^{loc} &= \frac{e\left(D_l, \tilde{C}_z''\right)}{e\left(D_l'\tilde{\mathrm{D}}_l'', C_z'\right)} \\ &= \frac{e\left(\left(gH_0(gid)\right)^{u_j} H_1\left(A_l\right)^{r_l}, \left(v_{\{l_c,l_c\}}\omega\right)^{l_z^0}\right)}{e\left(\omega^{r_l}\left(v_{\{l_c,l_c\}}\right)^{r_l}, H_1\left(A_l\right)^{l_z^0}\right)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j l_z^0} \cdot e\left(gH_0(gid), v_{\{l_c,l_c\}}\right)^{u_j l_z^0} \\ &= e\left(gH_0(gid), \omega\right)^{u_j l_z^0}.\end{aligned}$$

If a node x is independent of any time trapdoor and location trapdoor, namely, the trapdoor is not exposed, then the following equation is obtained:

$$\begin{aligned}F_x = F_x^{attr} &= e\left(gH_0(gid), \omega\right)^{u_j q_x^q} \\ &= e\left(gH_0(gid), \omega\right)^{u_j q_x^0}.\end{aligned}$$

If a node x is associated with a time trapdoor, obtain the following equation is obtained:

$$\begin{aligned}F_x &= F_x^{attr} \cdot F_x^{time} \\ &= e\left(gH_0(gid), \omega\right)^{u_j\left(q_x^1 + t_x^0\right)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j q_x^0}.\end{aligned}$$

If a node x is associated with a location trapdoor, the following equation is obtained:

$$\begin{aligned}F_x &= F_x^{attr} \cdot F_x^{loc} \\ &= e\left(gH_0(gid), \omega\right)^{u_j\left(q_x^1 + l_x^0\right)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j q_x^0}.\end{aligned}$$

If a node x is associated with a time trapdoor and a location trapdoor, the following equation is obtained:

$$\begin{aligned}F_x &= F_x^{attr} \cdot F_x^{loc} \cdot F_x^{\mathrm{time}} \\ &= e\left(gH_0(gid), \omega\right)^{u_j\left(q_x^1 + l_x^0 + t_x^0\right)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j q_x^0}.\end{aligned}$$

Finally we need to consider the recursive case when x is a non-leaf node. Child nodes z of node x constitute set S_x and the number of child nodes in the set is k_x. If there is no S_x, the decryption function returns $\perp$. Otherwise, the computation is operated as below:

$$\begin{aligned}\mathrm{F}_x^{\mathrm{attr}} &= \prod_{z \in S_x} F_z^{\Delta_i, S_x'(0)} \text{ where } \begin{cases} \mathrm{i} = \mathrm{index(z)} \\ \mathrm{S_x'} = \{\mathrm{index}(z) : z \in S_x\} \end{cases} \\ &= \prod_{z \in S_x}\left(e\left(gH_0(\ \mathrm{gid}\ ), \omega\right)^{u_j q_x^0}\right)^{\Delta_i, S_x'(0)} \\ &= e\left(gH_0(gid), \omega\right)^{u_j q_x^1}.\end{aligned}$$

Concerning the root node R, if the access control policy is satisfied, we will get

$$F_{\mathrm{R}} = e\left(gH_0(gid), \omega\right)^{u_j q_R^0} = e\left(gH_0(gid), \omega\right)^{u_j s}.$$

So the ciphertext can be decrypted to get the plaintext:

$$\kappa = \frac{C}{e\left(D, C'\right) \cdot F_R}.$$
$$\mathrm{m} = \mathrm{Dec}(\kappa, \tilde{C}).$$

6 TSC-CABE Analysis

6.1 Security Analysis

- Security model

This paper sets up a security simulation by attacker Alice and challenger Bob.

Initialization 1: Alice challenges the access structure Γ.Assume that it knows the relevant access policy A_P consisting of the set of attributes, the constraint T_P consisting of the time range, the constraint L_P consisting of the location range.

Initialization 2: Bob gets the public parameter PKP and the master key MK by operating the system initialization algorithm, and sends PKP to Alice.

Phase 1: Alice submits the private attributes, time interval and location range $T_{gid} = [t_a, t_b], L_{gid} = [l_a, l_b]$ of its own query to Bob. Then Bob gets SK_U based on the above information by operating the key generation algorithm and sends it to Bob.

Challenge: Bob Alice sends Alice Bob two messages m_0, m_1, of the same length as message M. Alice Bob selects any bit $b \in \{0, 1\}$ encrypts message M by accessing structure tree T to get m_b, and then sends the ciphertext to Alice.

Phase 2: Bob Alice repeats phase 1, and it is assumed that Bob Alice gets its own location range through AliceBob. However, due to $(S_u \wedge TI_u \wedge LP_u) \notin \Gamma$, the decryption fails.

Guess: Suppose that Bob Alice guesses that b could be b', the probability of the opponent making guesses during the entire game is $Pr\left[b' = b\right] - 1/2$.

Definition 1. *If all opponents with temporal polynomials have a non-negligible advantage to some extent, the proposed TSC-CABE scheme can be effective in defending against selective plaintext attacks.*

- Security for different types of enemy attacks
We further divide the attackers of the TSC-CABE scheme into two categories.

  1) Attackers who do not satisfy the attributes in the access tree.
  2) Attackers who do not satisfy the location/time range in the access tree.

  If it successfully defends against the two types of attacks, the scheme is resistant to any individual attack.

  The TSC-CABE scheme is further optimized on the basis of the TSC-CABE scheme by embedding the location range constraint into the access policy, but its algorithm does not destroy the structure of the original scheme, therefore, this scheme has the same data confidentiality as the TSC-ABAC scheme when attacked by type 1 attackers.

  We flexibly use the trapdoor in this scheme to embed location range constraint and time range constraint in the access tree. The setting and exposure of the trapdoor enable an identity-based encryption scheme, thus the scheme is secure in the random oracle model. It is impossible to obtain authorized access for attackers who do not satisfy the time and location range constraints.

- Security for different source attack
The TSC-CABE scheme resists illegal access from many different sources

  1) Resistance to illegal access from the cloud storage platform
  When encrypting data, the data owner first encrypts the message m with a symmetric key $ek \in G_T$ and then encrypts ek according to the defined access policy. The symmetric key is maintained by the cloud storage platform, but to decrypt the data, the root node value s of the access tree needs to be restored, which the cloud storage platform fails to do. As a result, the platform cannot share the secret data, and the scheme can effectively prevent the cloud storage platform from illegally accessing the data.
  2) Resistance to illegal access from time/location servers
  In the TSC-CABE scheme, the time/location servers only play a role in decrypting the trapdoor associated with time/location and have no other privileges to compromise the security of the scheme. If a time server or location server is attacked, it will only affect access to the relevant point, while other part of access control related to attributes or associated with temporal constraints is not affected.
  3) Resistance to illegal access from authorized institutions
  If it obtains the attribute key through illegal channels, to further decrypt the shared data, the authorized organization needs to obtain the symmetric key ek first. According to the bilinear mapping theory, the authorized institution has to collude with the cloud storage platform to obtain ek, but in our model, both are semi-trusted and there is no possibility of collusion. Therefore, this scheme can effectively prevent the authorized organization from accessing the data illegally.

6.2 Comprehensive analysis

- Function characteristics analysis
Concerning the analysis of functional characteristics, we compare the TSC-CABE scheme with the CP-ABE [21], CBE [29], PPLBAC [2], and TSC-ABAC [17] schemes as shown in Table 1. These schemes give solutions to handling dynamic attributes in the access control based on attribute-based encryption, The CP-ABE scheme achieves fine-grained access control by using an access policy tree that encrypts the user's set of attributes as leaf nodes, but the scheme is too old and more factors need to be considered at present. Seeing the access control is associated with multiple attributes, the CBE [22] scheme integrates comparison between attributes into the access control process, which enables the comparison of multiple attributes of users in the access process and achieves flexible access control. The TSC-ABAC scheme and the PPLBAC scheme consider temporal

and spatial constraints, but time and location are discussed separately. We consider both location and time as normal properties like user name and age, and propose the TSC-CABE scheme, which takes into account the temporal and spatial constraints, and does not require the extra revocation during access, making the whole access process more efficient and flexible.

Table 1: Comparison with other options

Schemes	[21]	[29]	[17]	[2]	Ours
fine-grained	√	√	√	√	√
Support for attribute comparison	×	√	√	√	√
Time frame constraint	×	×	√	×	√
Position range constraint	×	×	×	√	√
Attribute to cancel	Yes	No	No	No	No

- Complexity Analysis
  In this section, the TSC-CABE scheme is compared with the CBE scheme and the TSC-ABAC scheme. Similar to the CBE and TSC-ABAC schemes, our scheme focuses only on the bilinear pair and exponential operations in G and G_T and ignores the hash function operation and the multiplication operation. $|N|$ in the scheme represents the number of leaf nodes in the access policy tree. $|N_{A_t}|$, $|N_{A_l}|$ denote the number of nodes associated with the time range and location range respectively and $|A|$ is the number of attributes involved in encryption and decryption process. l_G, l_{G_T}, l_{Z_n} denote the size of the elements in G, G_T, Z_n respectively.P denotes the overhead consumed by a bilinear pairing, and $E(G), E(G_T)$ represents the exponential computation overhead in G, G_T.

  In Table 2, we compare the key size and ciphertext size of the three schemes. In our scheme, the total number of leaf nodes in the access policy tree is much larger than the number of nodes associated with location or time trapdoors, and there is no need for each server to generate parameters during the initialization phase. Therefore the storage cost is significantly reduced. In Table 3 and Table 4, We make comparison in terms of communication overhead and computational complexity. Since the CBE scheme cannot handle non-comparison based attributes, and the TSC-ABAC scheme cannot handle continuous location range, it is assumed that only a time trapdoor and a location trapdoor are embedded in our scheme, which are $|N_{A_t}|= 1$, $|N_{A_l}|= 1$. As shown in Table 3, our scheme handles simultaneously location range and time range without incurring additional expenses.

7 Research Developments

In most existing CP-ABE schemes, such as [4, 9, 21, 24], only one authority is responsible for maintaining the entire set of attributes, which can create a single point of bottleneck. Once the single authority breaks down, the system is paralyzed. Moreover, in real scenarios, attributes vary and require different authorities to distribute keys. Although CP-ABE schemes with multiple authorities have been proposed as in [5, 12, 15], those schemes fail to effectively deal with single-point bottlenecks and improve performance.

Literature [13] proposes a new multi-authority CP-ABE scheme called the TMACS scheme, which is a gated multi-authority access control scheme for public cloud storage. Multiple authorities jointly manage a set of attributes. The TMACS scheme utilizes a (t,n) threshold secret sharing mechanism in order that multiple authorities share the master key. The user needs to interact with t of the authorities to obtain the key. In other words, communication between AAs is not required during the key generation phase, which reduces coupling between attribute institutions. The scheme greatly reduces the communication overhead between AAs, but a problem is ensued that the computational overhead increases since each AA generates the key independently. To solve it, outsourcing the calculation to a cloud server can be considered on the premise of ensuring safety and reliability.

Based on the above analysis, this paper proposes a multi-authority access control scheme based on comparative attributes of spatio-temporal constraints in the cloud.

We regard spatio-temporal factors as normal attributes, and formulate a brief and secure MA-ABE cross-domain data access control scheme. The data owner (DO) defines the access policy tree based on the access policy, encrypts the data based on the tree, and then uploads the ciphertext to the cloud. In addition, DO generates some private key components to prevent joint attacks from several AAs and send them to users through secure channels. Users can freely obtain the ciphertext in the server, but decryption can be successful only when the attributes the user possesses satisfy the requirements of the access policy tree. When a user's attributes change, the cloud needs to re-encrypt the ciphertext and redistribute the private key components. As an attribute generation and authorization institution, AA is responsible for distributing attributes to authorized users and data owners and generating part of attribute-related private key components. CA is a trusted central authentication institution, which is responsible for generating a series of public parameters at the initial stage of authentication. The cloud server is an unreliable storage medium, which is mainly used to store user data.

The solution is as follows:

Table 2: Comparison of storage costs

Schemes	CBE	TSC-ABAC	Ours
key	$(1+4\|A\|)l_G$	$(5+2\|A\|)l_G$	$(7+3\|A\|)l_G$
cipher	$(1+4\|N\|)l_G+1\cdot l_{G_T})$	$(2+2\|N\|+2\|N_{A_t}\|)l_G+1\cdot l_{G_T}+1\cdot l_{Z_n}$	$(2\|N_{A_l}\|+2\|N\|+2\|N_{A_t}\|)l_G$ $+1\cdot l_{G_T}+1\cdot l_{Z_n}$

Table 3: Communication cost comparison

Schemes	CBE	TSC-ABAC	Ours
Setup	$1\cdot p+3\cdot E(G)$	$1\cdot P+(2+\|L\|)\cdot E(G)$	$1\cdot P+2\cdot E(G)$
KenGen	$(1+5\|A\|)\cdot E(G)$	$(7+3\|A\|)\cdot E(G)$	$(9+4\|A\|)\cdot E(G)$
Encrypt	$(1+4\|N\|)\cdot E(G)$ $+1\cdot E(G_T)$	$(2+2\|N\|+3\|N_{A_t}\|)\cdot E(G)$ $+2\cdot E(G_T)+1\cdot P$	$(3\|NAl\|+2\|N\|+3\|N_{A_t}\|)\cdot E(G)$ $+2\cdot E(G_T)+1\cdot P$
ReEncry	–	$\|N_{A_t}\|\cdot E(G)$	$(\|NAt\|+\|NAl\|)\cdot E(G)$
LocToken	–	$1\cdot P+1\cdot E(G_T)+1\cdot E(G)$	–
Delegate	$(1+5\|A\|)\cdot E(G)$	$(5+2\|A\|)\cdot E(G)$	–
DecryptProxy	$(1+4\|A\|)l_G$	$(2\|A\|+4)\cdot P+1\cdot E(G)+\|N\|\cdot E(G)$	–
DecryptUser	$1\cdot P+1\cdot E(G)$	$1\cdot E(G_T)$	$1\cdot E(G_T)$

Table 4: Calculate the cost comparison

scheme	CBE	TSC-ABAC	Ours
Setup	$6\cdot l_G+1\cdot l_{G_T}+2l_{Z_n}$	$(\|L\|+5)\cdot l_G+1\cdot l_{G_T}+2\cdot l_{Z_n}$	$5\cdot l_G+1\cdot l_{G_T}+2\cdot l_{Z_n}$
KenGen	$(1+4\|A\|)l_G$	$(5+2\|A\|)l_G$	$(7+3\|A\|)l_G$
Encrypt	$(1+4\|N\|)l_G+1\cdot l_{G_T}$	$(2+2\|N\|+2\|N_{A_t}\|)\cdot l_G+1\cdot l_{G_T}+1\cdot l_{Z_n}$	$(2\|N_{A_l}\|+2\|N\|+2\|N_{A_t}\|)l_G+1\cdot l_{G_T}+1\cdot l_{Z_n}$
ReEncry	–	–	–
LocToken	–	$2\cdot l_G+l_{Z_n}$	–
Delegate	$3\|A\|\cdot l_G$	$(6+2\|A\|)\cdot lG$	–
DecryptProxy	$1\cdot l_G+1\cdot l_{G_T}$	$1\cdot l_G$	–
DecryptUser	–	–	–

1) Initialization:Select the multiplication group G of prime order p. g is the generator of G. Construct the bilinear map $e : G \times G \to G_T$,randomly select $\alpha, \eta \in Z_P$, and generate the public key:

$$\begin{aligned} \mathrm{PK} &= (g, G, g^{\eta}, e(g,g)^{a}) . \\ MSK &= (g^{a}, \eta) . \end{aligned}$$

2) Encryption (PK, M, Γ): The data owner encrypts the message M according to the defined access policy. Firstly, the DO formulates an access policy tree according to the attributes distributed by each AA, and randomly selects $s, \rho, \eta \in Z_P$,so the value of the root node is $q_r(0) = s$. The private key value $\frac{q_y(0)}{\rho}$ is assigned to each leaf node in the tree in a top-down manner and the private key value of each leaf node is used for encryption. Let Y be the set of leaf nodes, the ciphertext is as follows:

$$\begin{aligned} &CT = (T, C' = M \cdot e(g,g)^{\alpha s}, C = g^{\eta s}, \\ &\forall y \in Y, C_y = H(\mathrm{att(y)})^{q_y(0)/\rho}, C_{y'} = g^{q_y(0)/\rho} \Big) . \end{aligned}$$

3) Key generation (MSK, S): Private key generation is completed by the DO and AA.

- The DO randomly selects $\lambda \in Z_P$ to generate the private key component,$D = g^{(\alpha-\lambda)/\eta}$,and sends D and parameter λp to the user through a secret channel. Since the λp value of each user's private key is different, it can prevent joint attacks launched by a group of users.
- Each AA randomly selects $r_i \in Z_P$,and generates the corresponding attribute private key component for any attribute $k \in S_j$:
  $\mathrm{SK}_j = (\forall k \in S_j, \mathrm{V}_i = g \cdot H(i)^{r_i}, \mathrm{L}_i = g^{r_i})$
  where $j = 1, \cdots, n, S_j$ represents the attribute set distributed to users by the jth AA. Let each AA send SK_j to the user via a secure channel.

4) Decryption (CT, SK): The decryption is divided into two parts, decryption by the CSP and decryption by the user. The CSP is only responsible for partial decryption of the data, and the decryption result is sent to the user. Although it can obtain partial result, the CSP cannot obtain the final plaintext, because the key parameter λp is only known by the DO and the user, which ensures the security of the data. The operation is as follows:

- Decryption by the CSP (DK): After receiving the key sent by the DO and each AA, the user sends the private key component $SK_j \in (1, \cdots, n)$ the CSP. The CSP receiving the private key component sent by the user, the decryption algorithm is operated, where the ciphertext as an access policy tree and the private key $SK_j \in (1, \cdots, n)$ are entered. The decryption is performed from bottom to top by an recursive algorithm to generate the parameters required for decryption. Let $i = attr(y)$, and $attr(y)$ denotes the attribute value of leaf node y. If x is a leaf node and $x \in S$, then there are

$$\frac{e(V_i, C'_x)}{e(L_i, C_x)} = \frac{e\left(g \cdot H(i)^{r_i}, g^{q_y(0)\rho}\right)}{e\left(g^{r_i} \cdot H(i)^{q_y(0)\rho}\right)} = e(g,g)^{q_y(0)\rho}.$$

If x is not a leaf node, for all child nodes z of node x, the result of decryption is denoted as F_Z. Let S_x be the set of child nodes z with the size of K_x. If there is no S_x, then the node x does not satisfy the requirements, the function returns $\perp$. Otherwise, perform the calculation below:

$$\begin{aligned} \mathrm{F}_x &= \prod_{z \in S_x} F_z^{\Delta_i, S'_x(0)} \\ &= \prod_{z \in S_x} \left(e(g, \quad g)^{q_z(0)/\rho}\right)^{\Delta_i, S'_x(0)} \\ &= e(g, \quad g)^{q_x(0)/\rho}. \end{aligned}$$

$$\text{where} \begin{cases} \mathrm{i} = \mathrm{index(z)} \\ \mathrm{S'_x} = (\mathrm{index}(z) : z \in S_x) \end{cases}$$

The algorithm calls the Lagrange interpolation function that generates the access policy tree. If the attribute set S satisfies requirements of the access policy tree Γ, then we have

$$DTK = e(g,g)^{q_R(0)\rho} = e(g,g)^{\frac{s}{\rho}}.$$

CSP calculates the DK and sends it to the legitimate user.

- User decryption: After receiving the DK sent by the CSP, the user uses the private key sent by the DO to decrypt again and the calculation below is operated.

$$\begin{aligned} &\left(e(D, C) \cdot (DTK)^{\lambda\rho}\right) \\ &= e\left(g^{(\alpha-\lambda)/\eta}, g^{\eta s}\right) \cdot e(g,g)^{\lambda\mu s/\rho} \\ &= e(g,g)^{\alpha s}. \end{aligned}$$

The result is

$$M = \frac{\mathrm{C}'}{e(g,g)^{\alpha s}}.$$

8 Conclusions

In the encryption of the access control scheme based on spatio-temporal constraints, we optimize the encryption structure of the traditional ABE scheme. The traditional ABE scheme uses the access policy tree to encrypt user's attributes, based on which the structure of the access policy tree is re-designed and the time and

location constraints are embedded into the access. The multi-dimensional distance derivation function combined with the trapdoor is used to determine the legitimacy of the user and improve the flexibility of the access process. Finally, through security analysis, function characteristics analysis, comparison of communication overhead and computation overhead, it is shown that the proposed comparative attribute-based encryption scheme based on spatio-temporal constraints is more efficient, flexible and secure than other attribute-based encryption schemes.

In the scheme, we modify the access policy tree to include temporal and spatial constraints. At the same time, we integrate the multidimensional range derivation function and embed it into the process of attribute encryption. The function utilizes the one-way property to represent the total order of integers, thus users who meet the constraints can access resources more flexibly.We also propose a multi-authority access control scheme in cloud environment based on spatio-temporal constraint comparison attributes. In future research, we will start from multi-attribute authorization institutions to study the access control scheme based on attribute encryption in cloud environment, so as to reduce its computing and communication costs. At the same time, we will consider whether users can be unaware in the process of encryption and decryption, and consider whether useless attributes can be eliminated from the perspective of space-time constraints, so as to further reduce the cost of related attributes in the process of encryption and decryption and improve the performance of the algorithm.

Acknowledgments

This study was supported by the Key Project Foundation of Tianjin under Grant 15ZXHLGX003901, Tianjin Natural Science Foundation under Grant 19JCYBJC15800 and National Natural Science Foundation of China under Grant 61802281 and 61702366. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] E. Androulaki, C. Soriente, L. Malisa, S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in *IEEE 34th International Conference on Distributed Computing Systems*, pp. 637-648, 2014.

[2] Y. Baseri, A. Hafid, S. Cherkaoui, "Privacy Preserving Fine-grained Location-based Access Control for Mobile Cloud," *Computers and Security*, vol 73, pp. 249-265, 2017.

[3] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-Policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[4] R. Bobba, H. Khurana, M. Prabhakaran, "Attribute-Sets: a practically motivated enhancement to attribute-based encryption," in *Computer Security - ESORICS 2009, 14th European Symposium on Research in Computer Security, Saint-Malo, France, September*, pp.21-23, 2009.

[5] M. Chase, "Multi-authority attribute based encryption," in *Proceedings of the 4th conference on Theory of cryptography February 2007*, pp. 515–534, 2007.

[6] G. Choi, S. Vaudenay, "Timed-Release Encryption with Master Time Bound Key," *Information Security Applications*, pp. 167-179), 2020.

[7] I. Denisow, S. Zickau, F. Beierle, A. Küpper, "Dynamic location information in attribute-based encryption schemes," in *9th International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 240-247, 2015.

[8] H. Ghafghazi, A. Elmougy, H. T. Mouftah, C. Adams, "Location-aware authorization scheme for emergency response," *IEEE Access*, vol. 4, pp. 4590-4608, 2016.

[9] V. Goyal, A. Jain, O. Pandey, A. Sahai, "Bounded Ciphertext Policy Attribute Based Encryption," in *Proceedings of the 35th international colloquium on Automata, Languages and Programming*, Part II. DBLP, 2008.

[10] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Ciphertext-Policy attribute-based encryption," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, 2006.

[11] J. Hong, K. Xue, Y. Xue, W. Chen, D. L. Wei, N. Yu, P. Hong, "TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud," *IEEE Transactions on Services Computing*, vol. 13, no. 1, pp. 158-171, 2020.

[12] A. Lewko, B. Waters, "Decentralizing attribute-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques Springer, Berlin, Heidelberg*, 2011.

[13] W. Li, K. Xue, Y. Xue, J. Hong, "TMACS: A robust and verifiable threshold multi-Authority access control system in public cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1484-1496, 2016.

[14] X. Li, T. Jung, "Search me if you can: Privacy-preserving location query service," in *2013 Proceedings IEEE INFOCOM*, pp. 2760-2768, 2013.

[15] H. Lin, Z. Cao, X. Liang, J. Shao, "Secure threshold multi-authority attribute based encryption without a central authority," *Information Sciences*, vol. 180, no.13, pp. 2618-2632, 2010.

[16] S. Liu, A. Liu, A. Yan, W. Feng, "Efficient LBS queries with mutual privacy preservation in IoV," *Vehicular Communications*, vol 16, pp. 62-71(10), 2019.

[17] Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, R. Zhang, Y. Wu, "A temporal and spatial constrained attribute-based access control scheme for cloud storage," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 614-623, 2018.

[18] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," *Concurrency and Computation: Practice and Experience*, vol 31, 2016.

[19] A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 3494, pp. 457-473, Springer, 2005.

[20] J. Shao, R. Lu, X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 244-252, 2014.

[21] E. Shi, J. Bethencourt, T. H. Chan, D. Song, A. Perrig, "Multi-Dimensional range query over encrypted data," in *2007 IEEE Symposium on Security and Privacy (SP'07)*, pp. 350-364, 2007.

[22] S. B. Wang, Y. Zhu, D. Ma, R. Q. Feng, "Lattice-based key exchange on small integer solution problem," *Sci. China Information Sciences*, vol. 57, pp. 1-12, 2014.

[23] Z. Wang, D. Huang, Y. Zhu, B. Li, C. J. Chung, "Efficient attribute-based comparable data access control," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3430–3443, 2015.

[24] B. Waters, "Ciphertext-Policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *AInternational Workshop on Public Key Cryptography Springer Berlin Heidelberg*, pp. 53-70, 2008.

[25] Q. Xie, L. Wang, "Efficient privacy-preserving processing scheme for location-based queries in mobile cloud," in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, pp. 424-429, 2016.

[26] Y. Xue, J. Hong, W. Li, K. Xue, P. Hong, "LABAC: a location-aware attribute-based access control scheme for cloud storage," in *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, 2016.

[27] K. Yang, Z. Liu, X. Jia, X. S. Shen, "Time-Domain attribute-Based access control for cloud-based video content sharing: A cryptographic approach," *IEEE Transactions on Multimedia*, vol. 18, no. 5, pp. 940-950, 2016.

[28] Y. Zhu, G. J. Ahn, H. Hu, S. S. Yau, H. G. An, C. J. Hu, "Dynamic audit Services for outsourced storages in clouds," *IEEE Transactions on Services Computing*, vol. 6, no. 2, pp. 227-238, 2013.

[29] Y. Zhu, H. Hu, G. J. Ahn, M. Yu, H. Zhao, "Comparison-based encryption for fine-grained access control in clouds," in *Proceedings of the second ACM conference on Data and Application Security and Privacy*, pp. 105–116, ACM, 2012.

[30] Y. Zhu, D. Ma, D. Huang, and C. Hu, "Enabling secure location-based services in mobile cloud computing," in *Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing*, pp. 27-32, ACM, 2013.

Biography

Junling Zhang is a graduate student of Tiangong University with a master's degree in software engineering.She received a bachelor's degree from Shanxi University in 2020. Her research interests include information security, privacy protection, access control and cryptography.

Ze Wang received the B.E. and M.E. degrees from Xi'an Jiaotong University, China, in 1998 and 2001, respectively, and the Ph.D. degree in computer applications technology from Northeastern University, China, in 2004. Since December 2016, he has been a Professor with the School of Computer Science and Technology, Tiangong University, China. His primary research interests include network security, big data modeling and analysis, and privacy computing.

Ping Zhao is a graduate student of Tiangong University with a master's degree in computer science and technology. He received a bachelor's degree from Tiangong University in 2018. His research interests include information security, blockchain data security and privacy protection.

Minghua Gao received a master's degree from Tiangong University in 2021.He received the bachelor degree from Tiangong University in 2018. His research interests include network security and mobile computing.

Shimin Sun received the M.S. and Ph.D. degrees in computer and information communication engineering from the Konkuk University of Korea, in 2009 and 2016, respectively. He is currently an associate professor with Tiangong University, China. His research interests include software-defined networking, the future network architecture, cloud computing, edge computing, and network security.

A Trust Assessment Mechanism of the IoV Based on Multi-factor Analytic Hierarchy Process

Peng-Shou Xie, Xin Tong, Hong Wang, Ying-Wen Zhao, Tao Feng, and Yan Yan
(Corresponding author: Xin Tong)

School of Computer and Communications & Lanzhou University of Technology
No. 36 Peng jia ping Road, Lanzhou, Gansu 730050, China
Email: 2505156603@qq.com

(Received July 25, 2021; Revised and Accepted Jan. 28, 2022; First Online Apr. 9, 2022)

Abstract

The impact of multiple factors on the trust of vehicle nodes is considered comprehensively in this paper, a trust assessment mechanism for the Internet of Vehicles is proposed. For multi-application scenarios, the analytic hierarchy process is used to quantify the degree of influence of each factor on vehicle trust in different application scenarios; initial trust is added to prevent vehicle cold start; Bayesian approach is improved based on the same quality of service strength, dynamic trust decay and malicious event influence; cosine similarity is employed to optimize recommendation trust weights, and weighted to establish global Roadside Unit trust. The effectiveness of this evaluation mechanism in portraying node behavior, identifying malicious nodes, and suppressing malicious recommendation behavior is verified by simulation experiments. The experiments show that this paper has advantages in recommendation trust evaluation accuracy and vehicle interaction success rate compared with other methods.

Keywords: Analytic Hierarchy Process; Cosine Similarity; Internet of Vehicles; Multi-Factor; Trust Assessment Mechanism

1 Introduction

The main purpose of Internet of Vehicles (IoV) is to improve road safety and reduce traffic congestion [6]. In recent years, with the rapid development of in-vehicle technologies, control technologies, wireless communication technologies, Internet of Things and information physical systems, the IoV has become an important research area [16]. However, the open network environment and diverse system resources of the Iov are prone to false information, rapid changes in network topology, and unreliable message propagation [25, 27–29], leading to threats to Iov security. Therefore, there is an urgent need to establish a reliable trust assessment mechanism for mutual communication between Iov vehicles to ensure a trusted communication environment and the security and stability of the network [19].

For IoV security-related applications, it is a very important task to ensure that the communication entities meet the trust requirements. In the trust assessment of wireless sensor networks, a fully mediated approach using node internal resources to assess node-level trust is proposed, which enables nodes to assess their own trust level [4]. In response to the traditional static trust model that cannot effectively create trust relationships between vehicles and cannot quickly and dynamically handle frequent vehicle interactions in the network topology, a novel trust model is established from initialization, service demand discovery, distributed evaluation and authentication, and trust transformation by improving trust chains and trustworthy computing theory [26]. For the traditional trust approach is not adapted to the cloud environment with dynamic attribute changes, an evidence-based trust model is proposed, this model uses various attributes of cloud services as evidence factors, it outperforms other models in terms of accuracy and efficiency [5]. To address the lack of objectivity and accuracy of the trust assessment model of wireless sensor network nodes, some researchers have improved the trust assessment model by combining trust management mechanism, trust factors, fuzzy sets and DS evidence theory to improve the security of the network [30]. Some researchers propose a multi-parameter trust calculation method which observes and detects malicious behavior of nodes based on time series theory [12]. There are also researchers who trustevaluate based on clusters and blockchains [11, 24]. In electric vehicle networks [21], researchers used maximum neighbor distance and access trees to improve the efficiency of trust assessment and reduce the whole transmission hops for trust assessment, thus extending the lifetime of the network. In in-vehicle self-organizing networks a method based on Hidden Markov Model for vehicle trust evaluation was proposed to improve the efficiency of trust updates and queries [15]. In the trust assessment of cloud services, researchers build a model based on weight and gray correlation analysis and use rough set theory and analytic hier-

archy process for direct trust by forming a comprehensive trust together with recommended trust [22]. The above-mentioned references on trust assessment of the IoV lacks consideration of Roadside Unit (RSU) in node assessment, and the trust features in recommended trust differ significantly from the evaluated entities, and the identification of malicious nodes needs further enhancement.

In order to correctly and effectively identify malicious nodes and provide trust support for vehicle interaction, this paper proposes a multi-factor trust evaluation mechanism based on hierarchical analysis. The trust of multiple factors of the vehicle is evaluated: including initial trust, direct trust, recommended trust, RSU global trust, and finally the adaptive weights of each factor are obtained by hierarchical analysis according to the application scenario, so as to aggregate and get the comprehensive trust value. The rest of this paper is organized as follows: Section 2 introduces the IoV network framework and trust assessment framework. In the framework of trust assessment, the problems existing in each module and research ideas are described in detail. Section 3 introduces the trust evaluation method in each module in detail. Section 4 shows the simulation experiment configuration environment and the results and analysis.

2 Trust Assessment Framework of the IoV

2.1 Network Framework of IoV

The IoV refers to a mobile communication network that combines wireless communication technology with a vehicle network and provides value-added services to vehicle users based on the social relationship between vehicles that communicate with each other. The IoV can continuously monitor and share road and traffic conditions. The main components of the IoV are vehicles embedded in On-board units (OBU), RSU, communication components including Radio frequency antenna antennas and processing units, and telecommunication networks, such as satellite communications.

The main communication technologies are our c-ellular vehicle networking [2] and IEEE802.11p. Th-ere are three main communication modes [13], Interv-ehicle communication (V2V), Vehicle-to-road-side com-munication (V2I), Interroad-side communication (I2I).

V2V: in this mode of communication vehicles with another vehicle with the help of OBU in every vehicle. In this communication mode, vehicle to vehicle communication with each other with wireless technology.

V2I: in this mode of communication, vehicles will communicate with the roadside communication equipment RSU. Furthermore, in this mode, a direct wireless communication link is established between vehicle and infrastructure units located around the road.

I2I: in this mode, communication RSU communicates with another RSU and core network, for example, 5G, satellite, or wired telecommunication system.

Trusted authority (TA): Trusted authority is the heart of the IoV system.The primary responsibility is registering the RSUs,OBUs,and vehicles.Secondary responsibilities include ensuring safety management through vehicle identity verification,user identification and OBU identification,and assigning initial trust to the vehicle.

RSU: these are communication-based units installed near highways, which transmit useful information to vehicles that came in the radio range of RSU. They are connected to a central network with means of wired or wireless. The network framework of the IoV is shown in Figure 1.

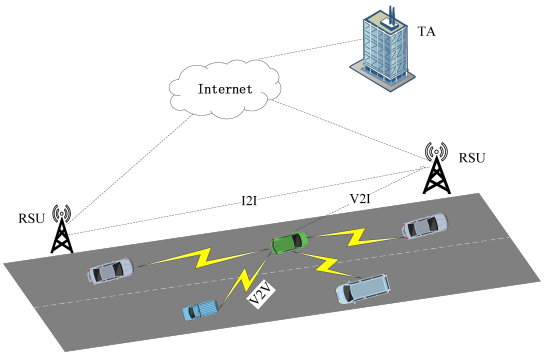


Figure 1: Internet of Vehicles network framework

2.2 Trust Evaluation Framework of the IoV

Trust is a subjective behavior. Vehicle nodes can choose which nodes to cooperate with. In the IoV, messages are filtered through mutual trust evaluation between vehicles. The trust assessment framework in this paper consists of the following modules. Initial Trust Module; Direct Trust Module; Recommended Trust Module; RSU Trust Module. Since vehicles can only interact when a trust value is available, the initial trust value setting provides the trust basis for direct vehicle interaction. The calculation of the direct trust value also provides the basis for the calculation of the recommended trust and RSU fusion trust. The proposed framework studies the computational approach between several trust modules. The dynamic weights of each module are calculated by the analytic hierarchy process, and then combined and weighted to obtain the comprehensive trust value.The trust evaluation framework is shown in Figure 2.

The problem analysis and research ideas of each module are described as follows.

A. Initial Trust Module

In the IoV, when a newly added vehicle node communicates with other vehicle nodes, other vehicle nodes cannot find the trust value to authenticate the new vehicle node, so a cold start problem occurs [8].

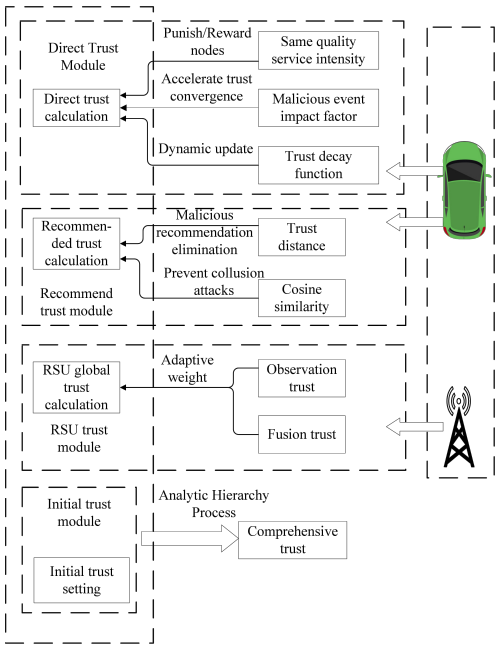


Figure 2: Trust evaluation framework

To address the above issues, the research idea of this paper is: Because newly registered vehicles do not have historical interaction data records, the legitimacy of the vehicle cannot be judged, so newly registered vehicles cannot have a high trust value. Therefore, the initial trust can be set to 0.1-0.4 according to the vehicle safety related attributes, which can effectively solve the problem of cold start (trust value = 0). Vehicle safety related attributes include: vehicle type, vehicle ID, whether there is security hardware support, etc.

B. Direct Trust Module

The main problems in direct trust assessment are as follows.

1) In most direct trust assessment methods based on Beta distribution, static decay factors are employed to achieve the decay of historical trust, but it is difficult to guarantee the validity of trust assessment;
2) Trust is built slowly during the node interaction. Ceteris paribus, trust value increases slowly due to good behavior and decreases quickly due to malicious behavior;
3) In the IoV, the quality of service of vehicle nodes may be affected when they are affected by non-intrusive factors such as signal interference. If the impact of non-intrusive factors is ignored and causes failed interactions, it will not be able to effectively distinguish malicious nodes from nodes with occasional abnormal behavior;

Taking into account the above problems, the research ideas of this paper are as follows.

1) Considering the time factor of direct trust [14], a dynamic trust decay function is designed to combine the historical trust value of the node with the latest observation value to realize the dynamic update of the direct trust value;
2) To increase the influence of malicious events, the effect of malicious events is introduced in this paper to quickly converge the trust value to within the trust threshold, thus speeding up the detection of malicious nodes;
3) To better characterize the behavior of nodes, effectively distinguish malicious nodes, and avoid malicious nodes from participating in cooperation, this paper designs the same quality service intensity evaluation factor to evaluate the overall behavior of nodes in the continuous monitoring cycle, and according to the same quality of nodes in the monitoring cycle Service intensity punishes nodes that continue to provide malicious services or motivates legitimate nodes;

C. Recommend Trust Module

The main problems with the recommended trust node calculation are as follows.

1) Malicious recommendations from malicious nodes;
2) Complex calculations required in the recommendation delivery process;
3) Malicious nodes are prone to perform malicious recommendations after obtaining high trust ratings from evaluation nodes by providing good services, which reduces the accuracy of recommendation trust calculation;

Considering the above problems, the research ideas are as follows.

1) To reduce malicious recommendations and improve the honesty of recommendations, trust distance is used in the computation of recommendation trust to exclude some malicious recommendation nodes;
2) To reduce the complicated calculation caused by recommendation transmission, this paper only considers the recommendation opinions of neighboring nodes within one hop of the subject;
3) Optimizing the weight calculation of recommendation trust using cosine similarity, reduce the situation that the trust characteristic of the malicious recommendation node is quite different from the evaluation entity, to improve the accuracy and reliability of the trust evaluation;

D. RSU Trust Module

The RSU acts as a roadside unit to detect the various states of the vehicle nodes, and when a vehicle

enters the communication range of the RSU the vehicle transmits the acquired trust value to the RSU. then the RSU fuses the trust of other vehicle nodes about a certain vehicle node. Therefore, RSU trust considers two aspects.

1) Various state attributes of the vehicle. As the trajectory of the vehicle changes, trust can be transmitted between RSUs in real-time. As an observer, the RSU will make a trust assessment of the various states of the vehicle;
2) A report on the trust value of a vehicle node to other vehicle nodes;

Considering the above problems, the research ideas are as follows.

1) Considering the different effects of different state attributes in the node trust calculation process, assign relevant values and weights to vehicle-related state attributes;
2) RSU integrates the trust value reported by other vehicles on a certain vehicle;

3 Trust Evaluation Method of IoV

3.1 Direct Trust Assessment

The validity of the trust record of the target vehicle node changes dynamically with the increase of time. The trust record that is far away from the current transaction time has a weaker ability to react to the current attributes of the node, while the nearest trust record is relatively more able to reflect the current node attributes and behavioral intentions.

To make more reasonable use of historical records, the distance between the moment of trust record generation and the current moment is adopted to measure the decay of trust records in the historical trust sequence, and accordingly improve the trust decay method based on the length of time window. Meanwhile, a decay rate adjustment factor is added to control the decay rate in different application scenarios and when nodes perform different cooperative behaviors. Accordingly, the trust decay function shown in Formula (1) is used to express the timeliness of trust.

$$FR(\alpha, t_i) = e^{-\alpha \cdot L(t-t_i)}. \tag{1}$$

Among them, α and $L(t-t_i)$ are two independent variables. α is the rate adjustment factor, and $0 < \alpha \leq 1$, which can be adjusted according to actual application scenarios. $L(t-t_i)$ is a time update function that represents the distance from the current moment t when the ith historical record occurred, and t_i is the moment when the ith interaction of the node was generated.

3.1.1 Same Quality Service Intensity Calculation

In order to better portray node behavior and avoid malicious nodes from participating in cooperation, this paper penalizes nodes that continue to provide malicious services or incentivizes legitimate nodes based on the sustained intensity of the same quality service during the monitoring period [10]. The proportion of the number of successful and failed interaction services generated by the evaluated node to the total number of interaction services in the monitoring cycle is the same quality service persistence intensity of the node, $F_B^c(c = r, p)$. F_B^p is the penalty factor of the evaluated node B, and F_B^r is the reward factor. F_B^c is calculated as Formula (2) [20].

$$F_B^{\mathrm{c}} = \frac{service_B^{type}}{service_B^{su} + service_B^{fa}}. \tag{2}$$

Among them, $type = su, fa$. $service_B^{su}$ and $service_B^{fa}$ are respectively the number of successful and failed interactive services provided by the evaluated node B during the monitoring period.

3.1.2 Direct Trust Calculation

In the Bayesian theory-based trust assessment method, if the state probability density function is known to be$P(\theta)$, then the probability density function is expressed as in Formula (3).

$$P(\theta) = \frac{\Gamma(u+f+2)}{\Gamma(u+1)\Gamma(f+1)}\theta^u(1-\theta)^f. \tag{3}$$

where $\theta \in [0, 1]$ and $\Gamma(\cdot)$ is the gamma function. θ is the probability that the subject node observes that the guest node is a normal node, and the recent successful interactions of the nodes are denoted as u, and the failed interactions are denoted as f. In this paper, a successful interaction means that the guest node successfully forwards the information it receives, and the opposite is considered as a failed interaction.

According to the above formula to predict future events, the probability of the next interaction success can be regarded as the expectation of the beta distribution, as shown in Formula (4).

$$P = E(\beta(u+1, f+1)) = \frac{u+1}{u+f+2} \tag{4}$$

The above formula is the expectation of future behavior. Referring to the definition of trust, it can be used to express the trust evaluation of node A to node B, as shown in Formula (5).

$$T_d = \frac{u_{AB}+1}{u_{AB}+f_{AB}+2} \tag{5}$$

The malicious event impact factor η is introduced in this paper to improve the original Bayesian model and increase

the impact of malicious events. The corrected A-to-B trust assessment value is shown in Formula (6).

$$T_d = \frac{u_{AB}+1}{u_{AB}+\eta f_{AB}+2} \tag{6}$$

Where η is a constant and $\eta > 1$, each vehicle node in the network has a trust information table, which is used to record the direct trust value of the vehicle node that has interacted with it. The calculation method is derived from the above formula.

Remember the success sequence of A and B historical interaction is $u'_{AB}(u'^{t1}_{AB}, u'^{t2}_{AB}, ..., u'^{tn}_{AB})$, and the failed interaction sequence is $f'_{AB}(f'^{t1}_{AB}, f'^{t2}_{AB}, ..., f'^{tn}_{AB})$. Among them, u'_{AB} and f'_{AB} are updated according to the following rules.

If node B provides a successful interactive service, the observation values obtained this time is $(u'^{pr}_{AB}, f'^{pr}_{AB}) = (1, 0)$. After A interacts with B i times, u_{AB} is updated by u'_{AB} as shown in Formula (7).

$$u_{AB}=\sum_{i=1}^{n} FR(\alpha, t_i)\cdot u'^{ti}_{AB} + F^r_B \cdot u'^{pr}_{AB} \tag{7}$$

If node B provides a failed interactive service, the observed values obtained this time is $(u'^{pr}_{AB}, f'^{pr}_{AB}) = (0, 1)$. After A interacts with B i times, f_{AB} is updated with Formula (8).

$$f_{AB} = \sum_{i=1}^{n} FR(\alpha, t_i)\cdot f'^{ti}_{AB} + F^p_B \cdot f'^{pr}_{AB} \tag{8}$$

3.2 Recommended Trust Assessment

3.2.1 Malicious Recommendations Elimation

In order to prevent unreasonable recommendations, this paper introduces the concept of "trust distance" to preclude malicious recommendations in order to effectively resist collusive attacks by malicious vehicle nodes. Assume that there are N recommended nodesk$_1, k_2, ..., k_i, ..., k_N$ within one hop of node A that have direct interaction with B, where the node k$_i$ is the most trusted recommended node of node A, the direct trust value of k$_i$ to B is the trust reference value T_{refer},and d is the trust distance threshold. As the trust distance threshold is too large or too small to effectively identify malicious nodes, it has been verified that the trust distance threshold in this paper is set to 0.2.The trust distance of recommended node and to node B can be calculated by Equation (9).

$$Dis(k_j, k_i) = |T_{d(k_j,B)}| - T_{d(k_i,B)} \tag{9}$$

Among them, $T_{d(k_j,B)}$ and $T_{d(k_i,B)}$ are the direct trust values of and to B respectively.The specific pseudocode to exclude malicious recommendations node is shown in Algorithm 1.

Taking the trust given by A's most trusted recommended node k$_i$ as a reference, if the distance between other nodes k$_j$ and its trust is less than the threshold d , it means that node k$_j$ can be used as a recommended node for A. Otherwise, it is considered as a malicious node and k$_j$ is deleted in the recommended node.

In Algorithm 2, find the most trusted recommended node k$_i$ of node A , and z is the total length of the direct trust table of node A.

Algorithm 1 Malicious recommendation node elimination

```
Begin
Find node k_i among the recommended of node A
T_refer ← T_d(k_i,B)
Dis_(k_j,k_i) ← |T_d(k_j,B) − T_refer|(j = 1, 2, ..., N&j ≠ i)
if Dis_(k_j,k_i) < d then
    keep k_j
else
    delete k_j
end if
End
```

Algorithm 2 search k$_i$

```
Begin
Input Trust table of node A
T_d(A,k_i) ← T_d(A,k_1)
For j=2 to z
if T_d(A,k_j) > T_d(A,k_i) then
    T_d(A,k_i) ← T_d(A,k_j)
end if
End For
Return k_i
End
```

3.2.2 Recommended Trust Calculation

After the malicious recommendation node exclusion algorithm excludes some of the malicious recommendations, the remaining n recommendation nodes can be represented as $K_i(i = 1, 2, ..., n)$. If there is no direct interaction experience between A and B, when calculating the trust value of A to B, the trust value of the recommended node to B is required. In the traditional trust model, the trust value of the node is used as the weight, as shown in Formula (10).

$$T_r(A, B) = \sum\nolimits_{i=1}^{n} T_d(A, K_i)T_d(K_i, B) \tag{10}$$

Where $T_d(A, K_i)$ is the direct trust value of A to K_i , and $T_d(K_i, B)$ is the direct trust value of K_i to B. This means that the higher the trust value of node A to K_i , the more important its recommendations are. However, this algorithm ignores the possibility of collusion attacks, so that malicious nodes can gain a higher trust value through camouflage and spread malicious resources to normal nodes. Therefore, it is inappropriate to use the trust value of A versus K_i as the weight. Therefore,

this paper uses similarity as the weight to calculate the recommended trust value of A versus B.

When calculating the trust value of A to B , A has no direct interaction experience with B , and the trust value of B needs to be calculated indirectly through the trust value of recommender K_i to B . The recommender K_i in this paper is obtained from the communication list of vehicle B stored in RSU.

The score similarity characterizes the similarity of the scores of node A and node K_i.This paper uses cosine-based similarity to measure the similarity between two vectors [17], let nodes A and K_i rate the same set of items, and then the cosine similarity is calculated according to Formula (11).

$$Sim(A,K_i)=\frac{|\sum_{j=1}^{m} r_{aj}r_{sj}|}{\sqrt{\sum_{j=1}^{m}(r_{aj})^2}\sqrt{\sum_{j=1}^{m}(r_{sj})^2}} \tag{11}$$

The score vectors of the successful transaction rate of m vehicles by node A and node K_i within a period of t are represented as $r_a = [r_{a1}, r_{a2}, ..., r_{am}]$ and $r_s = [r_{s1}, r_{s2}, ..., r_{sm}]$ respectively. Among them,$Sim \in [0,1]$. The larger the value of Sim , the higher the score similarity between the two nodes, which means that the scores of A and K_i on other nodes of the network are more consistent. r_{aj} is the successful transaction rate score of vehicle node A for the jth vehicle. It represents the ratio of the number of successful interactions between node A and j in the interaction history to the total number of interactions with node j.

The n advisers K_i feedback their trust value $T_d(K_i,B)$ to B, A uses the similarity $Sim(A,K_i) \in [-1,1]$ between himself and K_i as the weight to calculate the trustworthiness of A's recommendation on B, as in Formula (12).

$$T_r(A,B)=\sum_{i=1}^{n} Sim(A,K_i)T_d(K_i,B) \tag{12}$$

3.3 RSU Trust Assessment

The selection of RSU transfer trust attributes should be able to fully reflect the activity characteristics of vehicle nodes in the network, and accurately describe the real-time behavior of the vehicle. For example, the vehicle's moving speed, signal power, and the vehicle's participation in network communications. This may be a traffic violation when the vehicle is moving faster than the normal range compared to the surrounding vehicles. The low signal power of vehicles participating in normal communication, or deliberately discarding some messages or not participating in the network communication of message forwarding, may lead to the decline of vehicle trust level. The vehicle-related attributes are expressed as in Formula (13).

$$csa=[csa^1, csa^2, ..., csa^x] \tag{13}$$

Where x is the number of relevant attributes of the vehicle. Considering that different trust attributes play different roles in the process of node trustworthiness calculation, different trust weight is defined for each trust attribute, and the weight is defined as in Formula (14).

$$\omega_{csa}=[\omega_{csa}^1, \omega_{csa}^2, ..., \omega_{csa}^{\mathrm{x}}] \tag{14}$$

And $\sum_1^{\mathrm{x}} \omega_{csa} = 1$, then the observed trust value of the evaluated vehicle B is as in Formula (15).

$$OT_B=\sum\nolimits_1^{\mathrm{x}} csa\omega_{csa} \tag{15}$$

RSU can obtain the integrated trust value of the vehicle by fusing the trust value report of all other vehicles on the vehicle, as shown in Formula (16).

$$FT_B=[\prod_{i=1}^{s} T_d(A,B)^{\frac{1}{s}}] \tag{16}$$

Where s represents the number of vehicles that have estimated the trust value of vehicle B and $T_d(A,B)$ represents the direct trust value of vehicle A to vehicle B.

3.3.1 RSU Global Trust Calculation

The RSU global trust is obtained through observation trust and fusion trust, as shown in Formula (17).

$$T_{RSU}=\frac{\mathrm{x}}{s+\mathrm{x}}OT_B+\frac{s}{s+\mathrm{x}}FT_B \tag{17}$$

The weight of observation trust and fusion trust is adaptively obtained from the number of relevant attributes and the number of evaluated vehicles.

3.4 Comprehensive Trust Calculation Based on Analytic Hierarchy Process

The hierarchical analysis method decomposes the goal-related influencing factors and uses the decision maker's experience to compare multiple factors in two to arrive at the relative importance; it combines qualitative analysis with quantitative analysis to quantify the level of importance among multiple factors. Hierarchical analysis can be used in the program to determine the specific weights of each factor in trust assessment in a more reasonable and scientific way [23].

3.4.1 Weight Calculation Method

1) Build a hierarchical model

   Divide the decision-making goals, consideration factors (decision criteria), and decision objects into the highest level, middle level, and the lowest level according to their mutual relationship, and the multi-factor hierarchical structure model shown in Figure 3 can be obtained.

2) Constructing the judgment matrix

   Comprehensive trust is affected by four factors: initial trust, direct trust, recommendation trust, and

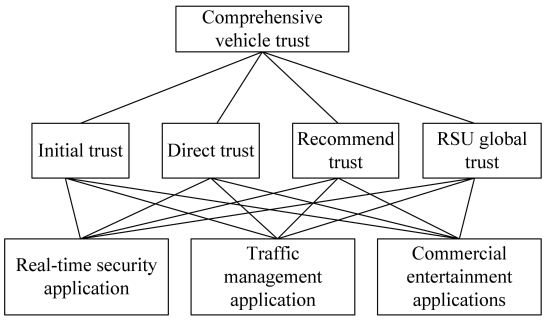


Figure 3: Multi-factor hierarchical structure model

RSU trust. The importance of various scenes relative to the four factors is different, so according to the different actual scenes, the consistent matrix method can be used to compare the importance of these factors relative to the upper layer. Construct multiple judgment matrices using the proportional scaling method as shown in Table 1, as shown in Figure 4.

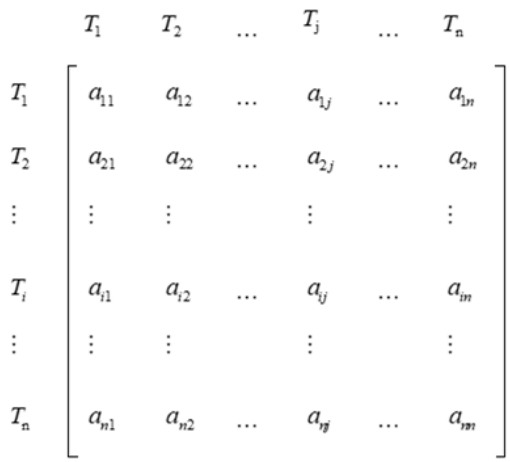


Figure 4: Judgment matrix

3) Judgment matrix solution and consistency check

Use the sum-product method to solve the matrix. The calculation is as follows: divide each item in the matrix by the sum of each item in the column of the item, standardize the matrix, use formula $b_{ij} = a_{ij}/\sum_{j=1}^{n} a_{ij}$; take the average of each row of the new matrix, Get the weight $w_i = \sum_{j=1}^{m} b_{ij}/m$ of each factor. When constructing the judgment matrix, there may be logical errors. For example, A is more important than B, B is more important than C, but C is more important than A. Therefore, it is necessary to use the consistency test to check whether there is a problem. Because we calculate the importance of the scene in the upper layer of trust factors, we adopt the hierarchical single ordering and the consistency test. The calculation steps are as follows: Calculate the maximum eigenvalue $\lambda_{\max} = \sum_{i=1}^{n} A_i/(nw_i)$ of each matrix A; Calculate the consistency index $CI = \frac{\lambda_{\max}-n}{n-1}$; the closer the CI is to 0, the more satisfactory the consistency, and the larger the CI, the more serious the inconsistency. The random consistency index RI is obtained by checking Table 2 from the order n of the matrix. Calculate the consistency ratio: $CR = \frac{CI}{RI}$. Generally, when the consistency ratio $CR < 0.1$, the degree of inconsistency of the matrix is considered to be within the allowable range. If the consistency is satisfactory, the consistency test is passed, and the corresponding weight vector obtained at this time is available. The element a_{ij} of the judgment matrix is given by Santy's 1-9 scale method, as shown in Table 1.

Calculation by the analytic hierarchy process, the weights of initial trust, direct trust, recommendation trust, and RSU trust in different scenarios can be determined, and the weights are set as w_1, w_2, w_3, and w_4 respectively.

Table 1: Random consensus indexesl

n	RI
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24

3.4.2 Comprehensive Trust Calculation Method

After a certain cycle, the comprehensive trust of the vehicle is calculated as in Formula (18).

$$T_{total} = w_1 IT + w_2 T_d + w_3 T_r + w_4 T_{RSU} \tag{18}$$

After the trust calculation, it is assumed that the message receiver decides to receive the message sender's information. After the message is received, it needs to give feedback on whether the information is true or not. If the number of inauthentic messages over some time is greater than or equal to half of the number of communications, the vehicle is considered to be a malicious vehicle. To reduce the storage burden of the vehicle, the vehicle will periodically clean up the vehicle trust values that have been in place for too long [3, 9].

4 Experiment and Result Analysis

4.1 Experimental Environment

The simulation environment configuration is as follows:

Table 2: "1-9" proportional scaling method

Scaling	Meaning
1	Indicates that two factors have the same importance compared to each other
3	Indicates that one factor is slightly more important than the other when compared to the two factors
5	Indicates that one factor is significantly more important than the other when compared to the two factors
7	Indicates that one factor is strongly more important than the other when compared to the two factors
9	Indicates that one factor is more extremely important than the other when compared to the two factors
2,4,6,8	The median of the above two adjacent judgments
Reciprocal	The comparison of factor i and j is judged as a_{ij} , and the judgment of factor j and i is judged as $a_{ji} = 1/a_{ij}$

Software: By using veins [18] as the V2V open-source framework and OMNET++ (as a network simulator) and SUMO (as a traffic simulator). Use SUMO to generate vehicle motion status files, and OMNET++ queries and dispatches vehicle motion status through TraCI.Hardware: Intel(R) Core i7-10510U CPU @1.80 GHZ processor, 16GB RAM. NVIDIA GeForce MX250 graphics display. Microsoft Windows 10 Professional operating system.

There are three main types of malicious vehicle node behavior introduced in the network: selfish nodes that do not send information, nodes that send false information and nodes that deliberately drop packets.Netedit is used to generate road network files,the experimental simulation parameter settings in this paper are shown in Table 3.

Table 3: Simulation parameters

Parameter Parameter	The values used in the simulation
Road length	1000m
Number of lanes	6
Required speed	40m/s
Frequency	V2V 5.9GHz
Packet size	200 bytes
Transmission rate	6Mbps
MAC protocol	IEEE802.11p
Network protocol	IEEE1609.4

4.2 Result Analysis

With the increase of malicious nodes, this paper compares the direct trust value of using Bayesian without considering the malicious factor [7] with the direct trust value of considering the malicious factor in this paper. The experimental results are shown in Figure 5.

Figure 5 shows that when the proportion of malicious nodes keeps increasing, the direct trust degree value with

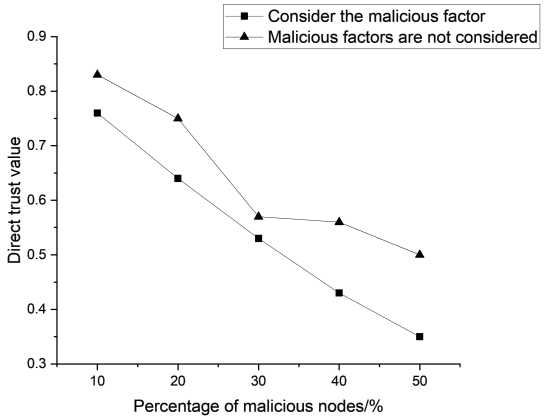


Figure 5: Comparison of whether to consider malicious factors

malicious factor considered decreases at the fastest rate. It can be seen that the calculation of the direct trust degree value of malicious factor being considered in this paper can better portray the node behavior and quickly identify malicious nodes.

To verify whether the direct trust value in this paper can better reflect the behavior of nodes and effectively identify malicious nodes, the direct trust calculation method in this paper is compared with the traditional Bayesian method in different time periods. To simulate the changes of direct trust degree values in different time periods, the direct trust degree values of nodes are calculated by setting the time period t from 0 to 20 minutes when the target nodes provide normal services. At t from 20 to 40 minutes,10% of malicious nodes are configured to randomly generate discarded packets to calculate the direct trust degree value of the nodes, and the experimental results are shown in Figure 6.

Figure 6 shows that with the accumulation of time after adding malicious nodes, the direct trust value of this paper decreases at the fastest rate and is lower than the

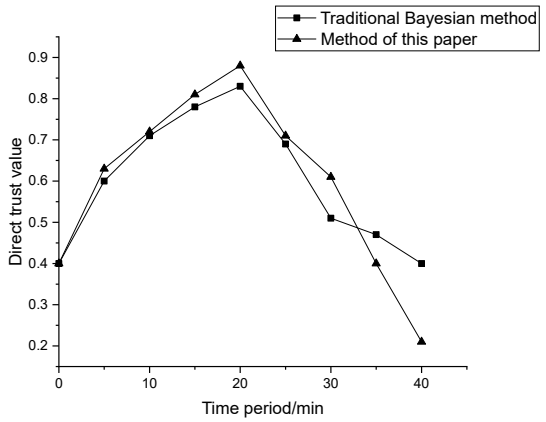


Figure 6: Changes in the value of direct trust

direct trust value obtained by traditional Bayes after 33 minutes. This shows that the direct trust degree calculation in this paper can better characterize the node behavior and identify malicious nodes quickly.

To evaluate the effectiveness of adding the malicious referral node exclusion algorithm to the recommendation trust calculation, this paper compares the packet loss rate of the network before and after adding the malicious referral node exclusion algorithm. The packet loss rate is the ratio of the total number of packets lost by the receiving node to the total number of packets sent by the sending node. The packet loss rate is compared between two groups of experiments, one without the malicious recommendation node exclusion algorithm and the other with the malicious recommendation node exclusion algorithm, where the excluded nodes are no longer added to the network. The simulation time is set to 5min, 10min, 15min, 20min, 25min and 30min. The experimental results are shown in Figure 7.

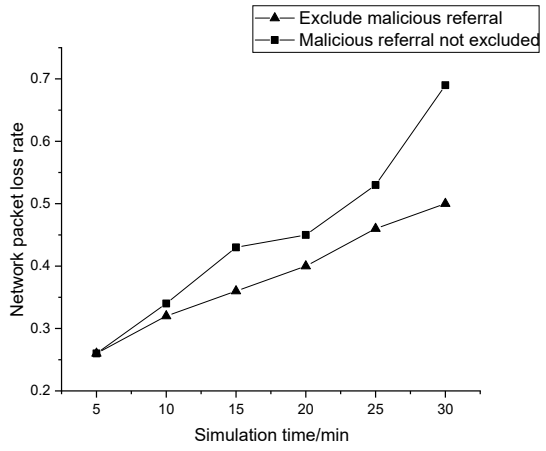


Figure 7: Comparison of network packet loss rate

As can be seen in Fig. 7, the network packet loss rate in different periods after adding the malicious recommendation node exclusion algorithm is significantly lower than the network packet loss rate without adding the malicious recommendation node exclusion algorithm. It shows that the malicious recommendation exclusion algorithm is added to exclude some of the malicious recommendation nodes, which makes the network packet loss rate decrease compared with that before the malicious recommendation exclusion algorithm is added, and also proves the effectiveness of the malicious recommendation exclusion algorithm.

By setting up different proportions of malicious nodes in the simulated environment, the accuracy rate of the recommended trust is calculated in this paper and the EigenTrust method. The accuracy rate of recommended trust = detection of real malicious nodes / detection of untrusted nodes. The experimental results are shown in Figure 8.

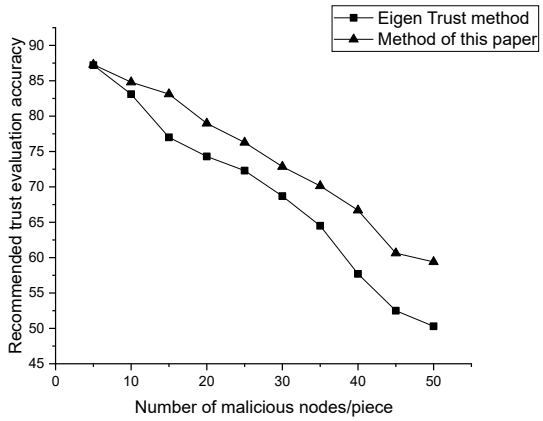


Figure 8: Comparison of recommended trust evaluation accuracy

Figure 8 shows that when the density of malicious nodes continues to increase, it can be seen that the accuracy of the recommendation trust evaluation in this paper is always higher than that of the EigenTrust method.

To test the overall performance of the trust evaluation in this paper, the experiment compared the trust evaluation mechanism of this paper with the EigenTrust method and the success rate of vehicle interaction under different malicious node ratios in the References [1]. Let the ratios of malicious nodes be 5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%. The experimental results are shown in Figure 9.

Figure 9 shows that when the proportion of malicious nodes is 15%-60%, the vehicle interaction success rate of the trust mechanism in this paper is higher than that of the other two models. It can be seen that the trust mechanism in this paper has certain advantages in the success rate of interaction.

5 Conclusion

The presence of malicious nodes in IoV can seriously affect network communication and may even cause incalculable

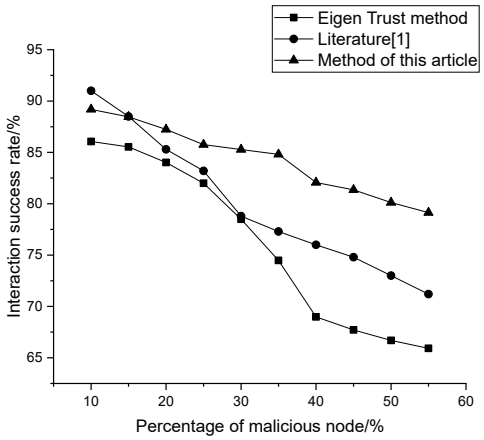


Figure 9: Comparison of recommended trust evaluation accuracy

consequences if a large number of malicious nodes invade and send shared false information once they exist. The trust assessment mechanism proposed in this paper integrates four trust factors from initial trust, direct trust, recommended trust, and RSU global trust regarding the trust assessment of vehicle nodes. The analytic hierarchy process is used to quantify the degree of influence of each factor and different application scenarios on vehicle trust. This trust assessment mechanism can detect and exclude some malicious referrals and also provides a basis for vehicle information reception and decision making, thus ensuring a trustworthy environment for vehicular communication. To solve the cold start problem, an initial trust module is added; to accelerate the rapid convergence of trust values of vehicle nodes, a malicious event impact factor is introduced to improve Bayes; to reduce malicious recommendation behavior, trust distance is used to exclude malicious recommendations from some malicious nodes; to effectively prevent the possibility of collusion attacks, cosine similarity is adopted as the weight of recommendation trust. In addition, to give full play to the role of RSU in trust evaluation, the influence of observed trust and fused trust on vehicle nodes in RSU is considered comprehensively. The research in this paper focuses on the evaluation of interaction information, and the next step will be to consider more influencing factors on node behavior, including node processing capabilities and specific application scenarios. In this paper the possibility of collusion attacks is considered, in the future, more complex and more possible attacks are considered in our plan to explore the resilience of the proposed mechanism.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No.61862040, No.61762059 and No.6176 2060.The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in iot-enabled vehicular networks," in *IEEE Wireless Days*, pp. 1–8. IEEE, 2019.

[2] S. Z. Chen, J. L. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of c-v2x: technologies, field testing, and challenges with chinese development," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3872–3881, 2020.

[3] T. Cheng, G. C. Liu, Q. Yang, and J. G. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 652–663, 2019.

[4] S. S. Desai and M. J. Nene, "Node-level trust evaluation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2139–2152, 2019.

[5] S. Deshpande and R. Ingle, "Evidence based trust estimation model for cloud computing services," *Internation Journal of Network Security*, vol. 20, no. 2, pp. 291–303, 2018.

[6] H. El-Sayed, S. Zeadally, M. Khan, and H. Alexander, "Edge-centric trust management in vehicular networks," *Microprocessors and Microsystems*, vol. 84, p. 104271, 2021.

[7] H. El-Sayed, S. Zeadally, and D. Puthal, "Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks," *Vehicular Communications*, vol. 24, p. 100227, 2020.

[8] Z. El-Yebdri, S. M. Benslimane, F. Lahfa, M. Barhamgi, and D. Benslimane, "Context-aware recommender system using trust network," *Computing*, no. 1, pp. 1–19, 2021.

[9] T. L. Gao, T. Li, R. Jiang, M. Yang, and R. Zhu, "Research on cloud service security measurement based on information entropy," *Internation Journal of Network Security*, vol. 21, no. 6, pp. 1003–1013, 2019.

[10] G. A. Ghazvini, M. Mohsenzadeh, R. Nasiri, and A. M. Rahmani, "A new multi-level trust management framework (mltm) for solving the invalidity and sparse problems of user feedback ratings in cloud environments," *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2326–2354, 2021.

[11] Z. G. He, "Multi-parameter and time series based trust for iot smart sensors," *Internation Journal of Network Security*, vol. 22, no. 4, pp. 589–596, 2020.

[12] V. S. Janani and M. S. K. Manikandan, "An outlook on cryptographic and trust methodologies for clusters based security in mobile ad hoc networks," *Internation Journal of Network Security*, vol. 20, no. 4, pp. 746–753, 2018.

[13] M. H. Junejo, A. H. A. Rahman, R. A. Shaikh, K. M. Yusof, I. Memon, H. Fazal, and D. Kumar, "A privacy-preserving attack-resistant trust model for

internet of vehicles ad hoc networks," *Scientific Programming*, vol. 2020, no. 2, pp. 1–21, 2020.

[14] T. Li, A. F. Liu, N. N. Xiong, S. B. Zhang, and T. Wang, "A trustworthiness-based vehicular recruitment scheme for information collections in distributed networked systems," *Information Sciences*, vol. 545, no. 12, pp. 65–81, 2021.

[15] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in vanets," *Journal of Parallel and Distributed Computing*, vol. 151, no. 2, pp. 61–69, 2021.

[16] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K. Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2020.

[17] S. O. Ogundoyin and I. A. Kamil, "A fuzzy-ahp based prioritization of trust criteria in fog computing services," *Applied Soft Computing*, vol. 97, p. 106789, 2020.

[18] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata. *Veins: The open source vehicular network simulation framework*, Recent Advances in Network Simulation, pp. 215–252. Springer, 2019.

[19] B. Su, C. H. Du, and J. Huan, "Trusted opportunistic routing based on node trust model," *IEEE Access*, vol. 8, no. 99, pp. 163077–163090, 2020.

[20] S. R. Tong, B. Z. Sun, X. L. Chu, X. R. Zhang, T. Wang, and C. Jiang, "Trust recommendation mechanism-based consensus model for pawlak conflict analysis decision making," *International Journal of Approximate Reasoning*, vol. 135, pp. 91–109, 2021.

[21] T. Wang, H. Luo, X. X. Zeng, Z. Y. Yu, A. F. Liu, and A. K. Sangaiah, "Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1797–1806, 2020.

[22] Y. B. Wang, J. H. Wen, X. B. Wang, B. M. Tao, and W. Zhou, "A cloud service trust evaluation model based on combining weights and gray correlation analysis," *Security and Communication Networks*, vol. 2019, no. 1, pp. 1–11, 2019.

[23] L. B. Wen, "Security evaluation of computer network based on hierarchy," *Internation Journal of Network Security*, vol. 21, no. 5, pp. 735–740, 2019.

[24] P. S. Xie, X. Q. Wang, X. J. Pan, Y. F. Wang, T. Feng, and Y. Yan, "Blockchain-based trust evaluation mechanism for internet of vehicles nodes," *Internation Journal of Network Security*, vol. 23, no. 6, pp. 1065–1073, 2021.

[25] H. Z. Zhao, Q. G. Chen, W. Shi, T. L. Gu, and W. Y. Li, "Stability analysis of an improved car-following model accounting for the driver's characteristics and automation," *Physica A: Statistical Mechanics and Its Applications*, vol. 526, p. 120990, 2019.

[26] H. Z. Zhao, D. H. Sun, H. Yue, M. Zhao, and S. Cheng, "Dynamic trust model for vehicular cyber-physical systems," *Internation Journal of Network Security*, vol. 20, no. 1, pp. 157–167, 2018.

[27] H. Z. Zhao, D. X. Xia, S. H. Yang, and G. H. Peng, "The delayed-time effect of traffic flux on traffic stability for two-lane freeway," *Physica A: Statistical Mechanics and its Applications*, vol. 540, p. 123066, 2020.

[28] H. Z. Zhao, H. Yue, T. L. GU, C. H. Li, and D. Zhou, "Low delay and seamless connectivity-based message propagation mechanism for vanet of vcps," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3385–3402, 2021.

[29] H. Z. Zhao, H. Yue, T. L. Gu, and W. Y. Li, "Cps-based reliability enhancement mechanism for vehicular emergency warning system," *International Journal of Intelligent Transportation Systems Research*, vol. 17, no. 3, pp. 232–241, 2019.

[30] J. H. Zhu, "Wireless sensor network technology based on security trust evaluation model," *International Journal of Online Engineering*, vol. 14, no. 4, pp. 211–226, 2018.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things. E-mail: xiepsh_lut@163.com

Xin Tong was born in Aug. 1995. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2505156603@qq.com.

Hong Wang was born in Oct. 1995. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2967589625@qq.com

Ying-Wen Zhao was born in Feb. 1996. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1075224210@qq.com

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, information security . E-mail: fengt@lut.cn

Yan Yan was born in Oct. 1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology. Her major research field is privacy protection, multimedia information security. E-mail: yanyan@lut.cn

An Assessment Method of Internet of Vehicles User Behavior Based on Hidden Markov Model

Peng-Shou Xie, Yi-Fan Wang, Zong-Liang Wang, Nan-Nan Li, Tao Feng, and Yan Yan
(Corresponding author: Yi-Fan Wang)

School of Computer and Communications, Lanzhou University of Technology
No. 36 Peng-jia-ping Road, Lanzhou, Gansu 730050, China
Email: 844782234@qq.com

(Received July 21, 2021; Revised and Accepted Apr. 13, 2022; First Online Apr. 23, 2022)

Abstract

In order to solve the problem that some attackers steal, tamper or destroy the stored sensitive data after passing the identity authentication on the Internet of Vehicles service cloud platform, an assessment method of Internet of Vehicles user behavior based on the Hidden Markov Model is proposed in this paper. Firstly, the critical behavior features of Internet of Vehicles users with higher weight values are extracted using Term Frequency-Inverse Document Frequency. Then, according to the behavior features, the Internet of Vehicles user behavior model is established using the Hidden Markov Model. Finally, the weight difference of the user's behavior sequence before and after is calculated by improving the Forward algorithm of the Hidden Markov Model to assess whether the user's current behavior is legal or not. The experimental results show that the method improves the comprehensive assessment index F1-Score on Internet of Vehicles user behavior assessment results.

Keywords: Behavior Assessment; Data Security; Hidden Markov Model; Internet of Vehicles Service Cloud Platform; Term Frequency-Inverse Document Frequency

1 Introduction

As an important communication server, the Internet of Vehicles service cloud platform has been widely used in the scene of the Internet of Vehicles. According to the risk analysis, it constructs a multi-dimensional integrated protection system for site security, host security, data security and business security, and so on [20]. In recent years, the state has promulgated the strategy of traffic power Internet of Vehicles (IoV) is taken as the key application scenario of 5G communication infrastructure construction. At the same time, many enterprises and individual car owners have begun to store data related to vehicle nodes in the service cloud platform. When IoV users use the service cloud platform in the process of stealing by others or unintentionally illegal operations leading to the leakage of the user's information is a very common security problem [5]. At the same time, it also increases the risk of data storage in the IoV service cloud platform [6]. Attackers forge and impersonate the identity of legitimate IoV users, illegally access the service cloud platform, tamper, steal or damage the stored sensitive data which poses a great threat to the property and information security of the IoV users.

User behavior analysis provides a new solution for the research of an access control model in an open network environment. People's daily behavior pattern is regular and it is the same when visiting the IoV service cloud platform [3]. Therefore, through the statistical analysis of the daily behavior data of users, the habitual behavior patterns of users can be obtained, to distinguish abnormal behaviors and judge whether the user is legitimate. Researchers at home and abroad use a variety of techniques to assess user behavior more accurately [10].For example, building analytical models [16], data mining [11], machine learning [19], artificial intelligence [15] and log auditing [7]. Although these methods improve the accuracy of behavior assessment, they often ignore the relevance and individual differences between the operation behaviors, failing to fully describe the user's operation behavior, which cannot meet the accuracy requirements of the access control of the IoV service cloud platform.

In order to better solve the above problems, this paper studies the behavior pattern of the IoV users in transaction processing on the service cloud platform and finds the differences between the behavior sequences in the behavior pattern. An assessment method of the IoV user behavior based on the Hidden Markov Model (HMM) is proposed. After the key features of command samples are effectively extracted by using Term Frequency-Inverse Document Frequency (TF-IDF), the user behavior model of IoV is established based on HMM, and an improved Forward algorithm to calculate the weight difference of the before and after behavior sequence. Finally, the effectiveness of the proposed assessment method is verified based on simulation experiments, which adds a security

guarantee of behavior authentication for access control of the IoV service cloud platform.

2 An Assessment Method of IoV User Behavior Based on HMM

By analyzing the behavior of IoV users, we can gain insight into the information hidden behind each transaction processing behavior and discover the corresponding network security problems, thus enhancing the network situational awareness and enhancing the defense ability of network security [17]. This method not only optimizes the access control system but also gives a timely warning of identity theft attacks, preventing attackers from modifying permissions, tampering with information stealing data in the network by stealing the legitimate certificates of IoV users, thus improving the security of the IoV service cloud platform.

When the user is a newly registered user or an old user has some new behaviors, the historical behavior data do not exist in the service cloud platform, so it cannot be judged only based on the historical behavior of a single user. In order to comprehensively assess the user behavior of the IoV, this paper studies the various behaviors of IoV user groups on the transaction processing of the service cloud platform, so as to assess the user's abnormal behavior, and dynamically adjust the access strategy [1].

1) First of all, collect and sort out the behavior information of the IoV user group in the transaction processing of the service cloud platform. The IoV user group is divided into known users and unknown users to learn the normal and abnormal behavior data of several known users, so as to assess the behavior of unknown users more accurately;

2) Secondly, TF-IDF [24] is used to extract the behavior features of known users, remove the redundant information in the original data set, and finally get the key behavior features with higher weight value;

3) Then, the IoV user behavior model is established based on HMM. The elements of HMM are redefined to make it more suitable for the IoV service cloud platform. According to the Baum-Welch algorithm [21], the model is trained and optimized;

4) Finally, the Forward algorithm of HMM is improved to calculate the difference of the weight value ΔW of the behavior sequence before and after the IoV users, so as to more accurately assess whether the IoV users' behavior is legal at a certain time. In case of abnormal behavior, adjust the access right immediately and conduct secondary identity authentication; If it is normal behavior, accept and continue to assess the follow-up behavior until it exits the IoV service cloud platform.

The flow chart of the IoV user behavior assessment method based on HMM is shown in Figure 1.

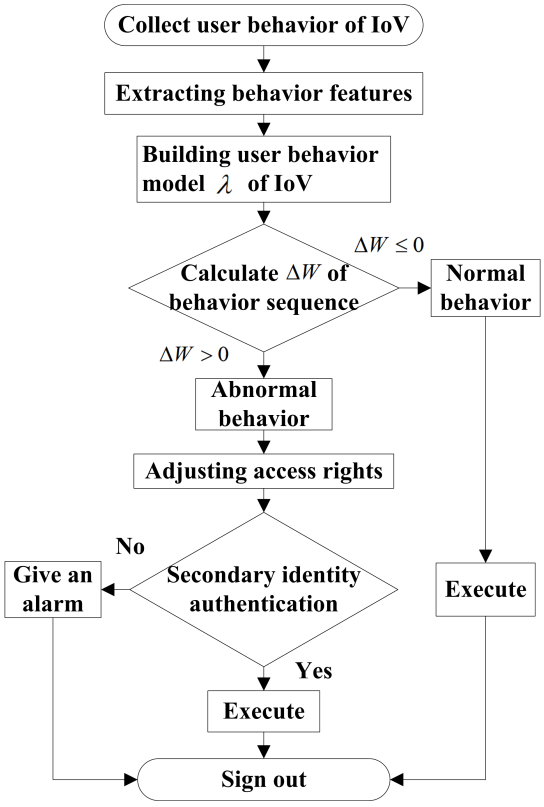


Figure 1: Flow chart of the IoV user behavior assessment

2.1 IoV User Behavior Feature Extraction

The operational command like send mail is a very common behavior in the user operation behavior, so the frequency of this command is higher. But after data desensitization, the command will not contain any important information and become an operation command with no difference. These operational commands would not be significant if they were the primary features of the IoV user behavior assessment. So this paper should look for those behaviors which are more frequent in a single user's operation but less frequent in all users.

In order to better solve the above problems. The TF-IDF method is used to extract features from the data set, select more meaningful behavior features and accurately assess the IoV user behavior. TF-IDF is a method of text data vectorization that is used in text analysis, Chinese and English keywords extraction, information retrieval, document classification, and so on.

Let $t_i(i = 0, 1, \cdots, n-1)$ be an operation command of an IoV user, and $d_j(j = 0, 1, \cdots, n-1)$ be a behavior data set of an IoV user including t_i.

Step 1. Calculate TF. That is, the probability of an operational command of the IoV user appearing in his behavior data set. Where $n_{i,j}$ is the number of times t_i appears in d_j, and $\sum_k n_{k,j}$ is the total number of operational commands contained in behavior data set

d_j. The calculation is shown in Equation (1):

$$tf_{i,j} = \frac{n_{i,j}}{\sum_k n_{k,j}} \quad (1)$$

Step 2. Calculate IDF. That is the probability that an operational command of the IoV user appears in all IoV user behavior data sets. Where $|D|$ is the total number of IoV users. $|\{j : t_i \in d_j\}|$ is the total number of IoV users including.If the operation command is not in any behavior data sets of IoV users, the denominator will be zero, so the denominator uses $|\{j : t_i \in d_j\}|+1$. The calculation is shown in Equation (2):

$$idf_i = lg\frac{|D|}{|\{j : t_i \in d_j\}|+1} \quad (2)$$

Step 3. Calculate TF-IDF. That is the weight value W_{a1} of an operational command of the IoV users. The calculation is shown in Equation (3):

$$W_{a1} = tf_{i,j} \times idf_i \quad (3)$$

If the weight value calculated by the TF-IDF is higher, it indicates that is more important in all IoV user behaviors. Taking this behavior as a key behavior feature is very helpful for a behavior assessment.

2.2 User Behavior Model of IoV is Established Based on HMM

In this paper, the observation variables, state variables, state transition probability matrix, observation variable probability matrix, and initial state probability vector of HMM are redefined. The user behavior model of IoV is established by using HMM, which is represented by $\lambda = (X, Y, A, B, \pi)$, the following will describe five parameters.

1) Observation variable X of the IoV user behavior model
The observation variables in this paper represent the behavior sequence when users process transactions on the IoV service cloud platform. Behavior sequence can be directly observed and contains key behavior features. Set X as $\{x_1, x_2, \cdots, x_m\}$,Where $x_i \in X$ represents the operation behavior sequence of the IoV users at i time. The number of different behavior features in each state is denoted by m. The observation set is O_i, that is $O_i \in X = \{x_1, x_2, \cdots, x_m\}$.

2) State variable Y of the IoV user behavior model
Set the state variable Y of the IoV user behavior model to $\{y_1, y_2, \cdots, y_n\}$, the state at i time is q_i, that is $q_i \in Y = \{y_1, y_2, \cdots, y_n\}$. The number of states in the model is denoted by n. Generally, Y cannot be observed. According to the behavior features of the IoV users, the state of sensitive data stored in the IoV service cloud platform is taken as the state variable of the model in this paper. According to real-life, the state of sensitive data is divided into two kinds: dangerous and safe.

3) State transition probability matrix A of the IoV user behavior model
A is used to represent the state transition probability matrix of the IoV user behavior model, denoted as $A = (a_{ij})_{n\times n}$. A is the probability distribution of mutual transfer between sensitive data states stored in the service cloud platform. $a_{ij} = P(q_{t+1} = y_j|q_t = y_i), 1 \le i \le n, 1 \le j \le n$, a_{ij} means the state of sensitive data stored by the IoV users at t time is q_t. The probability of its transition to the state of $t+1$ time is $q_t + 1$.

4) Observation variable probability matrix B of the IoV user behavior model
B is used to represent the probability matrix of the observed variables of the IoV user behavior model, denoted as $B = (b_{jk})_{n\times m}$. Each state variable corresponds to an observation variable and its relative probability distribution is calculated as $b_{jk} = P(O_t = x_k|q_t = y_j), 1 \le j \le n, 1 \le k \le m$. b_{jk} is the probability of generating the sequence of operation behavior x_k at t time sensitive data is in the state q_t.

5) nitial state probability vectorof the IoV user behavior model
π is used to represent the initial state probability vector of the IoV user behavior model, denoted as $\pi = (\pi_i)_{1*n} = \{\pi_1, \pi_2, \cdots, \pi_n\}$. π is the initial probability distribution matrix of order $1 \times N$. $\pi_i = P(q_1 = y_i), 1 \le i \le n$ is the probability that the stored sensitive data is in the state q_i when $t = 1$.

In order to establish the model more quickly and conveniently, based on the initial values of n, m, A, B and, combined with the Baum-Welch algorithm of HMM, the parameters of the IoV user behavior model is determined and the model is optimized.

Baum-Welch algorithm [22] starts from the initial estimation of parameters, and achieves the local optimal value through parameter learning training, and considers that the probability distribution of the initial state is uniform. Therefore, this method assumes that the user behavior model of the Internet of vehicles has T states and K observation symbols. Then the probability of taking any states as the initial state is $1/T$. The transition probability of each step between each state in the model is also $1/T$. In each of these states, the probability of behavior feature is $1/K$.

2.3 The Weight Calculation of User Behavior Sequence of IoV

There are three basic algorithms for HMM: Forward algorithm for model assessment, Viterbi algorithm for decoding, Baum-Welch algorithm for parameter learning. The

Forward algorithm can effectively calculate the probability $P(X|\lambda)$ of an observed variable X in the model λ.

In order to better reflect the relevance of user transaction processing behavior. In this paper, the weight of the behavior sequence of the IoV users is calculated by improving the Forward algorithm, and the difference between the weight values of the front and rear behavior sequences is calculated in order to assess whether the current behavior of the IoV users is legal. The weight of the behavior sequence refers to the number of times that the sequence of behaviors appears in all operating commands. If a large number of IoV users often perform the same transaction operation, the weight of the behavior sequence will be increased.

At t, λ outputs the observation variable $X_1 = x_1, x_2, \cdots, x_R$ with the length of R. This variable is the operational command of the IoV users from time 0 to time t, forming an initial observation variable. The weight valueof W_1 is X_1 calculated as shown in Equation (4):

$$W_1 = P(X_1|\lambda) = P(x_1, x_2, \cdots, x_R|\lambda) \tag{4}$$

At $t+1$, λ outputs the behavior x_{R+1}, discards x_1 in X_1 and obtains a new observation variable $X_2 = x_2, x_3, \cdots, x_R, x_{R+1}$ with R length. The weight value W_2 of X_2 is calculated as shown in Equation (5):

$$W_2 = P(X_2|\lambda) = P(x_2, x_3, \cdots, x_R, x_{R+1}|\lambda) \tag{5}$$

Calculate the difference ΔW between the weight values of the two observation variables, as shown in Equation (6):

$$\Delta W = W_1 - W_2 \tag{6}$$

If $\Delta W > 0$, indicates that the weight value of X_2 is smaller than that of X_1. Therefore, the probability of newly observed variability being accepted by the model is low, X_{R+1} may be an abnormal behavior. Discard X_{R+1}. Immediately adjust the user's access rights and conduct secondary identity authentication. If it is the user himself, accept and continue to assess the follow-up behavior; If it is an attacker, it will immediately report to the police and exit the IoV service cloud platform; But if $\Delta W \leq 0$,it shows that for the trained model, the weight of new observation variables is increasing. X_{R+1} is normal behavior. X_{R+1} is added to the observation variable as a new sequence which is used as the basic sequence to determine the validity of the next behavior.

As time goes on, the behavior patterns of the IoV users may be changed, adding new behavior sequences to the observed variability all the time. Its significance is to continuously learn the behavior patterns of the IoV users, reduce the false alarm rate and prevent missing some new malicious behaviors, so as to better adapt to the changes of the IoV users' behavior.

3 Simulation Experiment and Result Analysis

3.1 Experimental Environment and Assessment Index

The system environment of this paper is a win10 64-bit operating system. Python 3.6 is selected as the programming environment. Pycharm community 2019.2.1 is selected as the programming platform. The Confusion matrix is selected and a comprehensive assessment is made from four indicators: Accuracy, Precision, Recall and F1-Score. Because the transaction data of the IoV users on the service cloud platform cannot be obtained directly. SEA data set [14] was selected as the simulation experimental data in this paper.

The SEA data set is composed of operation command files of 50 users in the UNIX system. Each user's data set contains 15000 operation commands,such as $\{cpp, sh, cpp, mvdir \cdots\}$. The first 5000 commands in the dataset are the normal operation commands of users, in the remaining commands, the operation commands of 20 masquerades who are not among the 50 users are inserted with a certain probability as the abnormal behavior data of the masquerades. And every 100 commands as a command block, 0 means that there is no abnormal operation behavior in the command block, 1 means that there is an abnormal operation behavior in the command block.

In this paper, a confusion matrix is used to assess the assessment results. The assessment results of the IoV user behavior can be divided into four situations: TP, FN, FP, TN [18]. TP refers to the number of normal behaviors of IoV users assessed as normal behaviors; FN refers to the number of normal behaviors of IoV users assessed as abnormal behaviors; FP refers to the number of abnormal behaviors of IoV users assessed as normal behaviors; TN refers to the number of abnormal behaviors of IoV users assessed as abnormal behaviors. The confusion matrix is shown in Table 1:

Table 1: Confusion matrix

Actual	**Assessment**	
	Normal	Abnormal
Normal	TP	FN
Abnormal	FP	TN

According to the elements in the confusion matrix [9], four standard assessment indexes can be obtained, as shown in Equation (7), Equation (8), Equation (9) and Equation (10).

1) Precision

$$\Pr e = \frac{TP}{TP + FP} \tag{7}$$

2) Recall

$$\mathrm{Re} = \frac{TP}{TP + FN} \tag{8}$$

3) Accuracy

$$Acc = \frac{TP + TN}{TP + FN + FP + TN} \tag{9}$$

4) F1-Score

$$F1 = \frac{2 \times \mathrm{Pr}\, e \times \mathrm{Re}}{\mathrm{Pr}\, e + \mathrm{Re}} \tag{10}$$

Accuracy is the only assessment index used by some researchers, but Accuracy cannot fully represent the assessment method. For example, the behavior in the user behavior data set is normal and some kinds of assessment methods evaluate all behaviors as normal behaviors. In fact, this is wrong, the Accuracy of the method will be close to 100%. However, this method will bring huge losses to users when they encounter identity theft attacks. Therefore, four assessment indicators were selected by this paper to assess the method more comprehensively and scientifically [2].

3.2 Experimental Simulation and Result Analysis

Because the operation behavior habits and environment of each user are different, the behavior between users and users is different. Therefore, it will take a lot of time to model the operation behavior of each user separately. Moreover, the number of abnormal behaviors in the SEA data set is less [8]. Although this is more in line with the actual situation, if the training set and test set are randomly assigned, it is very easy to appear the training set without abnormal behaviors, which makes the discrimination of data not enough and affects the assessment results.

In order to better simulate the real situation in the simulation experiment in this paper, the normal behavior data and abnormal behavior data from user 1 to user 9 in the data set are selected as the known user behavior data of IOV, namely the training set; The behavior data of User 10 is regarded as the unknown user behavior data of IoV, namely the test set. The sampling distribution of the data set is shown in Table 2:

Table 2: Sample distribution of data set

Num	Type	Number of Samples	
		Training	Testing
0	Normal	131300	13700
1	Abnormal	3700	1300

TF-IDF is used to calculate the weight value W_{a1} of the nine users' behaviors, and the key behavior features of the IoV users' behavior assessment are selected according to the calculation results. The feature?s weight value W_{a1} of IoV user behavior is shown in Table 3:

Table 3: Features weight value W_{a1}

Num	Features	W_{a1}
0	rm	0.067231
1	whodo	0.040209
2	su	0.025281
3	write	0.022363
4	cp	0.021354
5	ls	0.016226
6	cat	0.015828
7	gcc	0.012199
8	egrep	0.012052

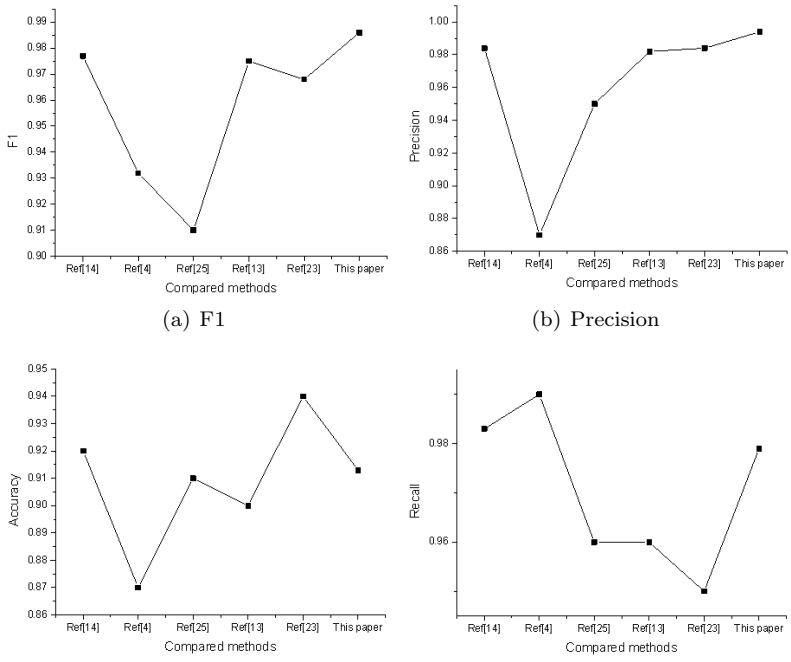
As can be seen from this Table: among all the operating commands of the nine IoV users, the most discriminative behavior features are rm and whodo. Because of the sixth behavior, the weight value W_{a1} is less than 0.02. If these behaviors are also considered as key behavioral characteristics of IoV user behavior assessment, the assessment results will be affected and time-consuming. Therefore, delete these redundant features or less important features. Only the first five operational behaviors were selected as key behavioral features. The behavior features of the IoV users are shown in Table 4:

Table 4: Behavior features of the IoV users

Num	Features	Description
0	rm	Delete sensitive data files
1	whodo	Query a user's access history
2	su	Change user account password
3	write	Talk to another user
4	cp	Copy sensitive file data

TF-IDF extracts five kinds of key behavior features of nine IoV users, which are rm, whodo, su, write, cp. That is, the number of corresponding behavior features in each state is $m = 5$, and the model parameter is; There are two states of sensitive data: dangerous and safe. That is, the number of model states is $n = 2$, and the model parameter. Using the Baum-Welch algorithm to train the model and determine the remaining parameters [12], a complete IoV user behavior model based on HMM is obtained to assess the behavior of unknown users of IoV. The confusion matrix of this paper is shown in Table 5:

In order to verify the performance of this method in the assessment of IoV user behavior, according to the confusion matrix, four indicators, Precision, Recall, Accuracy and F1-Score are compared with the existing research. In this paper, the methods proposed in reference [14], reference [4], reference [25], reference [13] and reference [23]



(a) F1 (b) Precision

(c) Accuracy (d) Recall

Figure 2: Comparison of experimental results

Table 5: Confusion matrix of this paper

Actual	**Assessment**	
	Normal	Abnormal
Normal	13413	289
Abnormal	86	1214

are selected as comparative experiments.

In reference [14], the bag of words model is used to process the data in the SEA dataset, and the LSTM algorithm is combined with a bimodal threshold mechanism to assess user security behavior. In reference [4], the bag of words model, N-Gram model and XG-Boost algorithm are combined to assess user behavior. N-Gram model can assess the difference between two strings and effectively compare the correlation of operational behavior before and after. In reference [25], the Random Forest algorithm is used to extract behavior features based on the user input frequency and effectively detect user's malicious operations. In reference [13], BiLSTM and Attention mechanisms are used to process serialized data and detect abnormal behavior. In reference [23], TF-IDF is used for feature extraction and LSTM training behavior model, so as to assess abnormal behaviors. The comparison of experimental results is shown in Figure 2.

According to this figure, Figure (a) is the experimental comparison diagram of F1-Score. Figure (b) is the experimental comparison diagram of Precision. Figure (c) is the experimental comparison diagram of Accuracy. Figure (d) is the experimental comparison diagram of Recall. Although the Recall index of the proposed method is lower than that of the reference [14] and reference [4]. Accuracy is lower than reference [14] and reference [23]. However, the comprehensive assessment indexes F1-Score and Precision are higher than other assessment methods. F1-Score is the harmonic average of Precision and Recall, and it is also the weighted average of Accuracy and Recall. When F1-Score is higher, it means that the assessment method is more effective in comprehensive behavior assessment. The experimental results show that the method based on HMM has obvious advantages over other methods in the field of IoV user behavior assessment.

In order to better verify the generalization ability of the proposed method, four users from User 11 to User 50 are randomly selected as test objects to detect whether the abnormal behaviors of these four users can be accurately assessed. The experimental results are shown in Figure 3.

From the analysis of the experimental results in figure, it can be seen that when the unknown users of IoV have many abnormal behaviors, such as (User24, User43). The method in this paper can accurately assess abnormal behavior; However, when there are few abnormal behaviors, such as (User25, User30), the model does not learn enough about abnormal behaviors, which leads to some errors in the assessment results. In addition, the improved weight calculation method for the user behavior sequence of IoV fully considers the correlation of user behavior, but it leads to the decrease of the weight value of some subsequent behaviors, which is regarded as abnormal behavior so that the assessed value of the experimental results is greater than the real value. This will be the need for

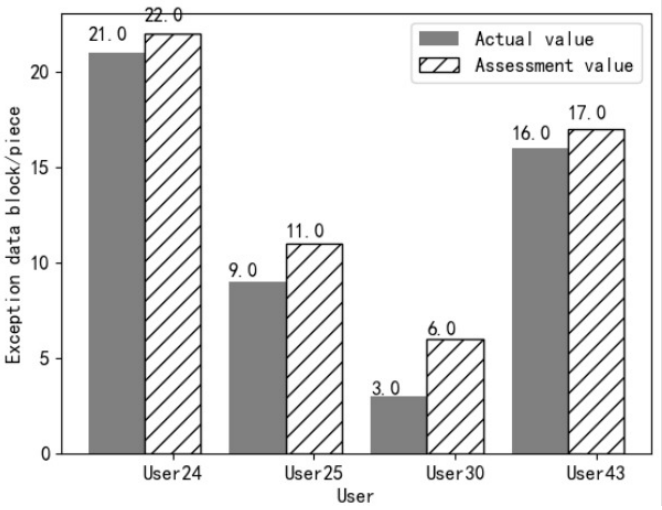


Figure 3: Assessment of abnormal behavior

improvement in future research.

4 Conclusion

This paper describes how to assess IoV user behavior based on HMM and TF-IDF, which adds a security guarantee of behavior authentication for the access control model of the IoV service cloud platform. Experimental results show that the method has the ability to assess the abnormal behavior of unknown users of IoV and it can also effectively protect the integrity, confidentiality and availability of sensitive data, and promote the popularization and promotion of the IoV service cloud platform.

In this paper, the assessment method of IoV user behavior based on HMM does not consider any special identity of IoV users, such as the administrator of the IoV service cloud platform and when there are abnormal behaviors in the behavior sequence, some subsequent behaviors will be regarded as abnormal behaviors. In future research, the method still needs to be improved to classify different identities of IoV users, so as to make the assessment method more comprehensive.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No.61862040, No.61762059 and No.6176 2060. The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] S. Ashry, W. Gomaa, and M. Abdu-Aguye, "Improved IMU based Human Activity Recognition Using Hierarchical HMM Dissimilarity," in *17th International Conference on Informatics in Control*, pp. 702–709. France, 2020.

[2] C. M. Chen, G. H. Syu, and Z.X. Cai, "Analyzing System Log based on Machine Learning Model," *International Journal of Network Security*, vol. 22, no. 6, pp. 925–933, 2020.

[3] G. R. Chen, K. Wang, and J. Tan, "A Risk Assessment Method based on Software Behavior," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 47–52. Shenzhen, 2019.

[4] M. S. Chen and K. H. Wu, "Internal Attack Detection based on Shell Commands," *Computerand Modernization (in chinese)*, no. 1, pp. 56–60, 2021.

[5] Y. Chule, A. Renzaglia, and A. Paigwa, "Driving Behavior Assessment and Anomaly Detection for Intelligent Vehicles," in *2019 IEEE International Conference on Cybernetics and Intelligent Systems (CIS)*, pp. 524–529. Bangkok, 2019.

[6] M. Fouad and A. H. Amr Talaat, "On Detecting IOT Power Signature Anomalies Using Hidden Markov Model HMM)," in *2019 31st International Conference on Microelectronics (ICM)*, pp. 108–112. Cairo, 2019.

[7] T. L. Gao, T. Li, and R. Jiang, "Research on Cloud Service Security Measurement based on Information Entropy," *International Journal of Network Security*, vol. 21, no. 6, pp. 1003–1013, 2019.

[8] J. B. He, J. Yang, and K. J. Ren, "Network Security Threat Detection under Big Data by Using Machine Learning," *International Journal of Network Security*, vol. 21, no. 5, pp. 768–773, 2019.

[9] L. C. Huang, C. H. Chang, and M. S. Huang, "Research on Malware Detection and Classification based on Artificial Intelligence," *International Journal of Network Security*, vol. 22, no. 5, pp. 717–727, 2020.

[10] J. Kim, J. Kim, and H. Kim, "Cnn-Based Network Intrusion Detection Against Denial of Service Attacks," *Electronics*, vol. 9, no. 6, pp. 916–937, 2020.

[11] M. Li, G. S. Xing, and Z. H. Wang, "Research on Real-time Online Intelligent Detection Technology of SQL Injection Behavior," *Journal of Hunan University (Natural Science Edition)(in chinese)*, vol. 47, no. 8, pp. 31–41, 2020.

[12] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, "Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing," *International Journal of Network Security*, vol. 21, no. 2, pp. 326–332, 2019.

[13] C. Z. Mu, Z. Xue, and Y. Shi, "Command Sequence Detection Method based on BILSTM and Attention," *Communication Technology(in chinese)*, vol. 52, no. 12, pp. 3016–3020, 2019.

[14] X. L. Tao, K. C. Kong, and F. Zhao, "Internal User Security Behavior Evaluation Method based on LSTM," *Journal of University of Electronic Science and Technology of China(in chinese)*, vol. 48, no. 5, pp. 775–789, 2019.

[15] X. N. Wang and X. Y. Li, "A Research of Gcforest Methods for Network Abnormal Behavior Detection," in *2020 International Conference on Computer Engineering and Application (ICCEA)*, pp. 218–221. Guangzhou, 2020.

[16] Z. N. Wu, L. Q. Tian, and Z. G. Wang, "Network User Behavior Authentication based on Hidden Markov Model," in *2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE)*, pp. 76–82. Chengdu, 2021.

[17] L. M. Xia and Z. M. Xia, "A New Method of Abnormal Behavior Detection Using LSTM Network with Temporal Attention Mechanism," *The Journal of Supercomputing*, vol. 4, no. 77, pp. 3223–3241, 2020.

[18] P. S. Xie, C. Fu, T. Feng, Y. Yan, and L. L. Li, "Malicious Attack Detection Algorithm of Internet of Vehicles based on CW-KNN," *International Journal of Network Security*, vol. 22, no. 6, pp. 1004–1014, 2020.

[19] P. S. Xie, C. Fu, X. Wang, T. Fen, and Y. Yan, "Malicious Atack Pevention Model of Internet of Vehicles based on IOV-SIRS," *International Journal of Network Security*, vol. 23, no. 5, pp. 835–844, 2021.

[20] H. W. Xue, Y. Liu, and W. C. Zhuang, "Vehicle Abnormal Behavior Detection Method based on Stacking Integrated Learning in Internet of Vehicles," *Automotive Engineering (in chinese)*, vol. 43, no. 4, pp. 501–508+536, 2021.

[21] P. Yang. *Research on Reverse Analysis Method for Network Protocol Behavior Model(in chinese)*. PhD thesis, Harbin Institute of Technology.

[22] X. Y. Ye, S. S. Hong, and M. Han, "Feature Engineering Method Using Double Layer Hidden Markov Model for Insider Threat Detection," *International Journal of Fuzzy Logic and Intelligent Systems*, vol. 20, no. 1, pp. 17–25, 2020.

[23] Y. H. Zhang, Z. Xue, and Y. Shi, "Rebound Shell Detection Method based on LSTM and TF-IDF," *Communication Technology (in chinese)*, vol. 53, no. 12, pp. 3046–3050, 2020.

[24] X. Zhou. *Research on Improved TF-IDF Feature Selection and Short Text Classification Algorithm(in chinese)*. PhD thesis, Anhui University.

[25] Z. Q. Zuo, S. Yong, and X. Zhi, "Malicious Command Detection Method Based on Machine Learning," *Communications Technology(in chinese)*, vol. 53, no. 11, pp. 2775–2779, 2020.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things.E-mail: xiepsh_lut@163.com

Yi-Fan Wang was born in Aug. 1996. She is a master student at Lanzhou University of Technology. Her major research field is network and information security. E-mail: 844782234@ qq.com

Zong-liang Wang was born in Mar. 1997. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1292094887@ qq.com

Nan-nan Li was born in Feb. 1997. She is a master student at Lanzhou University of Technology. Her major research field is network and information security. E-mail: 2500466296@ qq.com

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, network and information security technology. E-mail: fengt@lut.cn

Yan Yan was born in Oct.1980.She is a associate professor and a supervisor of master student at Lanzhou University of Technology. Hermajor research field is privacy protection, multimedia information security.E-mail:yanyan@lut.cn

Conditional Privacy-Preserving Authentication Scheme for IoV Based on ECC

Peng-Shou Xie, Xiao-Jie Pan, Hong Wang, Jia-Lu Wang, Tao Feng, and Yan Yan
(Corresponding author: Xiao-Jie Pan)

School of Computer and Communications, Lanzhou University of Technology
No. 36 Peng-jia-ping road, Lanzhou, Gansu 730050, China
Email: 1075224210@qq.com

(Received July 23, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 23, 2022)

Abstract

Internet of Vehicles (IoVs) is an important part of intelligent transportation systems that could improve the safety and efficiency of vehicle nodes. However, due to the mobility of IoVs, there are some security and privacy concerns in IoVs. The conditional privacy-preserving authentication (CPPA) scheme based on Elliptic Curve Cryptography (ECC) is proposed in this paper. This paper uses the small exponent test technology to achieve batch verification of multiple messages through Road Side Unit (RSU). To achieve anonymous authentication, our scheme uses the real identity of the vehicle node to generate an anonymous identity. According to security proof, our scheme can against adaptively chosen message attacks in the random oracle model. Furthermore, according to performance evaluation, our scheme reduces computation and communication costs without bilinear pairing. Therefore, our scheme is safer and more efficient than previous schemes, suitable for IoVs.

Keywords: Anonymous Identity; Authentication; Internet of Vehicles; Privacy-Preserving

1 Introduction

In recent years, with the progress of the development of wireless communication technology, IoVs have gradually become a promising research field [28]. As an application of intelligent transportation, IoVs have received a lot of attention as an important technology in the field of wireless network technology [3]. However, as an open wireless network, IoVs are in a state of high-speed movement, which has led to frequent privacy leakage accidents [26]. Thus, privacy of identity and secure communication cannot be ignored in IoVs [8].

In IoVs, each vehicle node transmits these messages to neighboring vehicle nodes via a dedicated short range communication (DSRC) protocol [2]. According to DSRC protocol, each vehicle in IoVs broadcasts a traffic message every 100-300 ms .Due to the fast-moving characteristics of vehicle nodes, vehicle nodes need to broadcast traffic message frequently, which require high real-time performance [17]. However, due to the limitations of wireless communication technology, vehicle nodes may suffer from message loss and forgery [24]. Therefore, it is necessary for receivers to authenticate messages and verify their integrity before receiving them. In addition, the security of traffic information and personal privacy is another issue in vehicle nodes communication [15]. In IoVs, attackers may obtain the user's personal information during the communication process, or obtain the vehicle's driving route by tracking the messages of On-Board Units OBU [11]. Besides, because the infrastructures in IoVs have the characteristics of openness and complexity, it will lead to a malicious attacker launches various attacks such as modification attack, denial of service attack(DoS) and so on [7, 23].

In recent years, security and privacy have become hot areas for IoVs. People want to enjoy the convenience of the vehicle network while keeping safety of the vehicle [20]. In order to solve these issues, a number of signature schemes for the authentication of traffic messages have been proposed by researchers.

1.1 Related Works

Security and privacy has always been an important area of research for IoVs. In order to achieve the secure communication between Vehicle-To-Vehicle (V2V) communication and Vehicle-To-Infrastructure (V2I)communication , a number of different authentication schemes have proposed in recent years [1]. Dissanayake *et al.* [6] proposed a novel digital signature algorithm with proving the efficiency against some kind of cyber attacks.The algorithm can be applied to the IoVs to ensure the security of messages. Hu *et al.* [9] used distributed and difficult-to-tamper characteristics of blockchain to propose an anonymous handover authentication scheme. Their scheme achieved robust security and high efficiency. Wang *et al.* [22] proposed a batch authentication scheme based identity. In their scheme, the secret key of the vehicle

node depended on the RSU to prevent the leakage of vehicle node's secret key effectively. However, their scheme is vulnerable to attack as malicious vehicle nodes could impersonate legitimate vehicle nodes to generate false signatures. Wang *et al.* [21] proposed a secure blockchain based authentication scheme. In their scheme, a trusted cloud server is designed to store the anonymous certificates of vehicle nodes. Although the scalability of system is improved, many certificates increase computation cost and communication cost.

In 2020, Xu *et al.* [27] proposed a new certificateless aggregate signature scheme which is efficient in generating a signature and verification. Their scheme is secure under the extended computational Diffie-Hellman assumption.

In 2019, Alazzawi *et al.* [19] proposed an effective and robust authentication scheme for pseudo-identity communication. In their scheme, vehicle nodes sign a beacon so that the Trusted Authority(TA) obtains the real identity of the malicious vehicle nodes, and then deletes malicious vehicle nodes from the registration list. However, side-channel attacks can gain access to the private messages of the vehicle nodes, which undermines the security of the vehicle nodes.

Li *et al.* [13] proposed a lightweight authentication protocol. The protocol used hash functions and XOR operations to reduce communication cost. However, their protocol has relatively high storage overhead because of distribution and revocation of the certificate list, which is not suitable for IoVs. Elliptic curve cryptography is used in some authentication schemes [10, 25]. In their schemes, the system master key is generated by Private Key Generator (PKG), which eliminate the cost of certificate management and storage. However, the integrity of their schemes rely on the PKG, and there is a risk that the private key will be leaked once the PKG is attacked.

In 2020, Ali *et al.* [8] proposed an effective ID-based signature scheme. Their scheme used general one-way hash functions to speed up the process of signature verification. At the same time, their scheme supported batch verification of a large amount of information from vehicle nodes in high traffic density area, which reduces the computation cost of the RSU. However, bilinear pairing is used in verification scheme, which increases the computation cost in the verification phase.

Liu and Wang [9] proposed a conditional privacy-preserving scheme based on ring signature. In their scheme, the process of creating a ring is restricted, therefore ring members can be audited. However, the bilinear pairing operation causes the RSU increase the computation cost in message verification phase. Li *et al.* [20] proposed an effective message authentication scheme, which can resist the attack of key exposure. However, the scheme [20] uses Map-to-Point hash function operations, which increase computation cost in message verification phase.

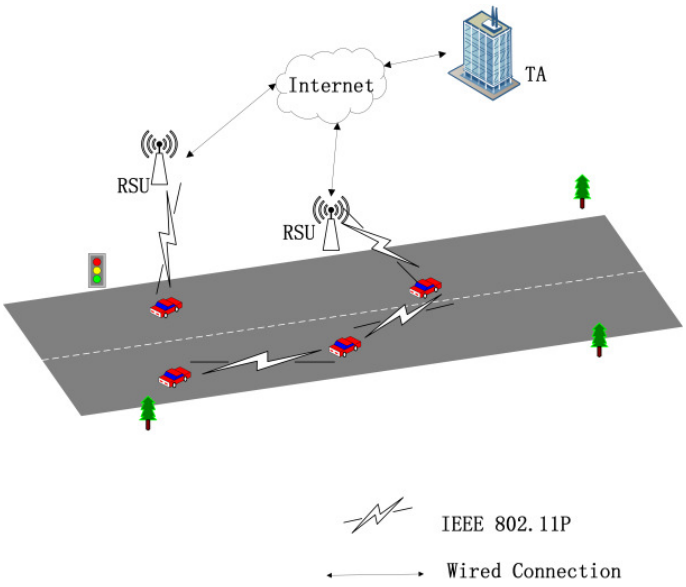


Figure 1: Network system of IoV

1.2 Our Contributions

In this paper, an efficient and secure authentication scheme is proposed in IoVs. The contributions of this paper are summarized as follows:

- Security analysis shows that our scheme can against forgery under adaptive chosen message attack under the random oracle model.
- Our scheme satisfies the security requirements for V2I communication in IoVs such as unlinkability requirements,traceability requirements and anonymous authentication.
- Our scheme without using pairing operations and Map-To-Point hash functions, which reduces computation cost and communication cost.

1.3 Organization

The rest of the this paper is organized as follows. Some preliminaries and security requirements are introduced for IoVs in Section2. The details of our scheme are shown in Section 3. Security analysis of our scheme is shown in Section 4. The performance of our scheme is shown in Section 5. Finally, Section6 concludes this paper.

2 Preliminaries

In this section, we introduce a network system of IoVs, security requirements and elliptic curve cryptography.

2.1 Network System

As shown in Figure 1, the network system of IoVs comprises three components:a trusted authority,a vehicle

node, and an RSU. Three components are described as follow:

- **TA:** In IoVs, the TA is a registration center for RSUs and OBUs, which can obtain the real identity of vehicle nodes. System parameters are generated by the TA and sent to vehicle nodes.
- **RSU:** In IoVs, the RSU has higher computing power than OBUs. It is capable of receiving and verifying the authenticity of the traffic messages from vehicle nodes. In addition, the RSU can communicate with trusted authority to obtain some messages , such as notification messages.
- **OBU:** In IoVs, each vehicle node is equipped with an OBU. OBUs communicate with other RSUs and vehicle nodes based on the DSRC protocol. Compared to RSUs and TAs, OBUs have smaller computation power and storage capacity.

2.2 Security Requirements

In this paper, our scheme should satisfy security requirements as follows:

- **Message authentication and integrity**

  In IoVs, the RSU can ensure senders are legal vehicle nodes. In addition, the RSU can detect whether the messages have been tampered in the process of communication.

- **Identity privacy preserving**

  In IoVs, any RSU and vehicle node cannot obtain the real identity of vehicle nodes from traffic messages. The real identity of vehicle nodes can only be obtained by the trusted authority when privacy of vehicle nodes is threatened.

- **Traceability**

  In IoVs, the TA as a trusted authority has the ability to obtain the real identities of attackers when malicious attackers destroy messages, then marks attackers as illegal nodes.

- **Unlinkability**

  Malicious attackers receive some messages from a vehicle node, but attackers could not infer that these messages come from the same vehicle node.

2.3 Elliptic Curve Cryptography

We assume that F_p is the finite field, which p is a prime number. An elliptic curve E over a finite field F_p and be defined as $y^2 = y^3 + ax + b \bmod p$,where $a, b \in F_p$ and $(4a^3 + 27b^2) \bmod q \neq 0$.Suppose O is a point at infinity on E. Point O and points of ECC make up an additive elliptic curve group G with the order q and generator P.

3 The Proposed Scheme

In this section, a secure and efficient conditional privacy-preserving authentication scheme is proposed in detail for IoVs. Our scheme consists of the following five phases: system initialization phase, handshaking phase, anonymous identity generation phase, message signing phase and message verification phase. The notations used in the scheme are shown in Table 1.

Table 1: Notations

Notations	Description
V_i	The ith vehicle node
RSU	A roadside unit
OBU	A onboard unit
p, q	Two large prime numbers
s	The private key of the system
G	Cyclic additive group
P	A generator of the group G
P_{pub}	The public key of the system
AID_i	The anonymous identity of a vehicle node
OID_i	The real identity of a vehicle node
h_0, h_1, h_2	Three one-way hash functions
T_i	Current timestamp
M_i	Message
$\|$	The message concatenation operation
R	The exclusive-OR operation

Step 1. System initialization phase

1) The TA selects an elliptic curve as $y^2 = y^3+ax+b \bmod p$. Then, TA selects an additive group G with the order q. The P is a generator of additive group G.
2) The TA chooses a number $s \in Z_q^*$ as the master key of the system randomly, and then computes $P_{pub} = sP$ as master public key. Three one-way general hash functions such as $h_0 : \{0,1\}^* \rightarrow Z_q^*$,$h_1 : \{0,1\}^* \rightarrow Z_q^*$,$h_2 : \{0,1\}^* \rightarrow Z_q^*$ are chosen by the TA. Hash function h_0 is not published across IoVs because of it only involve in generating an anonymous identity AID_i.
3) Public parameters of the system are set $params = \{G, q, P, P_{pub}, h_1, h_2\}$.Then, the TA publish params to RSUs and vehicle nodes through secure channel.

Step 2. Handshaking phase

1) When the vehicle node V_i enters the communication range of the RSU, real identity OID_i of the vehicle node is encrypted by the RSU's public key into $Q = ENC_{PK_{RSU}}(OID_i, SIG_{SK_{OBU}}(OID_i))$. Then, the vehicle node V_i sends handshake

message $Z = (Q, T_i)$ to the RSU, where T_i is a timestamp.

2) Once handshake message Z is received, the RSU checks whether T_i is valid. If T_i is valid, the RSU decrypts Z to get real identity OID_i. Then, the RSU encrypts OID_i and identity of RSU RID_i into $W = ENC_{PK_{TA}}((OID_i, RID_i))$ by TA's public key PK_{TA}. Finally, W is sent to TA.

3) Once W is received, TA decrypts W to get OID_i and RID_i. Then, TA checks whether RID_i is in the registration list. If so, then TA continues to check whether OID_i is not in revocation list. If OID_i is not in revocation list, the RSU and vehicle node V_i are allowed to join IoVs, then TA sends a notification message $(verified, u_i, a_i)$ to the RSU. Otherwise TA sends a notification message (not verified)to the RSU.Two secret values u_i and a_i are generated by TA.

4) Once notification message is received, the RSU checks notification message whether is $(verified, u_i, a_i)$, If so, the RSU computes $A_i = a_i P$ and $U_i = u_i P$. Otherwise the vehicle node V_i will be identified as illegal. We assume that β_i is the unique symbol of the vehicle node, where $\beta_i = U_i + A_i$. Finally, the RSU sends β_i to TA and the vehicle node V_i.

Step 3. Anonymous identity generation phase

Before generating an anonymous identity, the vehicle node V_i inputs the unique real identity OID_i and password PWD_i to the tamper-proof device firstly. The tamper-proof device checks whether OID_i and PWD_i are equal to the stored values. If they are equal, the anonymous identity is generated as follows.

1) TPD generates a secret value $\gamma_i \in Z_q^*$ randomly and computes $AID_{i,1} = \gamma_i P$. Then, the tamper-proof device sends $(AID_{i,1}, OID_i)$ to TA through secure channel.

2) Once $(AID_{i,1}, OID_i)$ is received, the TA computes $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$, where t_i is the timestamp that shows the validity of time for AID_i. Then, TA computes $SK_i = \eta_{AID_i} s \bmod q + u_i$. The secret key of the anonymous vehicle node V_i is (β_i, SK_i). In addition, we defined that $AID_i = (AID_{i,1}, AID_{i,2} \parallel t_i)$ and $\eta_{AID_i} = h_1(AID_i \parallel \beta_i)$.

Step 4. Message signing phase

In this phase, TA sends AID_i and (β_i, SK_i) to the vehicle node V_i through secure channel. Then vehicle node V_i signs message to ensure the authenticity of the message. The process of signing a message is as follows:

1) The vehicle node V_i randomly selects a number $r_i \in Z_q^*$. Then, the vehicle node V_i computes $R_i = r_i P$ and $\sigma_i = r_i + \mu_{AID_i}(a_i + SK_i \bmod q)$. The signature of a message M_i is (σ_i, R_i). Note that the R_i can be preloaded to the vehicle node V_i. We define that $\mu_{AID_i} = h_2(R_i \parallel AID_i \parallel M_i \parallel SK_i \parallel T_i)$ and $AID_i = (AID_{i,1}, AID_{i,2})$.

2) Finally, the vehicle node V_i sends a message as $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ to nearby RSUs.

Step 5. Message verification phase

In this phase, the RSU receives a message as $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ and verifies the validity of the message. Once the message is received, the RSU checks timestamp T_i whether is fresh firstly. If so, the RSU continues to verify the message. Otherwise, the RSU discards the message. The process of verification as follows:

Single Verification.

Once $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ is received from the vehicle node V_i, the RSU checks whether the following Equation (1) holds.

$$\sigma_i P = R_i + \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub}) \tag{1}$$

If the Equation (1) holds, we can conclude that message $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ is valid. The correctness of the Equation (1) is as follows:

$$\begin{aligned} &\sigma_i P = (r_i + \mu_{AID_i}(a_i + SK_i \bmod q))P \\ &= r_i P + \mu_{AID_i}(a_i P + (\eta_{AID_i} s \bmod q + u_i)P) \\ &= R_i + \mu_{AID_i}(A_i + \eta_{AID_i} P_{pub} + U_i) \\ &= R_i + \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub}) \end{aligned}$$

Therefore, the correctness of the Equation (1) is proved. The message from vehicle node V_i has not been altered by malicious attackers.

Batch Verification.

In order to improve the efficiency of verification, our scheme supports batch verification. The small exponent test technology [18] is used to batch verification. Once multiple messages are received from the vehicle node as $\{AID_1, \sigma_1, M_1, T_1, R_1\}$,$\{AID_2, \sigma_2, M_2, T_2, R_2\}$, $\{AID_n, \sigma_n, M_n, T_n, R_n\}$. The RSU checks whether Equation (2) holds for the following:

$$\begin{aligned} (\sum_{i=1}^{n} \nu_i \sigma_i)P \quad &= \quad \sum_{i=1}^{n} \nu_i R_i \\ &+ \sum_{i=1}^{n} \nu_i \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub}) \end{aligned} \tag{2}$$

If Equation (2) holds, we can conclude that multiple messages are valid. The correctness of the

Equation (2) is as follows:

$$\begin{aligned}
&(\sum_{i=1}^{n} v_i\sigma_i)P \\
= \ &(\sum_{i=1}^{n} v_i(r_i + \mu_{AID_i}(a_i + SK_i \bmod q)))P \\
= \ &(\sum_{i=1}^{n} v_i r_i)P + (\sum_{i=1}^{n} v_i\mu_{AID_i}(a_i P \\
&\quad +(\eta_{AID_i} s \bmod q + u_i)P)) \\
= \ &\sum_{i=1}^{n} v_i R_i + \sum_{i=1}^{n} v_i\mu_{AID_i}(A_i \\
&\quad +\eta_{AID_i} P_{pub} + U_i) \\
= \ &\sum_{i=1}^{n} v_i R_i + \sum_{i=1}^{n} v_i\mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub})
\end{aligned}$$

Therefore, the correctness of Equation (2) is proved.The messages from vehicle node V_i have not been altered by malicious attackers.

4 Security Proof and Security Analysis

The security of our scheme is proved in this section. Through security analysis, we have proved that our scheme can achieve the security requirements proposed in Section 3.

4.1 Security Proof

Mathematical Model: The security proofs of our proposed CPPA protocol is given in this subsection. The security model of proposed scheme is defined through a game played between a challenger C and an adversary A.Random oracle model is a mathematical model which abstracted from the hash function. It is widely used in provable security. In this paper, we use random oracle model to prove the our scheme is secure against adaptive chosen message attack. The adversary A could make the following queries in the game.

- Setup-Oracle: This query simulates the initialization of the VANET system.The system parameters are sent to the adversary A.
- $h_1$oracle: In response to this query, challenger C chooses a random number $r \in Z_q^*$ inserts the tuple (m, r) into the list Lh_1 and returns r to adversary A.
- $h_2$oracle: In response to this query, challenger C chooses a random number $r \in Z_q^*$ inserts the tuple (m, r) into the list Lh_2 and returns r to adversary A.
- Sign-Oracle: In this query, the adversary A sends a traffic information message M_i to challenger C.In response, C sends $\{\mathrm{AID}_i,\sigma_i,\mathrm{M}_i,\mathrm{T}_i,\mathrm{R}_i\}$ to the adversary A.

Theorem 1. *We assume that times of algorithm A requests random oracle query and request signature oracle query is Q and Y respectively. If our conditional privacy-preserving authentication scheme can be broken by algorithm A , then there is an algorithm C to solve the ECDL problem.*

Proof. We assume that A is an adversary that could forge the message $\{\mathrm{AID}_i,\sigma_i,\mathrm{M}_i,\mathrm{T}_i,\mathrm{R}_i\}$. Then, ECDL problem is be solved by challenger C with a non-negligible probability. The Lh_1 and Lh_2 are lists which maintained by the C. Now, query phase is shown as follows:

Setup-Oracle. Challenger C picks a number s randomly as its master key. Then, C calculates the public key as $P_{pub} = sP$ and sends system parameters $params = \{G, q, P, h_1, h_2\}$ to A.

h_1 **oracle.** The Lh_1 is a list which maintained by C. When adversary A issues a query with message (AID_i, β_i) to C, the C checks whether $\langle AID_i, \beta_i, \tau_1\rangle$ exists in Lh_1. If so, C issues $\tau_1 = h_1(AID_i, \beta_i)$ to A; otherwise, C picks a number $\tau_1 \in Z_q^*$ and then adds (AID_i, β_i) into Lh_1. Finally, C returns $\tau_1 = h_1(AID_i, \beta_i)$ to A.

h_2 **oracle.** The Lh_2 is a list which maintained by C. When adversary A issues a query with message $(R_i, AID_i, M_i, SK_i, T_i)$ to C, the C checks whether $\langle R_i, AID_i, M_i, SK_i, T_i, \tau_i\rangle$ exists in Lh_2. If so, C issues $\tau_2 = h_2(R_i, AID_i, M_i, SK_i, T_i)$ to A; otherwise, C picks a number $\tau_2 \in Z_q^*$ and then adds $(R_i, AID_i, M_i, SK_i, T_i)$ into Lh_2. Finally, C returns $\tau_2 = h_2(R_i, AID_i, M_i, SK_i, T_i)$ to A.

Sign-Oracle. When adversary A issues a query with a message M_i, challenger C checks the $\langle AID_i, \beta_i, \tau_1\rangle$ from Lh_1 firstly. The C then retrieves τ_1 from $\langle AID_i, \beta_i, \tau_1\rangle$ and selects two numbers r_i and H_i. Next, C selects two random numbers s_i and l_i to try again. The C computes $R_i = H_i^{-1}s_iP - Q$ and $\sigma_i = s_i$, then returns (R_i, σ_i) to A. We set H_i as $h_2(R_i, AID_i, M_i, SK_i, T_i)$.

The A could achieve two valid signatures $(R_i, \sigma_i = r_i + H_i(a_i + SK_i \bmod q))$ and $(R_i, \sigma_i' = r_i + H_i'(a_i + SK_i \bmod q))$ by forking lemma , where $H_i \neq H_i'$. The C can get value of r_i as follows:

$$\begin{aligned}
&\frac{H'_i\sigma_i - H_i\sigma'_i}{H'_i - H_i} \bmod q \\
= \ &\frac{H'_i r_i + H'_i H_i(a_i + SK_i) - H_i r_i - H_i H'_i(a_i + SK_i)}{H'_i - H_i} \\
= \ &r_i
\end{aligned}$$

We have proved the our scheme can against forgery under adaptive chosen message attack in the random oracle model.

□

4.2 Security Analysis

In this subsection, we introduce our scheme satisfies some security requirements as follows:

- **Message authentication and integrity**

  According to the above security proof, the ECDL problem is difficult to solve. Thus, malicious attackers cannot forge any signature. RSUs can verify the correctness of Equation (1) to determine whether the messages from a vehicle node has been tampered or forged by malicious attackers. Thus, we make a conclusion that our scheme satisfies message authentication and integrity.

- **Identity privacy preserving**

  In anonymous identity generation phase, our scheme generates anonymous identities $AID_{i,1}$ and $AID_{i,2}$. According to $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$ and $AID_{i,1} = \gamma_i P$, the anonymous identity $AID_i = (AID_{i,1}, AID_{i,2})$ contains two random secret numbers γ_i and s. In order to get OID_i, malicious attackers must compute $sAID_{i,1} = s\gamma_i P$ from $P_{pub} = sP$ and $AID_{i,1} = \gamma_i P$. It means that attackers must solve CDH problem. Thus, we make a conclusion that our scheme satisfies identity privacy-preserving .

- **Traceability**

  The real identity of a vehicle node is not available to any RSU or vehicle node. However, as a trusted authority, TA can obtain the real identity of malicious attackers when malicious attackers destroy messages. As a trusted center, TA computes $OID_i = AID_{i,2} \oplus h_0(sAID_{i,1} \parallel t_i)$ through $\{AID_n, \sigma_n, M_n, T_n, R_n\}$.Thus, we make a conclusion that our scheme satisfies traceability.

- **Unlinkability**

  Our scheme chooses two random secret numbers γ_i and s to generate an anonymous identity AID_i, where $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$ and $AID_{i,1} = \gamma_i P$. In addition, the vehicle node V_i chooses a random secret number r_i to generate a signature. That is to say, each message from vehicle node V_i has an unique anonymous identity and signature. Attackers can not link any message. Thus, we make a conclusion that our scheme satisfies unlinkability.

5 Performance Evaluation

In this section, we evaluate the performance of schemes in terms of computation cost and communication cost. The schemes [4,21,27] are based on ECC. The schemes [8,9,17, 20] are based on bilinear pairing. Our scheme is compared with these schemes.

5.1 Computation Cost

In this paper, we use a famous cryptographic library MIRACL to calculate the execution time of cryptographic operations. The experiment of our scheme is performed on a PC equipped with an Intel i5 2.30 GHZ CPU and 8 GB memory. The execution time of the encryption operations are shown in Table 2. We denote T_{BP} as the execution time of bilinear pairing operation, T_H as the execution time of Map-To-Point hash function,T_{PM-BP} as the execution time of point multiplication operation in bilinear pairing, T_{PA-BP} as the execution time of point addition operation in bilinear pairing,T_{PM-ECC} as the execution time of point multiplication operation in ECC, T_{PA-ECC} as the execution time of point addition operation in ECC.

Table 2: Execution time of the encryption operations

Cryptographic operation	Execution time(ms)
T_{BP}	4.2110
T_H	4.406
T_{PM-BP}	1.709
T_{PA-BP}	0.0071
T_{PM-ECC}	0.442
T_{PA-ECC}	0.0018

In single message verification phase, the Ali *et al.*'s scheme [8] requires one bilinear pairing operation, one point multiplication operation in bilinear pairing and one point addition operation in bilinear pairing. Thus, the verification time in this phase is $1T_{BP} + 1T_{PM-BP} + 1T_{PA-BP} \approx 5.9271ms$. In batch message verification, the verification time is $1T_{BP} + nT_{PM-BP} + nT_{PA-BP} \approx 1.7161n + 4.2110ms$. Similarly, the execution times of the other three schemes based on bilinear pairing are shown in Table 3.

In single message verification phase, our scheme requires three point multiplication operations in ECC and two point addition operations in ECC. Thus, the verification time in this phase time in this phase is $3T_{PM-ECC} + 2T_{PA-ECC} \approx 1.3296ms$.In batch message verification, the verification time is $(n+2)T_{PM-ECC} + (3n-1)T_{PA-ECC} \approx 0.4474n + 0.8822ms$. Similarly, the execution times of the other three schemes based on ECC are shown in Table 3.

The percentage improvement of our scheme with respect to single and batch signature verifications as compared to the scheme [17] is $\frac{7.6290-1.3296}{7.6290} \approx 82.57\%$ and $(\frac{3.4180n+4.2110-(0.4474n+0.8822)}{3.1480n+4.2110}) \approx 86.81\%$, respectively,where $n = 100$ is the number of signatures.Other percentage improvement could be achieved by using a similar method.The improvement on computation cost of the our scheme is shown in the Table 4.

The computation cost of single message verification is shown in Figure 2. From Figure 2, it can be seen that the computation cost of our scheme is lower than schemes [8,9,17,20] because of bilinear pairing is not used in our scheme. In schemes [4, 21, 27] based on ECC, the

Table 3: Comparison of computation cost

Scheme	Single Verification(ms)	BatchVerification(ms)
Scheme [17]	$2T_{PM-BP} + 1T_{BP} \approx 7.6290$	$1T_{BP} + 2nT_{PM-BP} \approx 3.4180n + 4.2110$
Scheme [8]	$1T_{BP} + 1T_{PM-BP} + 1T_{PA-BP} \approx 5.9271$	$1T_{BP} + nT_{PM-BP} + nT_{PA-BP} \approx 1.7161n + 4.2110$
Scheme [9]	$2T_{BP} + 1T_{PM-BP} \approx 10.1310$	$2T_{BP} + nT_{PM-BP} \approx 1.7090n + 8.4220$
Scheme [20]	$T_{BP}+1T_{PM-BP}+1T_{PA-BP}+1T_H \approx 14.5441$	$2nT_{BP} + nT_{PM-BP} + nT_{PA-BP} + nT_H \approx 14.5441n$
Scheme [4]	$4T_{PM-ECC} + 3T_{PA-ECC} \approx 1.7734$	$(2n + 3)T_{PM-ECC} + (4n - 1)T_{PA-ECC} \approx 0.8912n + 1.3242$
Scheme [21]	$4T_{PM-ECC} + 3T_{PA-ECC} \approx 1.7734$	$(2n + 2)T_{PM-ECC} + (4n - 1)T_{PA-ECC} \approx 0.8912n + 0.8822$
Scheme [27]	$4T_{PM-ECC} + 2T_{PA-ECC} \approx 1.7716$	$(2n + 2)T_{PM-ECC} + (3n - 1)T_{PA-ECC} \approx 0.8894n + 0.8822$
Our Scheme	$3T_{PM-ECC} + 2T_{PA-ECC} \approx 1.3296$	$(n + 2)T_{PM-ECC} + (3n - 1)T_{PA-ECC} \approx 0.4474n + 0.8822$

Table 4: Percentage improvement of the our scheme over other scheme

Scheme	Single Verification	Batch Verification
Scheme [17]	82.57%	86.81%
Scheme [8]	77.57%	74.05%
Scheme [9]	86.88%	74.56%
Scheme [20]	90.86%	96.86%
Scheme [4]	23.05%	49.56%
Scheme [21]	25.03%	49.31%
Scheme [27]	24.97%	49.21%

computation cost of our scheme is lower than Wang *et al.*'s scheme [4] and Ming *et al.*'s scheme [21] because of our scheme uses less point operation in message signing phase. The computation cost of batch signature verification is shown Figure 3, which increases with the number of messages.

5.2 Communication Cost

The size of the elements in G_1 is 128 bytes and the size of the elements in G is 40 bytes. In addition, we suppose that the size of a general one-way hash function is 20 bytes, and the size of a time-stamp is 4 bytes. In Lawrence *et al.*'s scheme [4], the signature $\{\sigma_i, t_i\}$ is sent from a vehicle node to the receiver, where $\sigma_i = (k_i, U_i, S_i)$, $U_i, S_i \in G_1$ and $k_i \in Z_q^*$. Thus, the communication cost is $128 \times 2 + 20 + 4 = 280bytes$. In Ali *et al.*'s scheme [5], the signature $\{AID_i, \sigma_i, t_i\}$ is sent from a vehicle node to the receiver,where $\sigma_i = (A_i, B_i)$,$AID_i = (AID_{i,1}, AID_{i,2})$, $A_i, B_i, AID_{i,1} \in G_1$ and $AID_{i,2} \in Z_q^*$. Thus, the communication cost is $128 \times 3 + 20 + 4 = 408bytes$. In Wang and Liu.'s scheme [14], the signature $\{AID_i, \sigma_i, t_i\}$ is sent from vehicle node to the receiver, where $\sigma_i = (A_i, B_i)$ and $A_i, B_i, AID_i \in G_1$.Thus, the communication cost is $128 \times 3 + 20 + 4 = 408bytes$. In Liu *et al.*'s scheme [12], the signature $\{OID_i, \sigma_i, t_i\}$ is sent from a vehicle node to the receiver, where $\sigma_i = (A_i, B_i, C_i)$, $A_i, B_i, C_i \in G_1$ and $OID_i \in Z_q^*$. Thus, the communication cost is $128 \times 3 + 20 = 404bytes$.

In Wang *et al.*'s scheme [22], the signature $\{AID1_{i,j}, AID2_{i,j}, U_{i,j}, \nu_{i,j}, T_i\}$ is sent from vehicle node to the receiver, where $AID1_{i,j}, AID2_{i,j}, U_{i,j} \in G$. Thus, the communication cost is $40 \times 3 + 20 \times 1 + 4 \times 1 = 144bytes$.In Ming *et al.*'s scheme [16], the signature $\{AID_i, tt_i, P_i, D_i, R_i, \sigma_i\}$ is sent from a vehicle node to the receiver, where $AID_i = (AID_{i,1}, AID_{i,2})$ and $P_i, D_i, R_i, \sigma_i \in Z_q^*$. Thus, the communication cost is $40 \times 1 + 20 \times 4 + 4 \times 1 = 124bytes$. In Thumbur *et al.*'s scheme [19],the signature $\{vpk_i, PID_i, T_i, \sigma_i\}$ is sent from a vehicle node to the receiver, where $PID_i = (PID_{i,1}, PID_{i,2}) \in G$, $\sigma_i = (U_i, S_i)$, $U_i, vpk_i \in G$ and $S_i \in Z_q^*$. Thus, the communication cost is $40 \times 4 + 20 \times 1 + 4 \times 1 = 184bytes$. In our scheme, the signature $\{AID_i, \sigma_i, M_i, T_i, R_i\}$ is sent from a vehicle node to the receiver, where $PID_i = (PID_{i,1}, PID_{i,2})$, $PID_{i,1}, R_i \in G$ and $PID_{i,2}, \sigma_i \in Z_q^*$. Thus, the communication cost is $40 \times 2 + 20 \times 2 + 4 \times 1 = 124bytes$.

As can be seen from Table 5, the bilinear pairing-based scheme [8,9,17,20] has higher communication costs than our scheme. In the schemes [4, 21, 27] based on ECC, the communication cost of our scheme is lower than schemes [4, 27]. Although our scheme is the same as scheme [21], it is superior to scheme [21] in individual signature verification and batch signature verification.

6 Conclusions

In this paper, a CPPA scheme is proposed, which uses a batch signature verification method to allow RSUs to

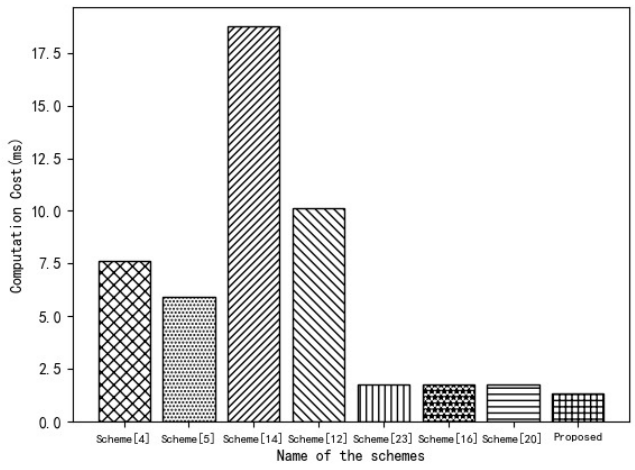


Figure 2: Computation cost for single message verification

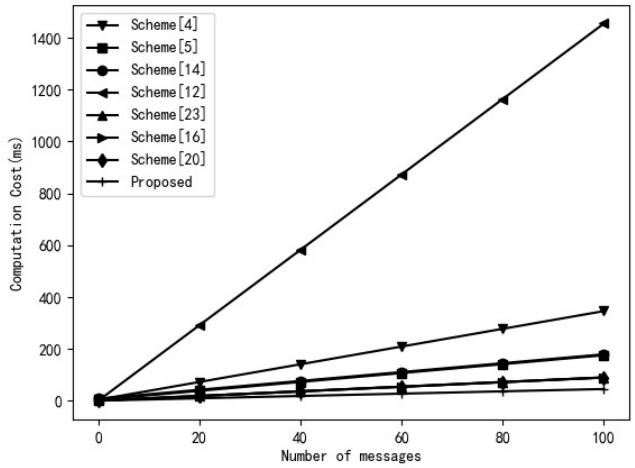


Figure 3: Computation cost for batch messages verification

Table 5: Comparison of communication cost

Scheme	Send a message	Send n messages
Scheme [17]	208 bytes	208 bytes
Scheme [8]	408 bytes	408 bytes
Scheme [9]	408 bytes	408 bytes
Scheme [20]	404 bytes	404 bytes
Scheme [4]	144 bytes	144 bytes
Scheme [21]	124 bytes	124 bytes
Scheme [27]	184bytes	184bytes
Our scheme	124 bytes	124 bytes

verify multiple messages. In order to prevent vehicle nodes from exposing their identities, our scheme generates anonymous identity during transmission. For malicious vehicle nodes, the trust authority TA can obtain its real identity, which realizes conditional privacy-preserving authentication. We provide a security analysis to show our CPPA scheme can satisfy security and privacy requirements. Hence, our scheme is suitable for IoVs.

Our scheme only considers the identity privacy of vehicle nodes, and does not consider the location privacy and route of vehicle nodes. In addition, the safety of vehicle nodes depends on TPD. Once the TPD is attacked, the safety of vehicle nodes will be destroyed. In the future, we should reduce the dependence of vehicle nodes on TPD and strengthen the protection of location privacy.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No.61862040, No.61762059 and No.6176 2060.The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," *Symmetry*, vol. 12, no. 10, p. 1687, 2020.

[2] I. Ali, Y. Chen, N. Ullah, M. Afzal, and W. He, "Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, 2021.

[3] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey," *Vehicular Communications*, vol. 16, no. APR., pp. 45–61, 2019.

[4] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11 266–11 280, 2020.

[5] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets," *Vehicular Communications*, vol. 22, p. 100228, 2020.

[6] M. W. Dissanayake, "A novel scheme for digital signatures," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 61–72, 2019.

[7] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless

body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.

[8] J. Han, Y. Li, and W. Chen, "A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities," *Computer Standards & Interfaces*, vol. 62, pp. 84–97, 2019.

[9] C. Hu, D. Zheng, R. Guo, A. Wu, L. Wang, and S. Gao, "A novel blockchain-based anonymous handover authentication scheme in mobile networks," *International Journal of Network Security*, vol. 22, no. 5, pp. 874–884, 2020.

[10] J. Jenefa and E. M. Anita, "An enhanced secure authentication scheme for vehicular ad hoc networks without pairings," *Wireless Personal Communications*, vol. 106, no. 2, pp. 535–554, 2019.

[11] L. Kang and L. Zhang, "A privacy-preserving data sharing system with decentralized attribute-based encryption scheme," *International Journal of Network Security*, vol. 22, no. 5, pp. 815–827, 2020.

[12] J. Li, Y. Liu, Z. Zhang, B. Li, H. Liu, and J. Cheng, "Efficient id-based message authentication with enhanced privacy in wireless ad-hoc networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018, pp. 322–326.

[13] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[14] F. Liu and Q. Wang, "Ibrs: An efficient identity-based batch verification scheme for vanets based on ring signature," in *2019 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2019, pp. 1–8.

[15] Z. C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26 307–26 317, 2018.

[16] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in vanets," *Mobile Information Systems*, vol. 2019, 2019.

[17] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *International Journal of Computers Applications*, vol. 42, no. 2, pp. 196–211, 2020.

[18] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, 2019.

[19] G. Thumbur, G. S. Rao, P. V. Reddy, N. Gayathri, D. K. Reddy, and M. Padmavathamma, "Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1908–1920, 2020.

[20] G. K. Verma, B. Singh, N. Kumar, M. S. Obaidat, D. He, and H. Singh, "An efficient and provable certificate-based proxy signature scheme for iiot environment," *Information Sciences*, vol. 518, pp. 142–156, 2020.

[21] L. Wang, D. Zheng, R. Guo, C. Hu, and C. Jing, "A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks," *International Journal of Network Security*, vol. 22, no. 6, pp. 981–990, 2020.

[22] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, 2020.

[23] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven iot-based big data environment: Survey and outlook," *Journal of systems architecture*, vol. 97, pp. 185–196, 2019.

[24] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, "A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62 785–62 793, 2019.

[25] F. Wu, X. Zhang, C. Zhang, X. Chen, W. Fan, and Y. Liu, "Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8144–8156, 2020.

[26] H. Xiong, Y. Bao, X. Nie, and Y. I. Asoor, "Server-aided attribute-based signature supporting expressive access structures for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1013–1023, 2020.

[27] Z. Xu, D. He, N. Kumar, and K.-K. R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in vanets," *Security and Communication Networks*, vol. 2020, 2020.

[28] M. B. Younes, "Secure traffic efficiency control protocol for downtown vehicular networks," *International Journal of Network Security*, vol. 21, no. 3, pp. 511–521, 2019.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things.E-mail: xiepsh_lut@163.com .

Xiao-jie Pan was born in Feb. 1996. He is a master student at Lanzhou University of Technology.His major research field is network and information security. E-mail:1075224210 @qq.com.

Hong Wang was born in Oct. 1997. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2967589625 @ qq.com.

Jia-lu Wang was born in Feb. 1997. He is a master

student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1126334429 @ qq.com.

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, network and information security technology. E-mail: fengt@lut.cn .

Yan Yan was born in Oct.1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology.Her major research field is privacy protection.E-mail:yanyan@lut.cn .

Ciphertext-Policy Attribute-Based Encryption Against Post-challenge Continuous Auxiliary Inputs Leakage

Yuyan Guo, Zhenhua Lu, Mingming Jiang, and Dongbing Zhang
(Corresponding author: Zhenhua Lu)

Department of Computer Science and Technology, Huaibei Normal University
Huaibei, Anhui 235000
Email: adrienlu@163.com

(Received Aug. 21, 2021; Revised and Accepted Jan. 13, 2022; First Online Apr. 9, 2022)

Abstract

Leakage-resilient attribute-based encryption (ABE) is widely used because it not only ensures data security but also enables fine-grained access. However, most leak-resistant ABE schemes consider only continuous and auxiliary input leakage models and are not concerned with post-challenge leakage. We propose a security model for post-challenge continuous auxiliary input (pCAI) leakage by combining the post-challenge leakage model with the continuous leakage model and the auxiliary input leakage model. Moreover, we propose a CP-ABE scheme that can protect against the continuous leakage of the secret user key and masters private key and the post-challenge leakage. The security of the proposed scheme is proved under the assumption of composite order bilinear group using dual-system encryption technology. At last, the scheme is proved to be effective through performance comparison with other schemes.

Keywords: Ciphertext-Policy Attribute-Based Encryption; Dual System Encryption; Linear Secret Sharing Scheme; Post-Challenge Continuous Auxiliary Inputs Leakage

1 Introduction

Nowadays, it has become the norm for users to store important data and information in cloud servers. However, due to the different types, quantities, and importance of information stored on cloud servers, personal data will become increasingly insecure [10]. On this basis, many encryption schemes have been proposed. In 2005, the concept of attribute-based encryption (ABE) was first proposed by Sahai and Waters [21], which is a new and improved encryption scheme for identity-based encryption (IBE). The difference between ABE and IBE is that the identity in an ABE scheme is regarded as a set of attributes. However, in their scheme, the threshold parameter is set by the authorized institution, besides the access structure cannot be determined by the sender. More importantly, in practical applications, the access structure needs to be more flexible to support different attribute operations. Therefore, Goyal *et al.* [8] proposed key-policy ABE (KP-ABE), in which the ciphertext is associated with a set of attributes, and the access policy is embedded in the key. In addition, Bethencourt *et al.* [3] proposed ciphertext policy ABE (CP-ABE), in which the key and attribute set and access policy are embedded in the ciphertext. After that, many ABE solutions were proposed, such as ABE with verifiable outsourcing decryption [14], ABE data sharing scheme [1], multi-authority ABE [2,17,20], traceable ABE [19], anonymous ABE [7,27], ABE under the hash proof system [30] and hierarchical ABE [11,15].

Traditional cryptosystems are secure primarily because the keys are not exposed, however, this is an ideal assumption. In recent years, the emergence of side-channel attacks has shattered this ideal assumption. In practice, various leaked information generated during the encryption operation can be used to obtain secret information, such as secret key information. Such attacks are known as side channel attacks. Many studies have shown that there are different attack methods for side-channel attacks and some schemes are also vulnerable to attacks [2,4,6]. Therefore, the introduction of leakage-resilient encryption technology guarantees the security of the scheme. Only computation leakage model [18], bounded retrieval model [6] and other leakage models have been proposed. In these models, the key has the ability resilient to leakage and can withstand certain leakage. However, these two leakage models do not consider the continuous leakage of the keys.

After that, the emergence of the continuous leakage model can allow the key to be continuously updated [12,15,16]. The model can get the updated secret key and the updated master private key through the

key update algorithm, which further improves the leakage-resilient capability. In 2009, The concept of auxiliary input (AI) leakage model was first given by Dodis *et al.* [5], then Yuen *et al.* [25] first proposed an IBE scheme that is resilient to AI leakage and proved its security. However, The security model in above schemes only considers the leakage that occurs before the challenge phase, but does not consider the leakage after the challenge phase. Therefore, Halevi *et al.* first proposed after-the-fact disclosure and formulates the concept of entropic leakage public-key cryptography in [9], which allows leakage after the challenge ciphertext is generated. Subsequently, the post-attack auxiliary input (pAI) leakage was defined by Yuen *et al.* [26], and an IBE scheme against pAI leakage is given in [26].

1.1 Related Work

The original ABE structure can only be used for the specified threshold access strategy. Since then, in order to apply the ABE scheme to variety scenarios, linear secret sharing schemes [2], monotonic span programs (MSPs) [13], minimum sets [29] and Boolean formulas began to appear in many ABE schemes as access structures. In [23], Waters constructed a CP-ABE scheme under the assumption of concrete rather than interactive passwords, using the LSSS matrix as the access structure. Lewko *et al.* [13] used Monotonic Span Program (MSP) as the access structure to construct ABE schemes and proved that it has adaptive security in complex bilinear groups. Then Zhang *et al.* [29] propose two ABE schemes with the access structure encoded as a minimum set, Zhang *et al.* [30] proposed the attribute-based hash proof system (AB-HPS) and gave the structure of AB-HPS in the lattice. However, this scheme is not efficient because the leakage rate is related to the ciphertext and key size.

After this, many leakage-resilient ABE schemes were proposed. Later, Li *et al.* [15] propose a hierarchical ABE scheme of ciphertext strategy with continuous leakage recovery capability, the security is proved under the assumption of composite order bilinear group using dual-system encryption technology. Wang *et al.* [22] proposed for the first time a CP-ABE scheme resilient to auxiliary inputs leakage, and proved the scheme is full security. Recently, an ABE scheme was constructed under the hypothesis of truncated decision q-augmented bilinear Diffie-Hellman exponent (q-ABDHE) [28], and the scheme was proved to be CCA2 security. Ma *et al.* [17] proposed a multi-authority ABE scheme against auxiliary input leakage, Li *et al.* [16] proposed a specific KP-ABE scheme against continuous auxiliary input leakage, and proved security under static assumptions. However, none of the above ABE schemes can achieve post-challenge continuous auxiliary input (pCAI) leakage, so it is of great significance to structure a pCAI-CP-ABE scheme.

1.2 Our Motivation and Contributions

According to the above trends, there are few studies on the ABE scheme for post-challenge continuous auxiliary input (pCAI). However, the pCAI leakage model is more practical because it allows the leakage of key information after the challenge phase.

Based on the work of [16] and [22], we proposed the framework of CP-ABE, which can resilient to pCAI leakage, we also give its security model and a CP-ABE scheme against pCAI leakage. Our scheme uses the LSSS matrix as the access structure, so it has a certain degree of flexibility.

Due to the existence of the auxiliary input function, Goldreich-Levin (GL) theorem for Large Fields [5] is used for divide master private key into several parts to resist leakage attacks. In the proof phase, we use the dual-system encryption technology, which divides the key and ciphertext into two types (such as normal and semi-functional) [24]. The semi-functional key is limited to decrypting normal ciphertext, while the normal key can decrypt normal ciphertext and semi-functional ciphertext. The master private key and user key will be randomized by using master private key update algorithm and secret key update algorithm to agsinst continuous leakage. In addition, a hard-to-invert strong extractor randomizes the user key to against post-challenge leakage. Therefore, this scheme prevents stronger key leakage compared with existing schemes.

1.3 Organization

In Section 2, some preliminaries were reviewed, including the three modified static assumptions proposed in Wang's proposal. In Section 3, we propose the security model and outline of CP-ABE against pCAI leakage. In Section 4, the structure of the scheme is proposed. In Section 5, the security of the program is proven through the use of dual-system encryption. In Section 6, the scheme is compared with other well-known schemes and performance comparison is given. In Section 7, a brief conclusion is given to summarize this work.

2 Preliminaries

2.1 Composite Order Bilinear Groups

First of all, the concept of bilinear group is reviewed as follows. Let G and G_T be the multiplicative groups of order $N = p_1p_2p_3$, g is a generator of G, p_1, p_2, p_3 are three different prime. Then $e : G \times G \to G_T$ is a bilinear map and it has these properties as follows:

1) Bilinearity: For $\forall x, y \in Z_N$, $e\left(g^x, g^y\right) = e(g, g)^{xy}$.

2) Non-degeneracy: $e(g, g) \neq 1_{G_T}$.

3) Computability: There is an algorithm to calculate e efficiently.

Now we show the definition of the composite order bilinear groups. It is similar to bilinear groups except the order of the group is the product of two or more distinct prime numbers. That is to say, G is a composite order group, G_{p_1}, G_{p_2}, G_{p_3} are its three subgroups of order p_1, p_2, p_3, and g_i are the generators of subgroups G_{p_i} (i=1,2,3). Any element $g \in G$ can be shown as the form of $g_1^{x_1} g_2^{x_2} g_3^{x_3}$, where $x_i \in Z_{p_i}$. $g_1^{x_1}$, $g_2^{x_2}$ and $g_3^{x_3}$ are respectively called the terms of the subgroups G_{p_1}, G_{p_2} and G_{p_3}. For $\forall \alpha \in G_{p_i}$ and $\forall \beta \in G_{p_j}$, If $\alpha \neq \beta$,$e(\alpha, \beta) = 1$. Let $G_{p_i p_j}$ represent a subgroup of order $p_i p_j$ in G. For $\forall R \in G_{p_i p_j}$, we define R be the product of a member of G_{p_i} and a member of G_{p_j}. Similarly, $G_{p_1 p_3}$ and $G = G_{p_1 p_2 p_3}$ can be defined.

2.2 Complexity Hardness Assumptions

First, we show the original three complexity assumptions that are used in many constructs [12, 29].

Assumption 1 (1-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no Probabilistic Polynomial-Time (PPT) adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$, $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_2}$, $\Gamma_1 \in G_{p_1}$.

Assumption 2 (2-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_1 U_2, U_3, V_2 V_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_1 U_2, U_3, V_2 V_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_2}$, $\Gamma_1 \in G_{p_1}$.

Assumption 3 (BSDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, g_1^a U_2, U_3, g_1^\theta V_2, W_2, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, g_1^a U_2, U_3, g_1^\theta V_2, W_2, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$, $U_2 V_2 \in G_{p_2}$, $U_3 \in G_{p_3}$, $\Gamma_0 \in G_{p_1 p_3}$, $\Gamma_1 \in G$.

Now we give the three modified assumptions already been used in [22]. Since Wang *et al.* has already proved it, we will not prove its hardness. Let $[l]$ denote $\{1, \cdots, l\}$. **Assumption 4 (modified 1-SDP assumption).** Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_{01}\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_{11}\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

$$\vdots$$

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, U_3, \Gamma_{0l}\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, U_3, \Gamma_{1l}\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$,$U_3 \in G_{p_3}$,$\Gamma_{0i} \in G_{p_1 p_2}$,$\Gamma_{1i} \in G_{p_1}$.

Assumption 5 (modified 2-SDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(E, g_1, \left(U_{1i} U_{2i}\right)_{i \in [l]}, U_3, V_2 V_3, \Gamma_0\right) = 1\right] \\ -\Pr\left[A\left(E, g_1, \left(U_{1i} U_{2i}\right)_{i \in [l]}, U_3, V_2 V_3, \Gamma_1\right) = 1\right] \end{array} \right| \leq \varepsilon,$$

where $g_1 \in G_{p_1}$,$U_{2i}, V_2 \in G_{p_2}$,$U_3, V_3 \in G_{p_3}$,$\Gamma_0 \in G_{p_1 p_3}$,$\Gamma_1 \in G$.

Assumption 6 (modified BSDP assumption). Given $E = (N = p_1 p_2 p_3, G, G_T, e)$, no PPT adversary A has a non-negligible probability ε such that

$$\left| \begin{array}{l} \Pr\left[A\left(\begin{array}{l} E, g_1, \left(g_1^{1/\rho_i}\right)_{i \in [l]}, \left(P_i^{a_i} U_2\right)_{i \in [l]}, \\ U_3, \left(P_i^{\theta_i} V_2\right)_{i \in [l]}, W_2, \Gamma a_0 \end{array}\right) = 1\right] \\ -\Pr\left[A\left(\begin{array}{l} E, g_1, \left(g_1^{1/\rho_i}\right)_{i \in [l]}, \left(P_i^{a_i} U_2\right)_{i \in [l]}, \\ U_3, \left(P_i^{\theta_i} V_2\right)_{i \in [l]}, W_2, \Gamma_1 \end{array}\right) = 1\right] \end{array} \right| \leqslant \varepsilon,$$

where $a_i, \theta_i, \rho_i \in Z_N$, g_1,$P_i = g_1^{\rho_i} \in G_{p_1}$, $U_2, V_2, W_2 \in G_{p_2}$, $U_3 \in G_{p_3}$, $\Gamma_0 = \prod_{i=1}^{l} e(g_1, P_i)^{a_i \theta_i}$, $\Gamma_1 \in G_T$.

2.3 Linear Secret Sharing Scheme (LSSS) and Access Structure

Definition 1 (Access Structure). Assume that $\mathrm{O} = \{attr_1, \cdots, attr_n\}$ is a set of attributes, $\mathcal{A} \subset 2^O$ is a non-empty subset of 2^O, where 2^O represents the set constituted by all subsets of O, that is, $\mathcal{A}$ is a non-empty set constituted by some subsets of O, We call $\mathcal{A}$ is an access structure on O. If for any P, Q satisfy the condition $P \in \mathcal{A}$ and $P \subseteq Q$, namely $Q \in \mathcal{A}$, then the set $\mathcal{A} \subseteq O$ is monotonic. Authorized set refers to the set in $\mathcal{A}$, on the contrary, the unauthorized set is not in $\mathcal{A}$.

Definition 2 (Linear Secret Sharing Scheme). Each row of the linear secret sharing matrix formed by access policy corresponds to an attribute value, that is, row vector and attribute value form a one-to-one mapping relationship. if the following two properties are satisfied, then a secret sharing scheme Σ on a set of $O = \{attr_1, \cdots, attr_n\}$ is called linear:

1) The shared secret key for each attribute is a vector formed on Z_N.

2) In scheme Σ, there is an $n \times m$ secret sharing matrix $\boldsymbol{A}$, whose row label is $b(i)$, $i \in \{1, 2, \ldots, l\}$. Given a secret sharing column vector $u = (\tau, u_2, \cdots, u_m)$, where $\tau \in Z_N$ is the secret key to be shared, $u_2, \cdots, u_m$ is selected at random, $\boldsymbol{A}u$ represents the vector of n shared secret keys according to Σ. Shared $\gamma_i = (\boldsymbol{A}u)_i$, that is the inner product $\boldsymbol{A}u$ belongs to the property $b(i)$, where b is a function that maps $i \in \{1, 2, \ldots, l\}$ to $b(i)$.

The LSSS matrix has an important feature, that is, linear reconstruction. Suppose Σ is a LSSS scheme representing access structure A, $Q \in A$ is an authorized set, then we can define $T \subset [n]$ as $T = \{i : b(i) \in Q\}$. If there has constant $\{\beta_i \in Z_N\}_{i \in T}$ that can be found in polynomial time such that $\{\gamma_i\}$ are valid shares of the secret key τ, then we have $\sum_{i \in T} \beta_i \gamma_i = \tau$. There is no such constant for any unauthorized set.

2.4 GL Theorem for Large Fields

Let q be a large prime and H be any subset of $GF(q)$, n be a positive integer. Let $h : H^n \to \{0,1\}^*$ be any function. Then choose random a vector $w \leftarrow GF(q)^n$, and randomly picks $u \leftarrow H^n$, compute $v \leftarrow h(u)$. If there exists a PPT distinguisher D runs in time δ such that

$$\left| \begin{array}{l} \Pr\left[D\left(v, w, \langle w, u \rangle\right) = 1\right] - \\ \Pr\left[z \leftarrow GF(q) : D\left(v, w, z\right) = 1\right] \end{array} \right| = \varepsilon,$$

Then exists an inverter A that runs in time $\delta' = \delta \cdot poly(n, |H|, 1/\varepsilon)$ such that

$$\Pr\left[u \leftarrow H^n, v \leftarrow f(u) : A(v) = u\right] \geqslant \frac{\varepsilon^3}{512nq^2}$$

3 CP-ABE with Post-challenge Continual Auxiliary Inputs

3.1 The Outline of CP-ABE

In our pCAI-CP-ABE, suppose $\mathcal{A}$ is a monotone access structure, Ω is a monotone attribute universe space. we define the security model of CP-ABE against post-challenge continual auxiliary inputs (pCAI-CP-ABE). First of all, we give the composition structure of CP-ABE, which is consisted of the following algorithms.

Setup $(1^k, \Omega)$***:*** This algorithm takes security parameter k and Ω as inputs, then it generates the public key *MPK* and master private key *MSK*.

KeyGen(*MSK*,$\mathbf{S}$***):*** Inputs the *MSK* and an attribute collection $\mathbf{S}$ of a user. It generates a secret key $SK_{\mathbf{S}}$.

Enc(*M*,$\mathcal{A}$***):*** Inputs a access structure $\mathcal{A}$ and a message *M*. It generates a ciphertext *C*.

Dec(*C*,$SK_{\mathbf{S}}$***):*** This algorithm takes *C* and $SK_{\mathbf{S}}$ as inputs, then it outputs *M* while $\mathbf{S}$ satisfies $\mathcal{A}$.

MSK-Update(*MPK*,*MSK* ***):*** Inputs *MPK* and *MSK*. It generates a new updated master private key MSK', where $|MSK| = |MSK'|$.

SK-Update(*MPK*,$SK_{\mathbf{S}}$***):*** Inputs *MPK* and $SK_{\mathbf{S}}$. It generates a new updated secret key $SK'_{\mathbf{S}}$, where $|SK_{\mathbf{S}}| = |SK'_{\mathbf{S}}|$.

3.2 Security Model of pCAI-CP-ABE

Based on [22], the security model of pCAI-CP-ABE is given. Let H_1 and H_2 be the polynomial-time computable function family, $\mathcal{A}^*$ is the challenge access structure. The security model of CP-ABE against the pCAI leakage model is defined by an indistinguishable game between adversary A and challenge B. A sends H_1 and H_1 to the challenge B. First, B define three lists L_{MSK}, $L_{SK} = (cnt, SK_{\mathbf{S}}, \mathbf{S})$, $L_{SK'} = (cnt', SK'_{\mathbf{S}}, \mathbf{S})$, where *cnt* and cnt' are two different counters and L_{MSK}, L_{SK} and $L_{SK'}$ are all empty at the beginning.

Setup. The Setup algorithm is first run by challenger B to generate *MPK* and *MSK*, and *MPK* is output to A.

Phase 1. A can issue the following query adaptively:

Secret Key Query: First takes an attribute set $\mathbf{S} \subset \Omega$ as input, B check the tuple L_{SK} with the form $(cnt, SK_{\mathbf{S}}, \mathbf{S})$. if there does not exist such tuple, KeyGen(MPK,MSK) is run by B to generate secret key SK_S and lets $cnt = 1$. Then, B adds $(cnt, SK_{\mathbf{S}}, \mathbf{S})$ to L_{SK}. Otherwise, it returns $SK_{\mathbf{S}}$ from the tuple $(cnt, SK_{\mathbf{S}}, \mathbf{S})$ and lets $cnt = cnt + 1$.

Pre-challenge Leakage Query: Input $h_i \in H_1$, then B returns $h_i(L_{MSK}, MSK, SK_{\mathbf{S}}, MPK, L_{SK}, \mathbf{S})$ to A.

MSK-Update Query: B first runs MSK-Update algorithm to get MSK', it then puts the MSK' into the L_{MSK}.

SK-Update Query: B first check the tuple with the form $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$, if there does not exist such tuple then let $cnt' = 1$, and B runs *SK-Update* algorithm to get $SK'_{\mathbf{S}}$, it then puts the $SK'_{\mathbf{S}}$ into the $L_{SK'}$. Otherwise, B return $SK'_{\mathbf{S}}$ from $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$ and let $cnt' = cnt' + 1$.

Challenge. First, two messages of equal length M_0 and M_1 are submitted by A, then A outputs $\mathcal{A}^*$, where any $\mathbf{S}$ does not satisfy $\mathcal{A}^*$. B samples a random bit $b \in \{0,1\}$, the ciphertext C^* is outputs to A.

Phase 2. A can issue the following query adaptively:

Secret Key Query: This query is same as the phase 1, but the attribute set that satisfies $\mathcal{A}^*$ cannot be queried by A.

Post-challenge Leakage Query: Input $h'_{i'} \in H_2$, then B samples the randomness of encryption $r' \in \{0,1\}^*$ and returns $h'_{i'}(r')$.

Guess. A submits a guess b' of b, thus we can define the advantage of A is $Adv_A^{pCAI-CPA}(\Omega) = |2\Pr[b = b] - 1|$.

A CP-ABE scheme is pCAI-CPA secure in the pCAI leakage model for H_1 and H_2 if there is no PPT adversary A with non-negligible advantage in the above game.

Auxiliary Functions. We give the definition of two families of functions H_1 and H_2. They are regarded as one-way families of $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ functions, respectively. And we will give the definitions of $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ later.

Let W^* represents the set of all private keys satisfying the challenge access $\mathcal{A}^*$, and W represents the set of q_s private keys such that $W \cap W^* = \emptyset$, where q_s represents the total number of times A made Secret Key Query. In order to facilitate, let $H_{ow}(f(k_e))$ and $H_{\mathcal{A}^*-ow}(f(k_e))$ are parameterized by the min-entropy k_e of the attribute secret key, where k_e is the length of key while key is random generated.

$H_{\mathcal{A}^*\text{-}ow}(f(k_e))$: The class of all polynomial time computable function, all $i \in [1, q_{pre}]$ (where q_{pre} is the total number of times A made Pre-challenge Leakage Query.) and given

$$\{MPK, \mathcal{A}^*, W, \{h_i(MSK, L_{SK'}, MPK, \mathbf{S})\}_{i\in[q_{pre}]}\},$$

where all $h_i \in H_{\mathcal{A}^*-ow}(g(k_e))$. In this case, there is no PPT algorithm can find $SK_{\mathbf{S}^*}$ with a probability greater than $f(k_e)$, where $f(k_e) \geq 2^{-k_e}$ is the hardness parameter. Hence, we have $\{h_i\}_{i\in[q_{pre}]} \subseteq H_{\mathcal{A}^*-ow}(f(k_e))$.

$H_{ow}(f(k_e))$: The class of all polynomial time computable function $h'_{i'} : \{0,1\}^* \to \{0,1\}^*$, all $i' \in [1, q_{post}]$ (where q_{post} is the total number of times A made Post-challenge Leakage Query.) and given $h'_{i'}(r')$, where all $h'_{i'} \in H_{ow}(g(k_e))$. In this case, there is no PPT algorithm can find $SK_{\mathbf{S}^*}$ with a probability greater than $f(k_e)$, where $f(k_e) \geq 2^{-k_e}$ is the hardness parameter. Hence, we have $\{h'_{i'}\}_{i\in[q_{post}]} \subseteq H_{ow}(f(k_e))$.

Definition 3 (pCAI-CPA-CP-ABE). A CP-ABE scheme is said to be $f(k_e)$-pCAI-CPA secure, if the CP-ABE scheme is CPA secure with respect to the families $(H_{ow}(f(k_e)), H_{\mathcal{A}^*-ow}(f(k_e)))$.

3.3 Strong Extractor with Hard-to-invert Auxiliary Inputs

Definition 4. Let $Ext{:}\{0,1\}^{l_1} \times \{0,1\}^{l_2} \to \{0,1\}^n$, l_1, l_2, $n \in Z_N$. If for any PPT adversary A we have that

$$\left| \begin{array}{l} \Pr\left[A\left(r, h'_{i'}(\sigma), Ext(r,\sigma)\right) = 1\right] \\ -\Pr\left[A\left(r, h'_{i'}(\sigma), \theta\right) = 1\right] \end{array} \right| < \varepsilon,$$

Ext is said to be a strong extractor with $(\varepsilon, f(k_e))$-hard-to-invert auxiliary inputs, where $0 < \varepsilon < 1$, $r \in \{0,1\}^{l_1}$, $\sigma \in \{0,1\}^{l_2}$, $\theta \in \{0,1\}^n$, $h'_{i'} \in H_{ow}(g(k_e))$, $g(k_e) \geq 2^{-k_e}$ and $i' \in [1, q_{post}]$.

Lemma 1. Let $r \in \{0,1\}^{l_1}$ be chosen uniformly random, For all $\sigma \in \{0,1\}^{l_2}$ and $h'_{i'} \in H_{ow}(g(k_e))$, given $(r, h'_{i'}(\sigma), Ext(r,\sigma))$, if no PPT adversary A has a non-negligible probability ε to find σ, then $Ext(r,\sigma)$ is a strong extractor with $(\varepsilon, f(k_e))$-hard-to-invert auxiliary inputs.

4 Construction

First each attribute is converted into a random number belonging to Z_N, where $N = p_1p_2p_3$ and p_1, p_2, p_3 are three different prime numbers, Π is a monotone universal attribute space. Then we define an injection map I_M, and for $\forall S_i \in \Pi$, we have $I_M(S_i) \in Z_N$. Then let $\Omega = I_M(\Pi)$ is a subset of Z_N and $I = |\Omega|$ denotes the cardinality of Ω, A is a monotone access structure.

Setup$(1^k, \Omega)$: Input the security parameter k, a monotone universal attribute space Ω. Then, the algorithm runs the bilinear group generator to produce $E = (N = p_1p_2p_3, G, G_T, e)$. Then, it randomly chooses generator $g_1, x_1, \cdots, x_I \in G_{p_1}$ and $g_3 \in G_{p_3}$. Let $l = (3\gamma)^{1/\varepsilon}$, where the security is with reference to 2^{-l^ε}-hard-to-invert auxiliary inputs. Then, it chooses random $\alpha, a_1, \cdots, a_l, \rho_1, \cdots, \rho_l \in Z_N$, $v_1, \cdots, v_l \in Z_{p_3}$ and $P_1 = g_1^{\rho_1}, \cdots, P_l = g_1^{\rho_l}$. Let $\sigma \in \{0,1\}^{l_2}$ and $Ext{:}\{0,1\}^{l_1} \times \{0,1\}^{l_2} \to \{0,1\}^n$, $l_1, l_2, n \in Z_N$, where the *Ext* is a strong extractor. Then, it outputs master public key is $MPK{=}\{E, g_1, g_3, (g_1^{\alpha/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}, \sigma\}$ and master private key is $MSK{=}(g_1^{a_i} \cdot g_3^{v_i}.)_{i\in[l]}$.

KeyGen$(MPK, MSK, \mathbf{S})$: Takes *MPK*, *MSK* and an attribute set $\mathbf{S}$ as input. Then it picks $y_{1,1}, \cdots, y_{1,l}, y_2, y_{3,1}, \cdots, y_{3,I}, t \in Z_N$ and outputs the secret key $SK_{\mathbf{S}} = \{(sk_{1,i})_{i\in[l]}, sk_2, (sk_{3,h})_{h\in\mathbf{S}}\} = \{(g_1^{a_i} \cdot g_1^{\alpha t/\rho_i} \cdot g_3^{y_{1,i}} \cdot g_3^{v_i})_{i\in[l]}, g_1^t \cdot g_3^{y_2}, (x_h^t \cdot g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$.

Enc(M, Π, MPK): Inputs a LSSS scheme $\Sigma = (\boldsymbol{A}, b)$ for $\mathcal{A}$, *MPK* and a message *M*. Note that $\boldsymbol{A}$ is an $n \times m$ matrix. The function b maps the i-th row of A to an attribute vector $u(i)$. The algorithm chooses random $q_1, \cdots, q_n \in Z_N, r_i \in \{0,1\}^{l_1}$ and computes $\theta_i = Ext(r_i, \sigma)$, it randomly chooses a vector $u = (\sum_{i=1}^{l} \theta_i, u_2, \cdots, u_m) \in Z_N^m$. For i to 1, it computes $\gamma_i = \boldsymbol{u} \cdot \boldsymbol{A}_i$, where $\boldsymbol{A}_i$ is i-th row vector of $\boldsymbol{A}$. It creates the ciphertext $C = \{c_1 = M \cdot \prod_{i=1}^{l} y_i^{\theta_i}, (c_{2,i} = P_i^{\theta_i})_{i\in[l]}, (c_{3,i} = g_1^{\alpha\gamma_i} \cdot x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$.

Dec$(C, SK_{\mathbf{S}}, MPK)$: The algorithm inputs the ciphertext C of the LSSS scheme Σ on $\mathcal{A}$, the secret key of set $\mathbf{S}$ and *MPK*. Then let $T \subset [n]$ be defined as $T = \{i : b(i) \in \mathbf{S}\}$ while $\mathbf{S} \in \mathcal{A}$ is an authorized set.If $\{\gamma_i\}$ are valid shares of A, then the algorithm can compute a set $\{\beta_i \in Z_N\}_{i\in T}$ make $\sum_{i\in T} \beta_i\gamma_i = \sum_{i=1}^{l} \theta_i$. Finally, it calculates:

$$\frac{\prod_{i=1}^{l} e(c_{2,i}, sk_{1,i})}{\prod_{i\in T} \left(e(c_{3,i}, sk_2)e(c_{4,i}, sk_{3,b(i)})\right)^{\beta_i}} = \prod_{i=1}^{l} y_i^{\theta_i}.$$

MSK-Update(MPK,MSK): The algorithm inputs MSP, then it picks $v'_i \in Z_N$, the updated master private key $MSK' = MSK \cdot g_3^{v'_i}$.

SK-Update(MPK, $SK'_{\mathbf{S}}$): The algorithm inputs $SK_{\mathbf{S}}$, then it picks random $y'_{1,1}, \cdots, y'_{1,l}, y'_2, y'_{3,1}, \cdots, y'_{3,I}, t' \in Z_N$ and computes $sk_{1,i} = (sk_{1,i} \cdot g_1^{\alpha t'/\rho_i} \cdot g_3^{y'_{1,i}})_{i\in[l]}$, $sk'_2 = sk_2 \cdot g_1^{t'} \cdot g_3^{y'_2}$, $sk'_{3,i} = (sk_{3,i} \cdot x_h^{t'} \cdot g_3^{y'_{3,h}})_{h\in\mathbf{S}}$. Final, the updated secret key $SK'_{\mathbf{S}} = \{(sk'_{1,i})_{i\in[l]}, sk'_2, (sk'_{3,h})_{h\in\mathbf{S}}\}$.

Correctness: The correctness of the equation is verified on the next page.

5 Security Proof

We use the dual system encryption mechanism to proof the security, first of all, three semi-functional (SF) structures are defined, note that g_2 is the generator of G_{p_2}.

SF master private key: $(g_1^{a_i} \cdot g_2^{\varphi_i} \cdot g_3^{v_i})_{i\in[l]}, \varphi_1, \cdots, \varphi_l \in Z_N$.

SF attribute-based secret key: $\{(g_1^{a_i+\alpha t/\rho_i} \cdot g_2^{d_i} g_3^{y_{1,i}})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in S}\}, z, d_1, \cdots, d_l, \in Z_N$.

SF ciphertext: $\{c_1 = M \cdot \prod_{i=1}^m y_i^{\theta_i}, (c_{2,i} = P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (c_{3,i} = g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i} g_2^{\omega_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}, \eta_1, \cdots, \eta_l, \omega_1, \cdots, \omega_l \in Z_N$.

According to the dual system encryption, a normal secret key can decrypt SF ciphertext, and normal ciphertext can be decrypted with SF attribute-based key. If a SF attributed-based secret key is used to decrypt a SF ciphertext, we have $e(g_2, g_2)^{\sum_{i=1}^l \eta_i d_i - z\sum_{i\in T}\omega_i\beta_i}$. If $\sum_{i=1}^l \eta_i d_i = z\sum_{i\in T}\omega_i\beta_i$, decryption will succeed, and we call a SF attribute-based secret key is a nominally SF attributed-based secret key. In the same way, the attribute-based generated by a SF master private key is also SF attributed-based secret key, then we have $e(g_2, g_2)^{\sum_{i=1}^m \eta_i\varphi_i - z\sum_{i\in T}\omega_i\beta_i}$. If $\sum_{i=1}^l \eta_i\varphi_i = z\sum_{i\in T}\sigma_i\beta_i$, then decryption will succeed and the corresponding attributed-based secret key is nominally SF attributed-based secret key.

Theorem 1. *If the modified assumptions 1, 2 and 3 holds, Our CP-ABE scheme is* (2^{-l^ε})*-pCAI-CPA leakage secure.*

Proof. A series of indistinguishable games are defined to prove the theorem, $\mathcal{A}^*$ is the monotone challenge access structure.

$Game_{real}$: $Game_{real}$: is the first real, and keys and ciphertexts are normal.

$Game_{restrained}$: The difference between $Game_{restrained}$ and $Game_{real}$ is that in $Game_{restrained}$ the adversary can't ask for any attribute set in $\mathcal{A}^*$.

$Game_j$: The $Game_j$ is similar to $Game_{restrained}$, but the ciphertext for the adversary is SF. Then we defined two types attribute-based secret keys:

TypeI:$\{(g_1^{a_i+\alpha t/\rho_i} g_2^{d_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,x}})_{x\in\mathbf{S}}\}$

TypeII:$\{(g_1^{a_i+\alpha t/\rho_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_2^z g_3^{y_2}, (x_h^t g_3^{y_{3,x}})_{x\in\mathbf{S}}\}$

For $j = 1, \cdots, q-1$ in $Game_k$, the first $j-1$ keys are SF of typeII, the j-th key is SF of typeI, and the rest keys are normal. Thus, in $Game_q$, all keys are SF of typeII. We note that the ciphertext is SF in $Game_0$, but all keys are normal. And in $Game_q$ all keys and ciphertexts are SF.

$Game_{final}$: It is similar to $Game_q$, but the message is not M_0 and M_1, but is blinded with a random value in G_T. □

Lemma 1. Suppose there is an adversary A such that $Adv_A^{Game_{real}} - Adv_A^{Game_{real2}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the Assumption 2.

Proof. $\mathcal{A}^*$ is the challenge monotone access structure. For $S^* = \{S_1^*, \cdots, S_n^*\} \in A^*$, where S^* has n attributes. Then, let $\mathcal{S}^* = \{\mathcal{S}'_1 | \mathcal{S}'_1 = S_1 \bmod p_2\} \bigcup \cdots \bigcup \{S'_n | S'_n = S_n \bmod p_2\}$ and Φ^* be the set of all $\mathcal{S}^*$, where $\mathcal{S}^*$ is a superset of S^*.

If adversary A wants to make key query on $\Omega^* \notin \mathcal{A}^*$, for $\forall S'_i \in \Omega^*$, the B's answer is as follows:

1) If $S'_i \notin \mathcal{S}^*$, for $\forall \mathcal{S}^* \in \Phi^*$. In this case, C runs the KeyGen and uses MSK as responses.

2) If $S'_i \in \mathcal{S}^*$, for $\exists \mathcal{S}^* \in \Phi^*$. Then we have $S'_i \neq S_i$ and $S'_i = S_i \bmod p_2$, C will computes $\alpha = \gcd(S_i - S'_i, N)$, then we can define $\beta = N/\alpha$, where $N = p_1p_2p_3$. Finally, we can get a tuple $(g, U_1U_2, U_3, V_2V_3, \Gamma)$, note that it is an example of the 2-SDP assumption.

   a. If $\alpha = p_1p_2$ and $\beta = p_3$, then B will verify whether $\alpha = p_1p_2$ from $(U_1U_2)^\alpha = 1$. If the equation is satisfied, B will continue to verify $e(U_2U_3, \Gamma)^{\beta \stackrel{?}{=} 1}$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$;

   b. If $\alpha = p_2p_3$ and $\beta = p_1$, then B will verify whether $\alpha = p_2p_3$ from $(V_2V_3)^\alpha = 1$. If the equation is satisfied, B will continue to verify $e(U_1U_2, \Gamma)^{\beta \stackrel{?}{=} 1}$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$;

   c. If $\alpha = p_2$ and $\beta = p_1p_3$, B will continue to verify $\Gamma^{\beta \stackrel{?}{=} 1}$ to distinguish between $\Gamma \in G_{p_1p_3}$ and $\Gamma \in G$.

□

Lemma 2. Suppose there is an adversary A such that $Adv_A^{Game_{restrained}} - Adv_A^{Game_{real0}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified 1-SDP Assumption.

Proof. Input a tuple $(N, g_1, U_3, G, G_T, (\Gamma_i)_{i\in[l]})$, which is an example of the modified 1-SDP assumption.

Setup. B constructs MPK=$\{g_1, U_3, (g_1^{\alpha t/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}\}$,$MSK$=$(g_1^{a_i} U_3^{v_i})_{i\in[l]}$,

$$\frac{\prod_{i=1}^{l} e(c_{2,i}, sk'_{1,i})}{\prod_{i\in T}\left(e(c_{3,i}, sk'_2)\cdot e(c_{4,i}, sk'_{3,b(i)})\right)^{\beta_i}} = \frac{\prod_{i=1}^{l} e(P_i^{\theta_i}, g_1^{a_i} g_1^{\alpha t/\rho_i} g_3^{y_{1,i}} g_3^{v_i} \cdot g_1^{\alpha t'/\rho_i} g_3^{y'_{1,i}})}{\prod_{i\in T}\left(e(g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i}, g_1^t g_3^{y_2}\cdot g_1^{t'} g_3^{y'_2})\cdot e(g_1^{q_i}, x_{b(i)}^t g_3^{y_{3,b(i)}} x_{b(i)}^{t'} g_3^{y'_{3,b(i)}})\right)^{\beta_i}}$$

$$= \frac{(\prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i})\cdot e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}}{\prod_{i\in T}\left(e(g_1^{\alpha\gamma_i}, g_1^t)\cdot e(g_1^{\alpha\gamma_i}, g_1^{t'})\cdot e(x_{b(i)}^{-q_i}, g_1^t)\cdot e(x_{b(i)}^{-q_i}, g_1^{t'})\cdot e(g_1^{q_i}, x_{b(i)}^t)\cdot e(g_1^{q_i}, x_{b(i)}^{t'})\right)^{\beta_i}}$$

$$= \frac{(\prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i})\cdot e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}}{e(g_1,g_1)^{\alpha t\cdot\sum_{i=1}^{l}\theta_i}\cdot e(g_1,g_1)^{\alpha t'\cdot\sum_{i=1}^{l}\theta_i}} = \prod_{i=1}^{l} e(P_i, g_1)^{a_i\theta_i} = \prod_{i=1}^{l} {y_i}^{\theta_i}$$

$a, \alpha_i, \rho_i \in Z_N$. Then, B send MPK to A.

Phase 1. A can issue the Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, and B will answer respectively.

Challenge. Two messages M_0 and M_1 with the same length and $\mathcal{A}^*$ are sent by A to B, then B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n$, $q_1, \cdots, q_n \in Z_N$ and outputs $C^* = \{c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, \Gamma_i), c_{2,i} = (\Gamma_i)_{i\in[l]}, (c_{3,i} = \Gamma_i^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$ to A.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, and B will answer respectively.

1) If $\Gamma_i = g_1^{\rho_i\theta_i} g_2^{z_i} \in G_{p_1p_2}$, then $C^* = \{M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, P_i^{\theta_i}), (P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (g_1^{\alpha\gamma_i} g_2^{\omega_i} x_{b(i)}^{-q_i}, g_1^{q_i})_{i\in[n]}\}$, where $\omega_i = ac_i \cdot \tilde{\gamma}_i$, η_i=ci, $\gamma_i = \rho_i \cdot \theta_i \cdot \tilde{\gamma}_i$ and C^* is a SF ciphertext. Hence B can simulate $Game_0$.

2) If $\Gamma_i \in G_{p_1}$, then C^* is normal. Hence an normal ciphertext game $Game_{restrained}$ can be simulated by B.

Thus, if A can distinguish between $Game_0$ and $Game_{restrained}$ with a non-negligible advantage ε, then B can break the modified 1-SDP Assumption with non-negligible advantage. □

Lemma 3. Suppose there is an adversary A such that $Adv_A^{Game_{j+1}} - Adv_A^{Game_j} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified 2-SDP Assumption.

Proof. Input a tuple $(g_1, (U_{1i}U_{2i})_{i\in[m]}, U_3, V_2V_3, \Gamma)$, which is an example of the modified 2-SDP assumption.

Setup. B constructs $MPK = \{E, g_1, g_2, (g_1^{\alpha t/\rho_i})_{i\in[l]}, P_1, \cdots, P_l, x_1, \cdots, x_I, (y_i = e(g_1, P_i)^{a_i})_{i\in[l]}\}$ and $MSK = (g_1^{a_i} g_3^{v_i})_{i\in[l]}$. Then, B send the MPK to A.

Phase 1. A can issue kth Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B, where $k \in N$.

- **Key Query:**

  If $k < j$, where $k \in [0, q]$, B answers with $\{(g_1^{a_i+\alpha t/\rho_i} g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t (V_2V_3)^x g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$, which is a typeII SF key.

  If $k = j$, then There are two different situations:

  1) B answers with $\{(g_1^{a_i} \cdot \Gamma^{\alpha} \cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, \Gamma \cdot g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$. If $\Gamma = g_1^a g_2^b g_3^c \in G$, the j-th is a typeI SF. If $\Gamma = g_1^a g_3^c \in G_{p_1p_3}$, the j-th key is normal.
  2) B answers with $\{(g_1^{a_i} \cdot \Gamma^{\alpha} \cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, \Gamma \cdot g_3^{y_2}(V_2V_3)^x, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$. If $\Gamma = g_1^a g_2^b g_3^c \in G$, the j-th is a typeI SF key. If $\Gamma = g_1^a g_3^c \in G_{p_1p_3}$, the j-th key is a typeII SF key.

  If $k > j$, then B will answer with normal keys.

- **Pre-challenge Leakage Query:** A issue the Pre-challenge Leakage Query, B returns $h_i(MSK, L_{MSK}, MPK, L_{SK}, \mathbf{S})$.

- **MSK-Update Query and SK-Update Query:**

  B answers the MSK-Update Query from A with MSK-Update algorithm, B returns MSK' and adds $(MSK', \cdot)$ to L_{MSK}, where MSK' is a SF key.

  B answers the SK-Update Query from A with SK-Update algorithm, B returns $SK'_{\mathbf{S}}$ and update cnt', then adds $(cnt', SK'_{\mathbf{S}}, \mathbf{S})$ to $L_{SK'}$, where $SK'_{\mathbf{S}}$ is a typeII SF key.

Challenge. B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n \in Z_N$, then it outputs the ciphertext $C = \{c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, U_{1i}U_{2i}), c_{2,i} = (U_{1i}U_{2i})_{i\in[l]}, (c_{3,i} = U_{1i}U_{2i}{}^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$ to A.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query to B, where Key Query are simulated as before. If we let $U_{1i}U_{2i} = g_1^{\rho_i\theta_i} g_2^{z_i}$, then we have that $c_1 = M_b \cdot \prod_{i=1}^{l} e(g_1^{a_i}, B_i^{\theta_i})$, $c_{2,i} = (B_i^{\theta_i} g_2^{\varphi_i})_{i\in[l]}$,$(c_{3,i} = g_1^{\alpha\gamma_i} g_2^{\omega_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}$, where $\omega_i = ac_i \cdot \tilde{\gamma}_i$, $\gamma_i = \rho_i \cdot \theta_i \cdot \tilde{\gamma}_i$, $\eta_i = ci$. Note that this is a SF ciphertext.

In conclusion, if $\Gamma \in G$, B simulates $Game_{j+1}$ correctly. If $\Gamma \in G_{p_1p_3}$, then B simulates $Game_j$ correctly. Thus, if A can distinguish between $Game_{j+1}$ and $Game_j$ with a non-negligible advantage ε, then B can break the

Table 1: Performance comparison with other schemes

Schemes	Ciphertext size	Secret key size	Encrypt cost	Decrypt cost
[12]	$(\tilde{k}+2l+1)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(3l+\tilde{k}+1)Ep+Ep_T$	$(2n+\tilde{k}+1)Pa$
[15]	$(\tilde{k}+3l+1)\|G\|+\|G_T\|$	$3(\tilde{k}+l+2+\|S\|)\|G\|$	$(3l+\tilde{k}+\tilde{p}l+1)Ep+Ep_T$	$(3n+\tilde{k}+1)Pa$
[27]	$(\tilde{k}+2l+2)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(3l+\tilde{k}+1)Ep+Ep_T$	$(2n+\tilde{k}+1)Pa$
[29]	$(\tilde{k}+2\tilde{m}+1)\|G\|+\|G_T\|$	$(\tilde{k}+2+\|S\|)\|G\|$	$(2\tilde{m}+\tilde{k}+2)Ep+Ep_T$	$(\tilde{k}+3)Pa$
ours	$(2n+l)\|G\|+\|G_T\|$	$(l+1+\|S\|)\|G\|$	$(2n+l)Ep+lEp_T$	$(2n+l)Pa$

modified 2-SDP Assumption with non-negligible advantage. □

Lemma 4. Suppose there is an adversary A such that $Adv_A^{Game_q} - Adv_A^{Game_{final}} \geq \varepsilon$, then there is an algorithm B that has advantage to break the modified BSDP Assumption.

Proof. Input a tuple $(g_1, (g_1^{1/\rho_i})_{i\in[l]}, (P_i^{a_i}U_2)_{i\in[m]}, U_3, (P_i^{a_i}V_2)_{i\in[m]}, W_2, \Gamma)$, which is an example of the modified BSDP assumption.

Setup. B sets $g_3 = U_3$, $g_2 = W_2$, $y_i = e(g_1, P_i^{a_i}U_2) = e(g_1, P_i)^{a_i}$, then constructs the MPK and the MSK=$(P_i^{a_i}U_2 g_3^{v_i})_{i\in[l]}$.

Phase 1. A can perform the Secret Key Query, Pre-challenge Leakage Query, MSK-Update Query and SK-Update Query to B.

For all queries of Key Query, B answers as $SK_{\mathbf{S}} = \{(sk_{1,i})_{i\in[l]}, sk_2, (sk_{3,h})_{h\in\mathbf{S}}\} = \{((P_i^{a_i}U_2)\cdot g_1^{\alpha t/\rho_i}\cdot g_3^{y_{1,i}+v_i})_{i\in[l]}, g_1^t g_3^{y_2}, (x_h^t g_3^{y_{3,h}})_{h\in\mathbf{S}}\}$.

Challenge. B picks random $\tilde{\gamma}_1, \cdots, \tilde{\gamma}_n, q_1, \cdots, q_n \in Z_N$, then it returns $C^* = \{c_1 = M_b \cdot \Gamma, c_{2,i} = (P_i^{\theta_i}V_2)_{i\in[l]}, (c_{3,i} = (P_i^{\theta_i}V_2)^{\alpha\tilde{\gamma}_i} x_{b(i)}^{-q_i}, c_{4,i} = g_1^{q_i})_{i\in[n]}\}$.

Phase 2. A can perform the Secret Key Query, Post-challenge Leakage Query to B.

1) If we let $P_i^{\theta_i}V_2 = P_i^{\theta_i} g_2^{z_i}$, $C^* = \{c_1, c_{2,i}, c_{3,i}, c_{4,i}\} = \{M_b\cdot\Gamma, (P_i^{\theta_i} g_2^{\eta_i})_{i\in[l]}, (g_1^{\alpha\gamma_i} x_{b(i)}^{-q_i} g_2^{\omega_i}, g_1^{q_i})_{i\in[n]}\}$, where $\omega_i = ac_i\cdot\tilde{\gamma}_i, \eta_i = ci, \gamma_i = \rho_i\cdot\theta_i\cdot\tilde{\gamma}_i$.
2) If $\Gamma = \prod_{i=1}^m e(g_1, P_i)^{a_i\theta_i}$, then C^* is SF, B simulates $Game_q$ correctly.
3) If $\Gamma \in G_T$ is a random value, B simulates $Game_{final}$ correctly. In conclusion, if A can distinguish between $Game_q$ and $Game_{final}$ with a non-negligible advantage ε, then B can break the modified BSDP Assumption with non-negligible advantage.

□

6 Performance Comparison

The performance of other related scheme [12,15,27,29] is compared with this scheme in this section. Let Ep and Ep_T denote exponential operation in G and G_T, Pa denotes pairing operation. $|G|$ and $|G_T|$ respectively denotes the length of G and G_T, $|S|$ is the number of elements in S. For convenience, let $\tilde{m}$ denotes the number of minimal sets, let the LSSS matrix with l rows and n columns, $\tilde{k}$ denotes the leakage parameter and $\tilde{p}$ denotes the number of elements in attribute vectors. Table 1 shows the efficiency analysis and comparison of each scheme.

From the data in Table 1, the leakage parameter is the decisive factor in the performance efficiency of the scheme [12, 15, 27, 29], that is, the size of the leakage parameter determines whether the scheme is efficient. However, our scheme is independent of the leakage parameters, but only depends on the scale of the LSSS matrix.

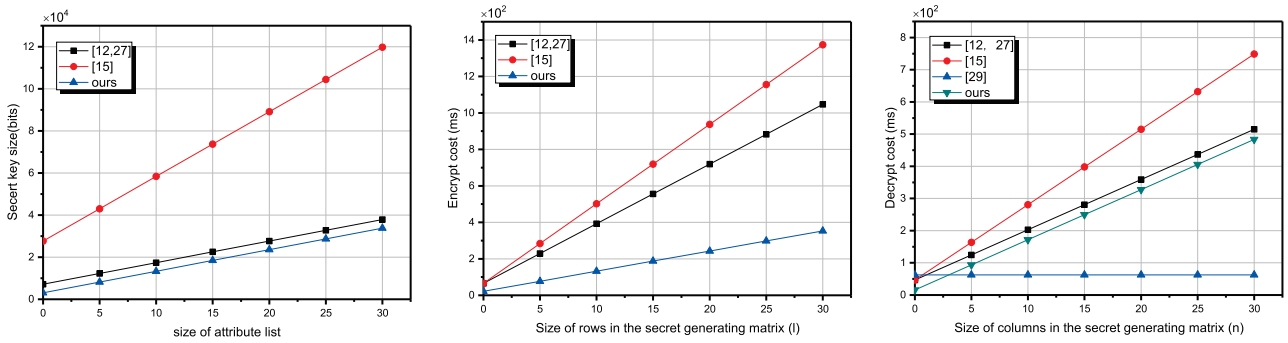
We use JPBC library version 2.0.0 for related experiments. The experiment was simulated on Windows system with an Intel(R) Core (TM) i5 CPU 3.20GHz and 8.00GB RAM to approximate the actual operation. We have obtained the measured values of exponentiation and pairing operations. The operating times of Ep, Ep_T and Pa are 10.9ms, 7.8ms and 0.15ms, respectively.

According to the above data, in order to achieve better leakage-resilient performance, We set N to be a 1024-bit number in the scheme [12, 15, 27, 29], we let $n = 1$ and $l = 2$ in the simulation of encrypt cost and decrypt cost respectively. Figure 1 shows the running time of different algorithms in these schemes.

Obviously, our scheme is more effective than [12,15,27, 29]. The efficiency of the scheme [15] is related to both the leakage parameters and the LSSS matrix. Although the minimum set used in [29] can improve the decryption time, LSSS is more flexible and can be applied in a variety of scenarios. What's more, our scheme is not affected by the leakage parameters. Therefore, from the above analysis, our scheme has certain advantages.

7 Conclusion

We propose an ABE scheme which resilient to post-challenge continuous auxiliary input leakage, and proved that the scheme is secure under the three modified static assumptions. Our scheme can tolerate auxiliary input and continuous leakage. In addition, if there is an adversary who can query the secret key information after the



(a) Secret key size (b) Encrypt time (c) Decrypt time

Figure 1: Efficiency comparison

challenge phase, our solution can tolerate post-challenge leakage. It may be even more interesting to construct certain KP-ABE schemes that can against pCAI.

Acknowledgments

This paper is supported by the National Natural Science Foundation of China under Grant No. 61902140, the Anhui Provincial Natural Science Foundation under Grant No. 1908085QF288, the Nature Science Foundation of Anhui Higher Education Institutions under Grant No.KJ2021A0527, No.KJ2019A0605, No.KJ2020A0032, No. KJ2020A0034.

References

[1] M. Bayat, M. Doostari, and S. Rezaei, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.

[2] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP)*, pp. 321–334, Berkeley, CA, USA, 2007.

[4] Z. Cao, L. Liu, and Z. Guo, "Ruminations on attribute-based encryption," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 9–19, 2018.

[5] Y. Dodis, S. Goldwasser, Y. T. Kalai, and C. Peikert, "Public-key encryption schemes with auxiliary inputs," in *Theory of Cryptography Conference (TCC)*, pp. 361–381, Zurich, Switzerland, 2010.

[6] A. Faonio, J. B. Nielsen, and D. Venturi, "Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model," *Theoretical Computer Science*, vol. 660, pp. 23–56, 2018.

[7] X. Gao and L. Zhang, "Efficient anonymous ciphertext-policy attribute-based encryption for general structures supporting leakage-resilience," *International Journal of Network Security*, vol. 22, no. 5, pp. 763–774, 2020.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS)*, pp. 89–98, Alexandria, VA, USA, 2006.

[9] S. Halevi and H. Lin, "After-the-fact leakage in public-key encryption," in *Theory of Cryptography Conference (TCC)*, pp. 107–124, Providence, RI, USA, 2011.

[10] M. S. Hwang, T. H. Sun, and C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits Systems and Computers*, vol. 26, no. 5, 2017.

[11] C. C. Lee, P. S. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[12] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Theory of Cryptography Conference (TCC)*, pp. 70–88, Providence, RI, USA, 2010.

[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 62–91, Riviera, FrenchA, 2010.

[14] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Transactions on Services Computing*, vol. 13, no. 3, pp. 478–487, 2020.

[15] J. Li, Q. Yu, and Y. Zhang, "Hierarchical attribute based encryption with continuous leakage-resilience," *Information Sciences*, vol. 484, pp. 113–134, 2019.

[16] J. Li, Q. Yu, Y. Zhang, and J. Shen, "Key-policy attribute-based encryption against continual auxiliary input leakage," *Information Sciences*, vol. 470, pp. 175–188, 2019.

[17] H. Ma, Z. Wang, J. Wang, and Z. Guan, "Multi-authority attribute-based encryption resilient against auxiliary-input leakage," *Journal of Computers*, vol. 31, no. 1, pp. 134–147, 2020.

[18] S. Micali and L. Reyzin, "Physically observable cryptography," in *Theory of Cryptography Conference (TCC)*, pp. 278–296, Cambridge, MA, USA, 2004.

[19] P. K. Premkamal and S. K. Pasupuleti, "Dynamic traceable cp-abe with revocation for outsourced big data in cloud storage," *International Journal of Communication Systems*, vol. 34, no. 2, p. e4351, 2021.

[20] J. Ren, L. Zhang, and B. Wang, "Decentralized multi-authority attribute-based searchable encryption scheme," *International Journal of Network Security*, vol. 23, no. 2, pp. 332–342, 2021.

[21] A. Sahai and B. R. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 457–473, Aarhus, Denmark, 2004.

[22] Z. Wang and S. M. Yiu, "Attribute-based encryption resilient to auxiliary input," in *The International Conference on Provable Security (ProvSec)*, p. 371–390, Kanazawa, Japan, 2015.

[23] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography Springer Berlin Heidelberg (PKC)*, pp. 53–70, Taormina, Italy, 2008.

[24] B. Waters, "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions," in *Annual International Cryptology Conference*, pp. 619–636, Santa Barbara, CA, USA, 2009.

[25] T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "Identity-based encryption resilient to continual auxiliary leakage," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 117–134, Cambgridge, UK, 2012.

[26] T. H. Yuen, Y. Zhang, and S. M. Yiu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *European Symposium on Research in Computer Security(ESORICS)*, pp. 130–147, Wroclaw, Poland, 2014.

[27] J. Zhang and L. Zhang, "Anonymous cp-abe against side-channel attacks in cloud computing," *Journal of Information Science and Engineering*, vol. 33, no. 3, p. 789–805, 2017.

[28] L. Zhang and Y. Shang, "Leakage-resilient attribute-based encryption with cca2 security," *International Journal of Network Security*, vol. 21, no. 5, pp. 819–827, 2019.

[29] M. Zhang, S. Wei, and C. Wang, "Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions," in *International Conference on Information Security Practice and Experience (ISPEC)*, pp. 75–90, Lanzhou, China, May 2013.

[30] M. Zhang, Y. Zhang, Y. Su, Q. Huang, , and Y. Mu, "Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments," *IEEE Systems Journal*, vol. 11, no. 2, pp. 1018–1026, 2017.

Biography

Yuyan Guo Associate professor in the School of Computer Science and Technology, Huaibei Normal University. She received her Ph.D. degree in computer science from Hohai University, Nanjing, China in 2016. Her research interests include cryptography and information security, cloud computing and trusted computing etc. She has published over 10 research papers in refereed international conferences and journals.

Zhenhua Lu MS. of Huaibei Normal University. His research interests include information security and cryptography.

Mingming Jiang Associate professor in the School of Computer Science and Technology, Huaibei Normal University. He received his PhD in cryptography from Xidian University in 2014, and received his MS and BS in cryptography from Huaibei Normal University in 2010 and 2007, respectively. His research interests include public key cryptography based on lattice and provable security.

Dongbing Zhang Born in 1974, Master. Now, he is an associate professor in Huaibei Normal University. His main research interests include algorithm optimization and information security.

An Improved Three-Factor Remote User Authentication Protocol Using Elliptic Curve Cryptography

Wan-Rong Liu, Bin Li, and Zhi-Yong Ji
(Corresponding author: Zhi-Yong Ji)

Shanghai Jiao Tong University Affiliated Sixth People's Hospital
Shanghai 201306, China
Email: joyer99@126.com

(Received Aug. 30, 2021; Revised and Accepted Jan. 22, 2022; First Online Mar. 26, 2022)

Abstract

With the rapid development of the Internet, more and more users' private information, such as patients' vital signs, is maliciously obtained by attackers. Therefore, we analyzed some of the protocols. Based on the security problems existing in the protocols between Jiang *et al.* and Li *et al.*, we have proposed an improved three-factor remote user authentication protocol using elliptic curve cryptography. The improved protocol uses the knowledge of elliptic curve cryptography, which is an algorithm for establishing public key encryption. Its main advantage is that it provides equivalent or higher security than other methods using more minor keys in some cases. We construct our protocol by using discrete logarithm and computational Diffie-Hellman problem. The protocol uses only random numbers to ensure the freshness and security of the protocol and does not use timestamps, so clock asynchrony will not occur. We performed Burrows–Abadi–Needham logic analysis, security analysis, and comparative security analysis on the protocol. The analysis shows that the improved protocol has higher security and does not add much computation.

Keywords: Anonymity; Authentication; Elliptic Curve Cryptography

1 Introduction

With the rapid development of the Internet, positive progress has been made in the application of the Internet in all fields of our life, such as wearable medical devices, industry, and smart homes [1, 2]. The Internet has become an important auxiliary means in many fields [3]. It can not only improve work efficiency, but also actively promote us to change the way of life and make continuous progress towards a more advanced and intelligent way. However, with our increasing dependence on the network, network security has become one of the important factors restricting the development of the network. Telemedicine information system is rapid development, can be implanted and wearable devices to the patient's blood pressure, body temperature, electrocardiogram monitoring, information related to health care personnel can access the server to obtain patient vital signs of real-time data [4], especially can provide better medical care to patients in remote areas, However, when sensitive vital sign data of patients are transmitted to medical personnel through public channels, there will be information leakage [5]. Wazid *et al.* [6] proposed a mutual user authentication mechanism between a remote surgeon and the robotic arms. Whether in the medical field or in other fields, it is very important to continuously improve network security and build a safe and reliable network environment for users [7]. In essence, network security is the information security of Internet users, that is, the data flowing and interacting on the network system is not subject to accidental or malicious damage, disclosure, tampering, etc. Considering the importance of data information security, in network use, we should combine the characteristics of database use, the information in the database identity authentication and other technologies. At present, with the development of the researchers on the network security, authentication from the perspective of a user authentication on the number of factors, from the initial single factor authentication protocol development up to now the double factor and three factors of authentication protocol, our agreement is a kind of based on the users passwords, smart cards and biometric information of three factor authentication protocol [8]. Compared with the traditional two-factor authentication protocol based on smart card and user password, the advantage of three-factor authentication protocol with user biometric is that there is no problem of forgetting or losing the user's biometric information [9], and it is hard for attackers to guess. This information is unique to the user. Due to the extensive application of basic pattern recogni-

tion system, more and more authentication schemes based on biometrics are proposed [10]. The following is a brief introduction to the work of other researchers close to our work. In 2018, Wazid *et al.* [11] proposed a protocol for generic IoT networks.

In 2019, Lu *et al.* [7] proved that the protocol of Das *et al.* [13] had some security flaws. In 2020, Jabbari *et al.* [14] proposed a new scheme in order to provide mutual authentication between users and sensor devices directly. Xu *et al.* [15] proposed a patient healthcare monitoring authentication protocol. And Alzahrani *et al.* [16] demonstrated that Xu *et al.*' protocol has privacy issues and is vulnerable to attacks such as replay attacks. Merabet *et al.* [17] proposed some protocols for IoT-based healthcare applications in 2020. Garg *et al.* [18] pointed out that Merabet *et al.*'s protocol cannot resist strong replay attack. Sharma *et al.* [19] thought Merabet *et al.*'s protocol cannot support blockchain solution. In 2015, He *et al.* [20] proposed an improved authentication protocol based on time certificate. In 2016, Jiang *et al.* [21] pointed out that He *et al.* had interior attack, stolen smart card attack and other security risks in their protocol and proposed their own protocol. In 2018, Li *et al.* [22] pointed out that the agreements of Jiang *et al.* and He *et al.* had some common shortcomings, such as the lack of password change stage, clock synchronization and other security problems. In the same year, Li *et al.* proposed an improved agreement based on Jiang *et al.*, but we found that there were some problems with Li *et al.*'s improved agreement.

1) Failure to provide three-factor certification: authentication protocols that provide three-factor security mean that attackers can only launch impersonation attacks until he/she has mastered all three factors: password, biometrics, and smart cards. Li *et al.* claimed that their protocol can provide three-factor security. However, we find that if an attacker steals a user's smart and acquires the user's biometric, he/she can perform an offline identity and password guessing attack, in which case, Li *et al.*'s protocol fails to provide the privacy protection and security attributes they claim.

2) Failure to resist forgery attack: Forgery attack is a common type of attack. The attacker can impersonate either party of the scheme using the communication messages collected from the public channel and the information in the user's smart card.

3) Failure to resist smart card loss attack.

4) Failure to provide user anonymity.

5) Failure to resist forward secrecy and so on.

We believe that the agreement proposed by Jiang *et al.* has a good framework. Therefore, based on the security problems existing in the agreement between Jiang et al and Li et al, an improved three-factor remote user authentication protocol using elliptic curve cryptography is proposed. Our improved protocol uses the knowledge of elliptic curve cryptography [23, 24], which is an algorithm for establishing public key encryption. The use of elliptic curves in cryptography was independently proposed by Neal Koblitz and Victor Miller in 1985. Its main advantage is that in some cases it provides equivalent or higher security than other methods using smaller keys, such as the RSA encryption algorithm. Another advantage is that can define a group of bilinear mapping between the double linear mapping has found a lot of application in cryptography, the downside is the same length under the key than any other mechanism of encryption and decryption operations take a long time, but you can use a shorter keys to achieve at the same level of security, so the safety degree of speed at the relatively faster. The probability of solving mathematical problems on elliptic curves by using polynomial time algorithm is negligible, so we construct our protocol by using discrete logarithm and computational Diffie-Hellman problem.

1) Discrete logarithm problem: given $P, aP \in E/Fq$, for unknown $a \in Z_n^*$, the probability of success of finding the value of a is negligible.

2) Computational Diffie-Hellman problem: given $P, aP, bP, P \in E/Fq$, for unknown $a, b \in Z_n^*$, the probability of success of finding the value of abP is negligible.

In addition, considering the clock synchronization problem, in wireless sensor networks, the clock precision of each network node is limited due to the cost limitation, and the difference between each node clock will be larger and larger with the passage of time [25]. Many important basic functions of wireless sensor networks require nodes in the network to maintain a relatively uniform time scale. In order to ensure the freshness of information transmission, researchers usually use the method of adding random numbers or timestamps into the protocol to resist replay attacks and man-in-the-middle attacks. Using both timestamp and random numbers in Jiang *et al.*'s protocol may encounter clock asynchronization problem. Our protocol uses only random numbers to ensure the freshness and security of the protocol, and does not use timestamps, so clock asynchrony will not occur [26]. Furthermore, the protocols of Jiang *et al.* and Li *et al.* both have the situation that the user name is sent in clear text, which cannot guarantee the anonymity of users. Our improved protocol ensures that the user name and password are not sent in clear text. Finally, we performed Burrows–Abadi–Needham logic [27] analysis, random oracle model analysis, security analysis and security comparative analysis on the protocol. The schematic diagram of the authentication process is shown in Figure 1.

2 Review of Jiang *et al.*'s Scheme

Jiang *et al.* put forward an untraceable two-factor authentication scheme for wireless sensor networks in 2016.

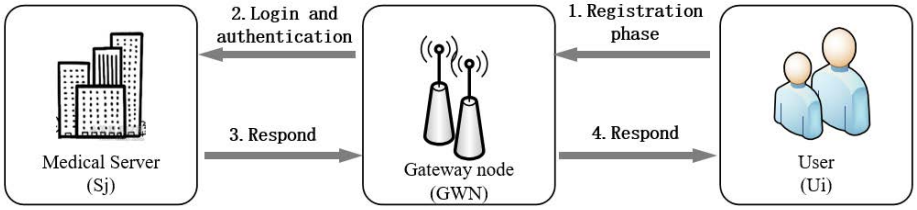


Figure 1: Schematic diagram of authentication process

Jiang *et al.*'s scheme consists of three phases: registration, login and authentication. This section is to review the scheme of Jiang *et al.* The notations used in the paper are summarized in Table 1.

Table 1: Notationas

Symbol	Definition
U_i	User
S_j	Medical Server
ID_i	Identity of U_i
PW_i	Password of U_i
GWN	Gateway node
c, y, g	A random number
P	A point on the elliptic curve
$P \cdot x$	The value of on x-axis
P_{par}	the parameters choosed by GWN
G	The additive group
SC	The smart card
n	A large prime order
F_P	A finite field
$h(\cdot)$	One-way hash function
$\oplus$	Bitwise XOR operation
$\|$	Concatenation operation
T	The current time of system
SID_j	Sensor node identity
PTC_i	The protected temporal credential of U_i
SK	Session-key
TC_i, TC_j	The temporal credential of U_i and S_j
TE_i	The expiration time of a user's temporal credential
b_i	Biological characteristics

2.1 User Registration Phase

Firstly, GWN chooses the additive group G generated by a point P with a large prime order n over a finite field F_P on an elliptic curve. The GWN randomly selects a number x as its private key and calculates $y = xP$ as public key. Finally, GWN stores x and publishes the system parameters $\{E(F_P), G, P, y\}$. Next, users register according to the following steps.

Step 1. As is supposed in He *et al.*'s scheme, U_i has a password PW_i shared with GWN, which maintains the value $\{U_i, H(PW_i)\}$. U_i imputs the old password PW_i, and selects a new one PW_i^{new}. Next, U_i chooses two random number a, $r_i \in Z_{p-1}^*$, calculates $A = aP, A' = ay = axP$, $VI_i = H(TS_1 \| H(PW_i) \| A \| A' \| H(PW_i^{new} \| ID_i \| r_i)$, $TPW_i = H(PW_i^{new} \| ID_i \| r_i) \oplus H(TS_1 \| H(PW_i) \| A \| A')$, sends messages $\{ID_i, TS_1, VI_i, TPW_i, A\}$ to GWN.

Step 2. GWN checks TS_1. If true, GWN calculates $A'' = xA = xaP$, $H(PW_i^{new} \| ID_i \| r_i) = TPW_i \oplus H(TS_1 \| H(PW_i) \| A \| A'')$, checks $VI_i \stackrel{?}{=} H(TS_1 \| H(PW_i) \| A \| A'' \| H(PW_i^{new} \| ID_i \| r_i))$, calculates $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$, $PTC_i = TC_i \oplus H(PW_i^{new} \| ID_i \| r_i)$, stores $\{H(\cdot), TE_i, PTC_i\}$ into a smart card, sends smart card to U_i.

2.2 Sensor Node Registration Phase

Step 1. S_j generates $b \in Z_{p-1}^*$, calculates $B = bP$, $B' = by = bxP$, $VI_j = H(TS_2 \| H(PW_j) \| B \| B')$, sends messages $\{SID_j, TS_2, VI_j, B\}$ to GWN.

Step 2. GWN checks TS_2. If true, GWN calculates $B'' = xB = xbP$, checks $VI_j \stackrel{?}{=} H(TS_2 \| H(PW_j) \| B \| B'')$, $TC_j = H(K_{GWN-S} \| SID_j)$, $REG_j = TC_j \oplus H(TS_3 \| H(PW_j) \| B \| B'')$, $VI_{GWN} = H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B''))$, sends messages $\{TS_3, REG_j, VI_{GWN}\}$ to S_j.

Step 3. S_j checks TS_3. If true, calculates $TC_j = REG_j \oplus H(TS_3 \| H(PW_j) \| B \| B')$, checks $VI_{GWN} \stackrel{?}{=} H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B'))$. If these two value are unequal, S_j terminates the session; otherwise, it stops.

2.3 Login and Authentication Phase

Step 1. U_i inputs ID_i and PW_i, the smart card calculates $TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$, U_i randomly generates $c \in Z_{p-1}^*$. Then U_i computes $C_i = cP$, $D_i = cy = cxP$, generates K_i, calculates $DID_i = ID_i \oplus H(C_i \| D_i)$, $PKS_i = K_i \oplus H(TC_i \| TS_4 \| D_i)$, $E_i = H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i)$, sends

messages $\{DID_i, C_i, PKS_i, TS_4, E_i\}$ to GWN. TS_4 is the current timestamp.

Step 2. Once receiving the message from U_i. GWN checks TS_4. If true, GWN calculates $D_i = xC = xcP$, $ID_i = DID_i \oplus H(C_i \| D_i)$, checks ID_i and retrieves TE_i, $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$, checks $H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i) \stackrel{?}{=} E_i$, $K_i = PKS_i \oplus H(TC_i \| TS_4 \| D_i)$, $TC_j = H(K_{GWN-S} \| SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i \| TC_j \| TS_5)$, $C_{GWN} = H(ID_i \| TC_j \| TS_5)$, $PKS_{GWN} = K_i \oplus H(TC_j \| TS_5)$, sends messages $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j. TS_5 is the current timestamp.

Step 3. Once receiving the message from GWN. S_j checks TS_5. If true, S_j calculates $ID_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_5)$, checks $C_{GWN} \stackrel{?}{=} H(ID_i \| TC_j \| TS_5)$, generates K_j, calculates $K_i = PKS_{GWN} \oplus H(TC_j \| TS_5)$, $SK_{ij} = H(K_i \oplus K_j)$, $C_j = H(K_j \| ID_i \| SID_j \| TS_6)$ $PKS_j = K_j \oplus H(K_i \| TS_6)$, sends messages $\{SID_j, TS_6, C_j, PKS_j\}$ to U_i. TS_6 is the current timestamp.

Step 4. Once receiving the message from S_j. U_i checks TS_6. If true, U_i calculates $K_j = PKS_j \oplus H(K_i \| TS_6)$, checks $C_j \stackrel{?}{=} H(K_j \| ID_i \| SID_j \| TS_6)$. Finally, U_i calculates the session key $SK_{ij} = H(K_i \oplus K_j)$.

3 Weaknesses of Jiang *et al.*'s Scheme

3.1 Weakness 1: No User Anonymity

In Jiang *et al.*'s scheme and Li *et al.*'s scheme, ID_i is sent in plaintext in the registration. Once the attacker as a co-worker in the same organization, he/she acquires the information $\{ID_i, RPW_i, b_i\}$ and has knowledge of ID_i.Jiang *et al.*'s protocol does not guarantee user anonymity.

3.2 Weakness 2: Failure to Defend Known Session-Specific Temporary Information Attack

Once the session-specific temporary information of the protocol is leaked, such as random numbers that make up the session password, the session key is still secure, which indicates that the protocol can resist the known session-specific temporary information attack. In Jiang *et al.*'s scheme, the session key $SK_{ij} = H(K_i \oplus K_j)$, where K_i is generated by U_i and K_j is generated by S_j in the login and authentication phase. If an attacker knows information K_i and K_j, the session key will be exposed to the attacker. So in that sense, Jiang *et al.*'s scheme cannot defend known session-specific temporary information temporary information attack.

3.3 Weakness 3: No Password Change Phase

At present, authentication protocols are vulnerable to offline password guessing attacks and online password guessing attacks. Moreover, most users habitually use some anniversaries or dates with special meanings, which will further reduce the security of passwords. Jiang *et al.*'s scheme has no password change phase, which not only prevents users from changing their password when they forget it, but also makes their protocol vulnerable to password-related attacks. Of course, we know that we need not only the password change phase, but also the user authentication in the password change stage. Otherwise any illegal user will be able to change the password of the legitimate user, which will also have security risks.

3.4 Weakness 4: Inapplicable to IoT Environments

Wireless sensor network is very different from the traditional wireless communication network. The primary design goal of the traditional wireless communication network is to provide the highest possible service quality, and node energy can be supplemented, so consumption is a secondary consideration. However, the nodes of wireless sensor networks cannot replenish energy, so extending the life cycle of the network system as far as possible has become the primary design goal of wireless sensor networks [25]. Sensor nodes use low-power devices as much as possible, and the research on energy consumption is also based on low-power devices. Communication module is the department with the largest energy consumption among nodes, and it is also the focus of the research on wireless sensor network nodes. In the login and authentication phase of Jiang *et al.*'s protocol, a part of the information is transmitted directly between the user and the server, rather than building a communication platform for the user and the server through a third party GWN, which is inconsistent with the wireless sensor network's need to extend the life cycle of the network system as far as possible.

3.5 Weakness 5: No Clock Synchronization Mechanism

In information transmission, we need to ensure the freshness of information transmission and ensure that the information transmitted by legitimate users will not be intercepted and utilized by attackers, such as replay attack and man-in-the-middle attack, etc. Generally, researchers solve this problem by two methods: timestamp mechanism and random numbers. However, in wireless sensor

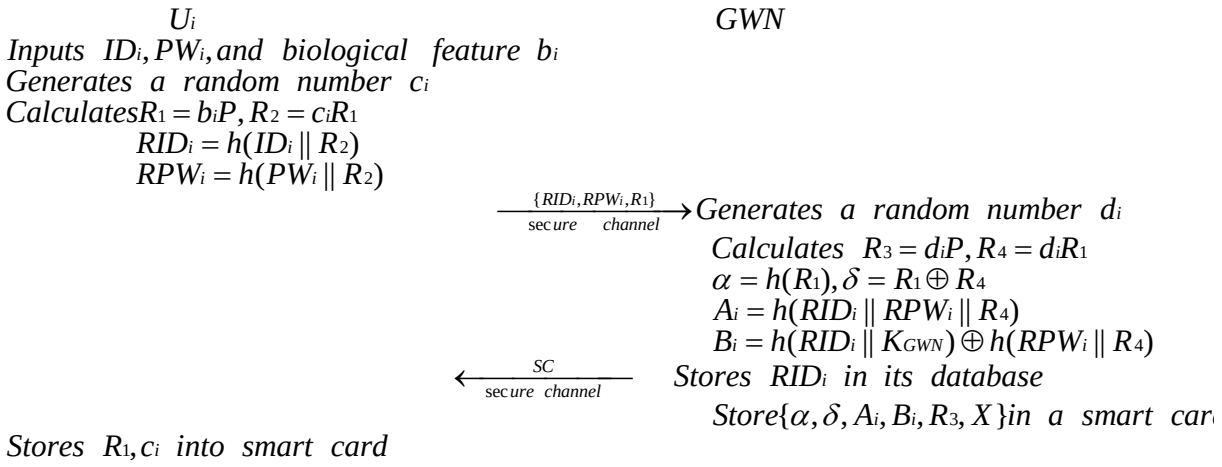


Figure 2: Registration phase of proposed protocol

networks, the clock precision of each network node is limited due to the cost limitation, and the difference between each node clock will be larger and larger with the passage of time. Many important basic functions of wireless sensor networks require nodes in the network to maintain a relatively uniform time scale. Using both timestamp and random numbers in Jiang *et al.* 's protocol may encounter clock asynchronization problem.

4 Proposed Protocol

At present, user biometric information is widely used in three-factor authentication protocols because of their uniqueness. We believe that Jiang *et al.* 's protocol has a good framework, so we propose an improved remote identity authentication protocol based on elliptic curve cryptography based on Jiang *et al.*' s two-factor authentication protocol. Our protocol not only improves the disadvantages of Jiang *et al.*'s protocol, but also adds user biometric to improve the security of the protocol.

Furthermore, we use elliptic curve cryptography, which provides equal or higher levels of security while using smaller keys than other methods.

4.1 Registration Phase

Firstly, GWN chooses the parameters $\{E(F_P), G, x, X, P_{par}, K_{GWN}\}$, $X = xP_{par}$, like Jiang *et al.*'s protocol in user registration phase. The registration phase of proposed protocol is shown in Figure 2.

During the registration phase, he/she will perform the following steps complete the registration.

4.2 Login and Authentication Phase

Once the user is registered, he/she will follow the steps below to begin the login and authentication phase. The login and authentication phase of proposed protocol is shown in Figure 3.

4.3 Password Change Phase

Compared with the protocol of Jiang *et al.*, our proposed improved protocol allows the user to change his/her password. Once the user wants to change his/her password, he/she will proceed as follows: U_i inserts smart card into a card reader, inputs biological feature b_i, SC calculates $R_4 = \delta \oplus R_1$, checks to see if the equation $R_4 = \delta \oplus R_1 \stackrel{?}{=} R_4' = b_i'R_3$ is true, and if so, SC continues to calculate the equation $A_i' = h(h(ID_i \| c_ib_i'P) \| h(PW_i \| c_ib_i'P) \| R_4') \stackrel{?}{=} A_i$ in its database. If they are equal, SC accepts $U_i's$ request to change passwords and sends U_i a request to enter a new password. Once U_i enters a new password, SC calculates $A_i^{new} = h(h(ID_i \| R_2) \| h(PW_i^{new} \| R_2) \| R_4')$, $B_i^{new} = h(h(ID_i \| R_2) \| K_{GWN}) \oplus h(h(PW_i^{new} \| R_2) \| R_4')$, updates A_i^{new} and B_i^{new} with A_i and B_i respectively. Following this step, the user makes a password change.

5 Security Analysis

In this section, we conducted a security analysis of our proposed protocol, and we demonstrated that our protocol can withstand all the major attacks.

User anonymity. In our improved protocol, either the user name U_i or the password PW_i is transmitted in plaintext. And U_i passes $RID_i = h(ID_i \| R_2), RPW_i = h(PW_i \| R_2)$ to GWN, where $R_2 = c_ib_iP$. According to DL and CDH problem, we can know that even if the attacker obtains the information R_1 in the channel, he/she cannot calculate R_2. So our protocol can guarantee user anonymity.

Resist known session-specific temporary information attack. In Jiang *et al.*'s scheme, the session key $SK_{ij} = H(K_i \oplus K_j)$, where K_i is generated by U_i and K_j is generated by S_j in the login and authentication phase. If an attacker knows information K_i and K_j, the session key will be exposed

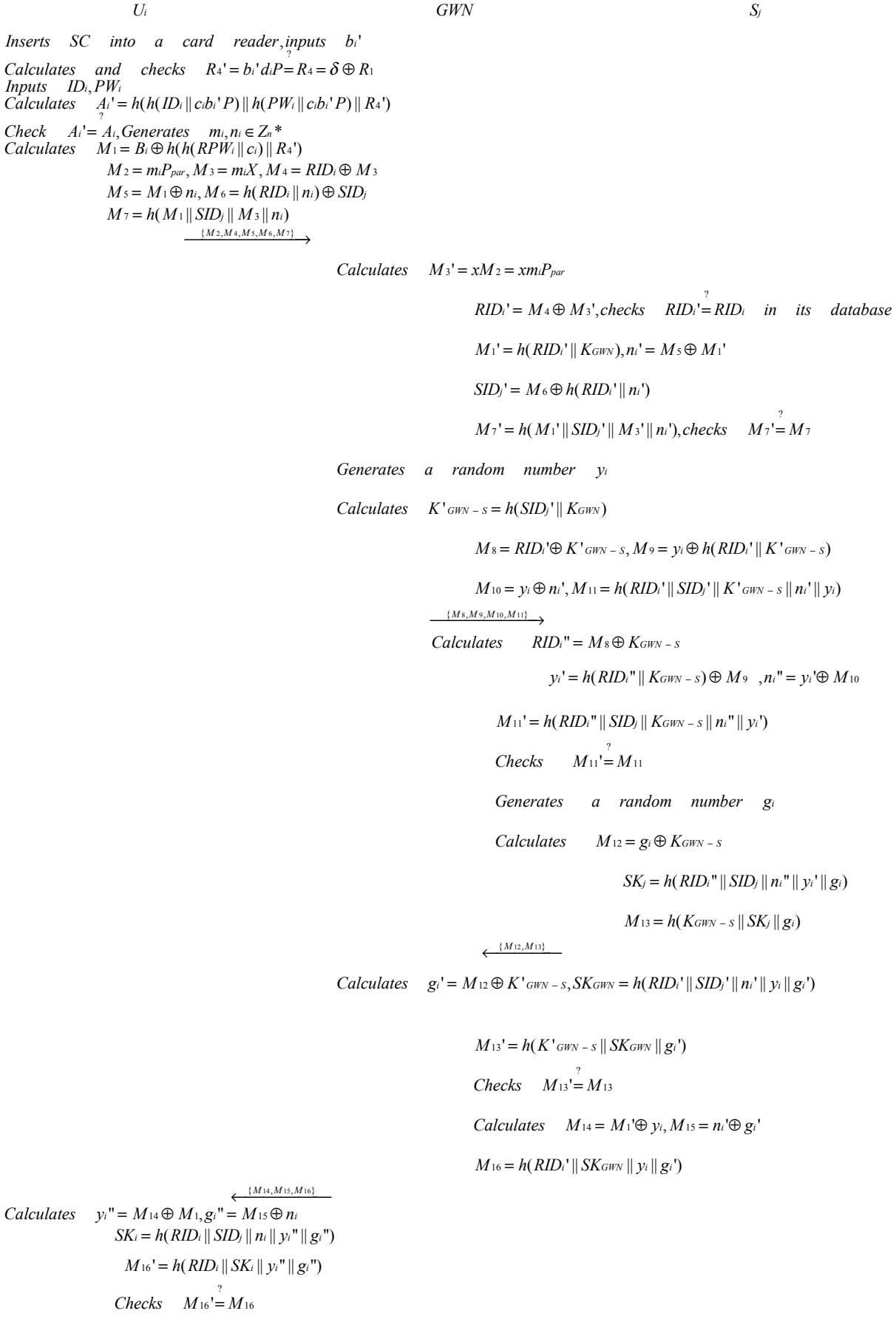


Figure 3: Login and authentication phase of proposed protocol

to the attacker. In our improved protocol, the session key $SK_i = h(RID_i \| SID_j \| n_i \| y_i'' \| g_i'')$, where $RID_i = h(ID_i \| R_2)$, $SID_j = M_6 \oplus h(RID_i \| n_i)$, $n_i \in Z_n^*$, y_i and g_i are random numbers. Even though an attacker knows the information y_i, g_i, it would not be able to calculate SK_i without the information SID_j.

Efficient password change. Jiang *et al.*'s protocol does not have a password change mechanism. Our proposed improved protocol has a password change mechanism, and once the user wants to change his/her password, the system will verify it first. The system will only let the user go through the password change phase if the authentication has passed.

Applicable to IoT environments. In the login and authentication phase of Jiang *et al.*'s protocol, a part of the information is transmitted directly between the user and the server, rather than building a communication platform for the user and the server through a third party, which is inconsistent with the wireless sensor network's need to extend the life cycle of the network system as far as possible. We modified this part of Jiang *et al.* 's protocol to ensure that the information transfer between the user and the server needs to be carried out through a third party GWN.This form of information transmission is more suitable for the Internet of Things environment

Clock synchronization mechanism. In order to resist replay attack or man-in-the-middle attack, scholars usually add timestamp mechanism or random number into the protocol. However, when both of these are used in the protocol, the clock asynchronous problem will be caused, so we only use random numbers in the improved protocol, without the use of timestamp mechanism, which ensures the protection against replay attacks or man-in-the-middle attacks, while keeping the clock synchronized.

Resist privileged insider attack. In general, users tend to register on different systems with the same password in order to remember the password more easily. Once a privileged internal staff member obtains the user's password, she/he can use the same password for access on other systems. However, our proposed protocol does not pass the user's username and password over the channel in clear text, and it also uses CDH mathematical puzzle to mask them.

Resist stolen smart attack. In our improved protocol, the massages $\{\alpha, \delta, A_i, B_i, R_3, X, f(\cdot)\}$ are stored on the smart card, where $A_i = h(RID_i \| RPW_i \| R_4)$, $B_i = h(RID_i \| K_{GWN}) \oplus h(RPW_i \| R_4)$. So given the CDH problem, even if the attacker knows c_i, d_i, R_1, he/she cannot compute R_4 or R_2. So attackers cannot get important information from smart cards even if they use side-channel attack such as strong analysis.

Provide mutual authentication. In Jiang et al,' protocol, the session key $SK_{ij} = H(K_i \oplus K_j)$. We think it failures to defend known session-specific temporary information attack. In our protocol, the session key $SK = h(RID_i \| SID_j \| n_i \| y_i \| g_i)$, where $RID_i = M_4 \oplus M_3$, $SID_j = M_6 \oplus h(RID_i \| n_i)$, y_i' and g_i are random numbers. The attacker cannot derive the correct RID_i without M_3. And we never send M_3 on the message channel. So our protocol can be safely authenticated to each other.

5.1 Security Analysis Using BAN Logic

The goals to be achieved by using BAN logic are mutual authentication among, GWN, and S_i. The goals are described by using BAN logic language as follows:

$G1 : S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G2 : S_j| \equiv U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G3 : U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G4 : U_i| \equiv S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G5 : GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$

$G6 : GWN| \equiv U_i| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$

$G7 : GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} S_j$

$G8 : GWN| \equiv S_j| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} S_j$

The messages that U_i, GWN, and S_i communicate with each other are described in BAN logic language as follows:

$M_1 : U_i \rightarrow GWN : \{M_2, M_4, M_5, M_6, M_7\}$
$\{miP_{par}, \langle RID_i \rangle_{miX}, \langle n_i \rangle_{h(RID_i \| K_{GWN})}, \langle SID_j \rangle_{h(RID_i \| n_i)},$
$(SID_j \| n_i) miX, h(RID_i \| K_{GWN})\}$
$M_2 : GWN \rightarrow S_j : \{M_8, M_9, M_{10}, M_{11}\}$
$\{\langle RID_i' \rangle_{K_{GWN-S}}, \langle y_i \rangle_{h(RID_i' \| K_{GWN-S}')}, \langle n_i \rangle_{y_i},$
$(RID_i \| SID_j)(n_i, y_i, K_{GWN-S}')\}$
$M_3 : S_j \rightarrow GWN : \{M_{12}, M_{13}\}$
$\{\langle g_i \rangle_{K_{GWN-S}}, (g_i)(SK_j, K_{GWN-S}')\}$
$M_4 : GWN \rightarrow U_i : \{M_{14}, M_{15}, M_{16}\}$
$\{\langle y_i \rangle_{h(RID_i \| K_{GWN})}, \langle g_i' \rangle_{n_i'}, (RID_i')(y_i, g_i', SK_{GWN})\}$

To demonstrate the security of our proposed protocol, we propose a number of hypotheses:

$A_1 : U_i| \equiv \#n_i$

$A_2 : GWN| \equiv y_i$

$A_3 : S_j| \equiv \#g_i$

$A_4 : U_i| \equiv U_i \overset{miX}{\longleftrightarrow} GWN$

$A_5 : U_i| \equiv U_i \overset{SK_j}{\longleftrightarrow} S_j$

$A_6 : GWN| \equiv GWN \overset{mixP}{\longleftrightarrow} U_i$

$A_7 : GWN| \equiv GWN \overset{K_{GWN-S}}{\longleftrightarrow} S_j$

$A_8 : S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$A_9 : S_j| \equiv S_j \overset{K_{GWN-S}}{\longleftrightarrow} GWN$

$A_{10} : U_i| \equiv S_j \Rightarrow g_i, SK_j$

$A_{11} : U_i| \equiv GWN \Rightarrow y_i, SK_{GWN}$

$A_{12} : GWN| \equiv U_i \Rightarrow n_i, SK_i, mixP$

$A_{13} : GWN| \equiv S_j \Rightarrow g_i \oplus K_{GWN-S}$

$A_{14} : S_j| \equiv GWN \Rightarrow y_i \oplus h(RID_i \| K_{GWN-S})$

$A_{15}: S_j| \equiv U_i \Rightarrow n_i, SK_i$

According to the above initial state and based on BAN logic inference rules, the properties of the protocol are analyzed and deduced as follows:

From $M_1: U_i \rightarrow GWN: \{M_2, M_4, M_5, M_6, M_7\}$, we have

$S_1: GWN \triangleleft \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According to S_1, A_6, and message meaning rule, we have

$S_2: GWN| \equiv U_i \sim \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i) miX, h(RID_i\|K_{GWN})\}$.

According to S_2, A_1, and freshness conjucatenation and nonce verification rules, we have

$S_3: GWN| \equiv U_i| \equiv \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According to S_3, A_6, A_{12}, and jurisdiction rule, we have

$S_4: GWN| \equiv \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According S_4, and session key rule, we have

$S_5: GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$. (G5)

According S_5, A_2, and nonce-verification rule, we have

$S_6: GWN| \equiv U_i| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$. (G6)

According M_2, we have

$S_7: S_j \triangleleft \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j)(n_i, y_i, K'_{GWN-S})\}$.

According to S_7, A_9, and message meaning rule, we have

$S_8: S_j| \equiv GWN \sim \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i \|SID_j) (n_i, y_i, K'_{GWN-S})\}$.

According to S_8, A_2, A_{14}, and freshness conjucatenation and nonce verification rules, we have

$S_9: S_j| \equiv GWN| \equiv \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j) (n_i, y_i, K'_{GWN-S})\}$.

According M_4, we have

$S_{10}: U_i \triangleleft \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{10}, A_4, and message meaning rule, we have

$S_{11}: U_i| \equiv GWN \sim \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{11}, A_2, A_{11}, freshness conjucatenation and nonce verification rules, we have

$S_{12}: U_i| \equiv GWN| \equiv \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_9, A_9, A_{14}, and jurisdiction rule, we have

$S_{13}: S_j| \equiv \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j)(n_i, y_i, K'_{GWN-S})\}$.

According to S_{12}, A_4, A_{11}, and jurisdiction rule, we have

$S_{14}: U_i| \equiv \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{13}, and the session key rules, we have

$S_{15}: S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} GWN, S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$. (G1)

According to S_{13}, A_{14}, and the session key rules ,we have

$S_{16}: S_j| \equiv GWN| \equiv S_j \overset{SK_j}{\longleftrightarrow} GWN, S_j| \equiv U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$. (G2)

According to S_{14}, and the session key rules, we have

$S_{17}: U_i| \equiv U_i \overset{SK_i}{\longleftrightarrow} GWN, U_i| \equiv S_j \overset{SK_i}{\longleftrightarrow} U_i$. (G3)

According to S_{14}, A_{11}, A_5 and the session key rules ,we have

$S_{18}: U_i| \equiv GWN| \equiv U_i \overset{SK_i}{\longleftrightarrow} GWN, U_i| \equiv S_j| \equiv S_j \overset{SK_i}{\longleftrightarrow} U_i$. (G4)

According $M_3: S_j \rightarrow GWN: \{M_{12}, M_{13}\}$, we have

$S_{19}: GWN \triangleleft \{\langle g_i\rangle K_{GWN-S}, (g_i)(SK_j, K'_{GWN-S})\}$.

According S_{19}, A_7, and message meaning rule, we have

$S_{20}: GWN| \equiv S_j \sim \{\langle g_i\rangle K_{GWN-S}, (g_i) (SK_j, K'_{GWN-S})\}$.

According S_{20}, A_3, we have

$S_{21}: GWN| \equiv S_j| \equiv \{\langle g_i\rangle K_{GWN-S}, (g_i) (SK_j, K'_{GWN-S})\}$.

According S_{21}, A_7, A_{13}, and jurisdiction rule, we have

$S_{22}: GWN| \equiv \{\langle g_i\rangle K_{GWN-S}, (g_i)(SK_j, K'_{GWN-S})\}$.

According to S_{22}, A_{13}, A_{15}, we have

$S_{23}: GWN| \equiv S_j| \equiv S_j \overset{SK_{GWN}}{\longleftrightarrow} GWN$. (G8)

According to S_{22}, A_8, we have

$S_{24}: GWN| \equiv S_j \overset{SK_{GWN}}{\longleftrightarrow} GWN$. (G7)

According to the BAN logic proof, mutual authentication can be achieved between them.

5.2 Security Analysis Using Random Oracle Model

We conduct a security proof in the random oracle model. Through strict formal verification using random Oracle, it can be proved that the scheme is secure against an adversary.

Definition 1. *Reveal: Given a hash value $y = h(x)$, this random oracle unconditionally outputs the input x.*

Theorem 1. *Under the assumption that a one-way hash function $h(\cdot)$ behaves like an oracle, the proposed scheme is probably secure against an adversary A for deriving the identity ID_i, the password PW_i, the biometric key b_i of a legal user U_i and the secure key K_{GWN} of the GWN, even if user U_i's smart card is lost/stolen.*

Proof. For the proof, we assume that an adversary A is able to derive the identity ID_i, the password PW_i, the biometric key b_i of a legal user U_i, and the secret key K_{GWN} of the GWN. We assume that the adversary A has lost/stolen smart card of the user U_i and A can extract all the sensitive information stored in smart card using the power analysis attack. For this, A uses the Reveal oracle to run an experimental algorithm $EXP1^{3FAKA}_{HASH,A}$ shown in Algorithm 1for

the proposed three-factor authentication and key agreement(3FAKA). We define the success probability for $EXP1^{3FAKA}_{HASH,A}$ as $Succ1^{3FAKA}_{HASH,A} = |\Pr[EXP1^{3FAKA}_{HASH,A} = 1] - 1|$, where $\Pr[E]$ is the probability of an event E. The advantage function for this experiment becomes $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) = \max A\{Succ1^{3FAKA}_{HASH,A}\}$ in which the maximum is taken over all A with execution time t_1 and the number of queries q_R made to the Reveal oracle. According to the attack experiment described in Algorithm 1, if the adversary A has the ability to invent the one-way hash function $h(\cdot)$, then A can directly obtain $U_i's$ ID_i, PW_i and b_i and $GWN's$ K_{GWN}, and win the game. However, it is computationally infeasible problem to invert $h(\cdot)$, i.e., $Adv1^{3FAKA}_{HASA,A}(t_1) < \varepsilon$, for any sufficiently small $\varepsilon > 0$. Then, we have $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) \leq \varepsilon$, since $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) \leq \varepsilon$ depends on $Adv1^{3FAKA}_{HASA,A}(t_1)$. Therefore, the proposed scheme is provably secure against the adversary A for deriving ID_i, PW_i, b_i and K_{GWN}, even if the smart card is lost/stolen by A. □

1: Extract the information $\{\alpha, \delta, A_i, B_i, R_3, X\}$ from smart card using the power analysis attack.
2: Call the Reveal oracle. Let $(RID_i^*, K_{GWN}*, RPW_i^*, R_4*) \leftarrow \mathrm{Re}\,veal(B_i)$
3: Call the Reveal oracle. Let $(R_1* = b_i^*P) \leftarrow \mathrm{Re}\,veal(\alpha)$
4: Compute $R_1' = R_4 * \oplus\delta$
5: **if** $(R_1' = R_1*)$ **then**
6: Call the Reveal oracle. Let $(ID_i^*, R_2*) \leftarrow \mathrm{Re}\,veal(RID_i)$
7: Call the Reveal oracle. Let $(PW_i^*, R_2*) \leftarrow \mathrm{Re}\,veal(RPW_i)$
8: Compute $A_i^* = h(h(ID_i^*\|R_2*)\|h(PW_i^*\|R_2*)\|R_4*)$
9: **if** $(A_i^* = A_i)$ **then**
10: Intercept the message $\{M_8, M_9, M_{10}, M_{11}\}$
11: Call the Reveal oracle. Let $(RID_i^*, SID_j*, K'_{GWN-S}*, n_i^*, y_i^*) \leftarrow \mathrm{Re}\,veal(M_{11})$
12: Call the Reveal oracle. Let $(SID_j **, K_{GWN} * *) \leftarrow \mathrm{Re}\,veal(K'_{GWN-S}*)$
13: Compute $M_8* = RID_i^* \oplus K'_{GWN-S}*$
14: Compute $B_i^* = h(RID_i^*\|K_{GWN} * *) \oplus h(RPW_i^*\|R_4*)$
15: **if** $(M_8* = M_8)$ and $(B_i^* = B_i)$ **then**
16: Accept ID_i^*, PW_i^* and b_i^* as the correct identity ID_i, PW_i and b_i of the user, an
17: $K_{GWN} **$ as the correct parameters of GWN.
18: **return** 1
19: **else**
20: **return** 0
21: **end if**
22: **else**
23: **return** 0
24: **end if**
25: **else**
26: return 0
27: **end if**

Algorithm 1 $EXP1^{3FAKA}_{HASH,A}$

Theorem 2. *Under the assumption that a one-way hash function $h(\cdot)$ behaves like an oracle, the proposed scheme is probably secure against an adversary A for deriving the session key SK_j/SK_i shared between U_i and S_j.*

Proof. We assume that an adversary A is able to derive the session key shared between a legal user and medical server S_j. For this, A user the Reveal oracle to run an experimental algorithm $EXP2^{3FAKA}_{HASH,A}$ shown in Algorithm 2. We define the success probability for $EXP2^{3FAKA}_{HASH,A}$ as $Succ2^{3FAKA}_{HASH,A} = |\Pr[EXP2^{3FAKA}_{HASH,A} = 1] - 1|$. The advantage function for this experiment becomes $Adv2^{3FAKA}_{HASA,A}(t_2, q_R) = \max A\{Succ2^{3FAKA}_{HASH,A}\}$ in which the maximum is taken over all A with execution time t_2 and the number of queries q_R made to the Reveal oracle. According to the attack experiment described in Algorithm 2, if the adversary A has the ability to invert the one-way hash function $h(\cdot)$, then A can easily derive SK_j/SK_i and win the game. However, it is computationally infeasible problem to invent $h(\cdot)$, i.e., $Adv2^{3FAKA}_{HASA,A}(t_2) \leq \varepsilon$, for any sufficiently small $\varepsilon > 0$. Then, we have $Adv2^{3FAKA}_{HASA,A}(t_2, q_R) \leq \varepsilon$ is also dependent on $Adv2^{3FAKA}_{HASA,A}(t_2)$. The proposed scheme is provably secure against the adversary A for deriving S_j. □

1: Extract the login request information $\{M_2, M_4, M_5, M_6, M_7\}$ during the login phase.
2: Call the Reveal oracle. Let $(M_1'\|SID_j'\|M_3'\|n_i') \leftarrow \mathrm{Re}\,veal(M_7)$
3: Compute $RID_i' = M_4 \oplus M_3'$
4: Compute $n1* = M_5 \oplus M_1'$
5: **if** $(n1* = n1')$ **then**
6: Intercept the message $\{M_8, M_9, M_{10}, M_{11}\}$, $\{M_{12}, M_{13}\}$
7: Call the Reveal oracle. Let $(K * GWN - S\|SK_j * \|g_i^*) \leftarrow \mathrm{Re}\,veal(M_{13})$
8: Compute $g_i^{*'} = M_{12} \oplus K * GWN - S$
9: **if** $(g_i^* = g_i^{*'})$ **then**
10: Compute $y_i^* = M_{10} \oplus n_i'$
11: Compute $SK_j*' = h(RID_i'\|SID_j'\|n_i'\|y_i^*\|g_i^{*'})$
12: **if** $(SK_j*' = SK_j')$ **then**
13: Accept SK_j*' as the correct session key shared between U_i and S_j.
14: **return** 1
15: **else**
16: **return** 0
17: **end if**
18: **else**
19: **return** 0
20: **end if**
21: **else**
22: **return** 0

Table 2: Comparison of security features

Performance	Jiang *et al.* (2016) [21]	Farash *et al.* (2016) [?]	Wazid *et al.* (2018) [11]	Amin *et al.* (2018) [?]	Li *et al.* (2018) [22]	Ours
F1	Yes	No	Yes	No	No	Yes
F2	Yes	Yes	Yes	Yes	No	Yes
F3	No	No	No	Yes	No	Yes
F4	No	Yes	Yes	Yes	Yes	Yes
F5	No	Yes	Yes	Yes	Yes	Yes
F6	No	Yes	Yes	Yes	Yes	Yes
F7	No	Yes	No	No	Yes	Yes
F8	No	No	Yes	Yes	Yes	Yes
F9	Yes	No	No	No	No	Yes
F10	Yes	Yes	Yes	Yes	Yes	Yes
F11	No	No	No	No	No	Yes

F1: Provide three-factor security; F2: Resist forgery attack; F3: User anonymity; F4: Defend known session-specific temporary information attack; F5: Password change phase; F6: Applicable to IoT environments; F7: Clock synchronization mechanism; F8: Resist offline guessing attack; F9: Resist forward secrecy; F10: session key agreement; F11: Smart card loss attack.

Table 3: Comparison of efficiency characteristcs

	U_i	S_i	GWN	Total
Jiang *et al.*(2016) [21]	8 $T1$ +2 $T3$	6 $T1$	9 $T1$ + $T3$	23 $T1$ +3 $T3$
Farash *et al.*(2016) [?]	11 $T1$	7 $T1$	14 $T1$	32 $T1$
Wazid *et al.*(2018) [11]	13 $T1$ +2 $T2$	4 $T1$ +2 $T2$	5 $T1$ +4 $T2$	21 $T1$ +8 $T2$
Amin *et al.*(2018) [?]	12 $T1$	6 $T1$	16 $T1$	34 $T1$
Li *et al.*(2018) [22]	8 $T1$ +2 $T3$	4 $T1$	9 $T1$ + $T3$	21 $T1$ +3 $T3$
Our	7 $T1$ +2 $T3$	4 $T1$	9 $T1$ + $T3$	20 $T1$ +3 $T3$

$T1$: The cost for executing the hash function operation; $T2$: The cost for symmetric encryption/decryption operation; $T3$: The ECC operation for the ECC operation

23: **end if**

Algorithm 2 $EXP2^{3FAKA}_{HASH,A}$

6 Comparison of Security Features and Efficiency Characteristics

Table 2 is the comparison of security features. Table 3 is the comparison of efficiency characteristics.

7 Conclusions

Based on the security problems existing in the protocols between Jiang et al and Li et al, we have proposed an improved three-factor remote user authentication protocol using elliptic curve cryptography. Our improved protocol uses the knowledge of elliptic curve cryptography, which is an algorithm for establishing public key encryption. Its main advantage is that in some cases it provides equivalent or higher security than other methods using smaller keys. We construct our protocol by using discrete logarithm and computational Diffie-Hellman problem. And our protocol uses only random numbers to ensure the freshness and security of the protocol, and does not use timestamps, so clock asynchrony will not occur. We performed BAN logic analysis, security analysis and security comparative analysis on the protocol. From the analysis, we can see that the improved protocol has higher security and does not add much computation.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments

References

[1] B. A. Alzahrani, A. Irshad, A. Albeshri, *et al*, "A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Net-

works," *Wireless Personal Communications*, vol. 117, no. 1, pp. 47– 69, 2021.

[2] R. Amin, S. K. H. Islam, G. P. Biswas, *et al*, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018

[3] A. Angelucci, D. Kuller, A. Aliverti, "A home telemedicine system for continuous respiratory monitoring," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 4, pp. 1247– 1256, 2021.

[4] M. Burrows, M. Abadi, R. Needham, "A logic of Authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.

[5] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.

[6] M. L. Dow, S. R. Dugan, "Hypothesis: A wearable device may help COVID-19 patients improve lung function," *Medical Hypotheses*, vol. 146, 2021.

[7] M. S. Farash, M. Turkanovi´c, S. Kumari, *et al*, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[8] N. Garg, M. Wazid, A. K. Das, *et al*, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[9] D. He, N. Kumar, N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263–277, 2015.

[10] A. Jabbari , J. B. Mohasefi, "Usersensor mutual authenticated key establishment scheme for critical applications in wireless sensor networks," *Wireless Networks*, vol. 27, no. 1, pp. 227– 248, 2021.

[11] X. Y. Jia, D. B. He, N. Kumar, *et al*, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[12] Q. Jiang, S. Zeadally, J. F. Ma, *et al*, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376– 3392, 2017.

[13] X. Li, J. W. Niu, S. Kumari, *et al*, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[14] S. G. Liu, X. Wang, Y. W. Liu, *et al*, "Fast scalar multiplication algorithms based on 5p+ q of elliptic curve over gf (3ˆ m)," *International Journal of Network Security*, vol. 23, no. 4, pp. 604–611, 2021.

[15] W. R. Liu, X. He, Z. Y. Ji, "An improved authentication protocol for telecare medical information system," *International Journal of Electronics and Information Engineering*, vol. 12, no. 4, pp. 170–181, 2020.

[16] W. R. Liu, X. He, Z. Y. Ji, "Security analysis and enhancements of a user authentication scheme," *International Journal of Network Security*, vol. 23, no. 5, pp. 895–903, 2021.

[17] Y. R. Lu, G. Q. Xu, L. X. Li, *et al*, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[18] F. Merabet, A. Cherif, M. Belkadi, *et al*, "New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 439–474, 2020.

[19] J. Q. Mo, W. Shen, and W. S. Pan, "An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems," *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[20] R. Sharma, M. Wazid, P. Gope, "A blockchain based secure communication framework for community interaction," *Journal of Information Security and Applications*, vol. 58, 2021.

[21] S. Q. Cao, W. R. Liu, L. L. Cao, *et al*, "An Improved Authentication Protocol Using Smart Cards for the Internet of Things," *IEEE Access*, vol. 7, pp. 157284–157292, 2019.

[22] C. Wang, H. Y. Qi. "Visualising the knowledge structure and evolution of wearable device research," *Journal of Medical Engineering & Technology*, vol. 45, no. 3, pp.1-16, 2021.

[23] H. Wang, F. Yu, M. Li, *et al*, "Clock Skew Estimation for Timestamp-Free Synchronization in Industrial Wireless Sensor Networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 90–99, 2021.

[24] M. Wazid, A. K. Das, J. H. Lee, "User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions," *Pervasive and Mobile Computing*, vol. 54, pp. 71–85, 2019.

[25] M. Wazid, A. K. Das, V. Odelu, *et al*, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[26] F. Wu, X. Li, L. L. Xu, *et al*, "A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2021.

[27] Z. S. Xu, C. Xu, H. X. Chen, *et al*, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," in *Concurrency and Computation: Practice and Experience*, vol. 31, 2019.

[28] F. Yan, L. G. Xing, Z. C. Zhang, "An improved certificateless signature scheme for iot-based mobile

payment," *International Journal of Network Security*, vol. 23, no. 5, pp. 904–913, 2021.

Biography

Liu Wanrong received her master's degree from Shanghai Ocean University in 2021. At present, she has worked in Shanghai Jiao Tong University Affiliated Sixth People's Hospital. Her main research is communication security and Internet of things technology.

Li Bin received his master's degree in NMR Analysis Center from East China Normal University in 1990. From 1990 to 1996, he worked in hospital and global medical equipment manufacture, and has been trained on MRI and CT technology four times in Japan and United States of American. From 1997 he has been in charge of device management and quality control of medical equipment in Shanghai Sixth people's hospital for 20 years. He authorized and co-authorized six books, published over 60 articles in national statistical source journal. He is the Vice-director of east-campus of Shanghai Sixth People's Hospital Affiliated to Shanghai Jiao Tong University now. His research interests include regional medical equipment management and quality control, assessment and management of medical equipment suppliers, management of service and rating of customer satisfaction, evaluation of medical imaging equipment performance and service system, and IOT and communication safety in medical technology management. Mr. Li is Director of Shanghai Quality Control Centre of Management of Medical Equipment, Chairman of Clinical Engineering Society of Chinese Medical Association, Vice Chairman of Clinical Engineers branch of Chinese medical doctor association, Council Member of Chinese society of Biomedical engineering, and Committee member of medical device classification technology of China SFDA. Coopted Member of Clinical Engineering Division of IFMBE.

Ji Zhiyong received his bachelor's degree from Nanjing University of Aeronautics and Astronautics in 2012. He received his MS degree Jiangsu University in 2017. He is the master's supervisor of mechanical engineering of Shanghai Ocean University. He is also the medical equipment senior engineer and deputy director of Shanghai Sixth People's Hospital East. His research directions include the development and application of wearable medical devices based on the Internet of things and the information security of the medical Internet of things.

Research on Network Intrusion Detection Based on Improved Machine Learning Method

Yan Jian[1], Liang Jian[2], and Xiaoyang Dong[3]
(Corresponding author: Yan Jian)
Henan Polytechnic, Zhengzhou, Henan 450014, China[1]
No. 210, Ping'an Avenue, Zhengdong New District, Zhengzhou, Henan 450014, China
Email: rhj995@yeah.net
Zhengzhou Vocational University of Information and Technology, Zhengzhou, Henan 450008, China[2]
Henan Logistics Vocational College, Zhengzhou, Henan 450000, China[3]
(Received Sept. 22, 2020; Revised and Accepted Mar. 12, 2022; First Online Apr. 27, 2022)

Abstract

With the development of the mobile network economy, wireless network security has attracted more and more attention from industry and scholars. In order to improve the security level of wireless networks, a wireless network intrusion detection model based on an improved ladder self-coding network is designed. The single classification SVM (support vector machine) algorithm is used to improve the classification effect of an upgraded joint classifier. The simulation test of the model shows that the overall detection accuracy of the model on the AWID-CLS data set is 98.75%, and the classification F1 indexes of flood attack and camouflage attack under small samples are 83.04% and 89.18%, respectively, which are significantly higher than the traditional wireless network intrusion detection algorithm. The experimental results show that the wireless network intrusion detection ability and attack type classification ability of the model are strong.

Keywords: Cascade Classifier; Machine Learning; Network Intrusion; Single Classification SVM; Wireless Network

1 Introduction

Since the opening of the era of mobile Internet, wireless network technology has developed rapidly and gradually become an indispensable part of modern human life. However, the subsequent wireless network security problems have obviously hindered the further promotion of this technology [12].

According to relevant media reports, the number of public WiFi in China will be about 800 million in 2020, of which nearly half will face the risk of network intrusion [10]. It can be seen that network intrusion has become a common Internet attack mode and poses a potential threat to user data, enterprise sensitive information and government information in various existing mobile Internet ecosystems. Therefore, in recent years, experts and scholars in academia and industry pay more and more attention to network security, and study various targeted protective measures.

However, there is less research on improving the existing in-depth learning methods for specific research problems and applying them to build intrusion information recognition model. Therefore, this time, the improved ladder self coding neural network is used to extract the dimensionality reduction features of network data, and the single classification SVM is used as the basic learner to build a cascade multi classifier to classify the dimensionality reduced data, so as to build an intelligent model for detecting wireless network intrusion information. After the completion of the model, the classic wireless network AWID-CLS data set is used to design simulation experiments to verify the detection effect of the model, and the classification accuracy, classification recall and F1 are used as the test indicators of its detection accuracy.

The specific improvement of the algorithm is to add sparse penalty coefficient to the optimization function of the unsupervised part of the stepped self coding neural network, so as to improve the generalization ability of the stepped self coding network and better deal with the wireless network data with complex correlation.

At the same time, in order to improve the classification effect of the model on identifying difficult samples, the supervised partial loss function of the stepped self coding network is modified to focal loss function. Moreover, the classifier of the model is also optimized. In view of the impact of the type imbalance in the intrusion detection task of wireless network on the classification accuracy of the model, the unsupervised learning single classification SVM algorithm is used as the basic learner to construct a cascade classifier. It can be seen that this research can provide some reference clues for the subsequent construc-

tion of a more practical and efficient wireless network intrusion detection system.

2 Related Works

Feature dimensionality reduction is a technology to reduce the feature redundancy and number of features of the original data set by screening features and fusing some features. The common ways of feature dimensionality reduction are feature screening and feature extraction. At present, some traditional machine learning algorithms can achieve better feature dimensionality reduction. At the same time, with the development of artificial intelligence technology, the popularity of applying deep learning algorithm to feature dimensionality reduction is gradually increasing.

Aiming at the problem of feature extraction of time series data, Christ *et al.* designed a feature processing application combining feature selection and data hypothesis testing using tsfresh toolkit in Python programming language, which improved the feature extraction speed of time series information [4].

In order to improve the analysis accuracy of human walking gait, Anwar team proposed an automatic gait feature extraction method by analyzing the relationship between the location of shoe prints and the changes of information collected by sensors, deployed it into Android applications, and selected 15 volunteers for gait test, The results show that this method improves the accuracy of gait recognition to 97.77% [2].

Zhou and other scholars proposed a fingerprint feature data extraction algorithm based on Wavelet and neural network, which effectively reduces the redundant information in the data used to train the fingerprint identification model. This algorithm is combined with the nearest neighbor algorithm to build a fingerprint identification system, and the fingerprint image is selected for training and testing.

The test results show that, The addition of the fingerprint extraction algorithm significantly enhances the robustness of the fingerprint identification system [15]. In order to reduce the negative impact of light intensity, expression and other factors on face recognition, Guo *et al.* designed an improved 3D face recognition algorithm.

The test results on Bosphorus data set show that this method can effectively extract the structural information of human face [5]. Jia *et al.* proposed an improved view invariant feature selector method for gait recognition, which improves the rationality of feature selection by introducing additional constraints. The evaluation results show that the gait recognition accuracy of this method is significantly higher than that of the previous method [8]. Cai team believes that high-dimensional data analysis is a challenge for researchers in the field of machine learning. They specifically discussed common feature selection methods and their application in machine learning models, and discussed the future challenges faced by feature selection Engineering [3].

Scholars at home and abroad have also done a lot of research in dealing with the classification task of category unbalanced data sets. In order to explore the impact of class imbalance data set on the classification accuracy of classifier, Thabtah *et al.* selected several classical machine learning and deep learning algorithms, trained and tested them with the data of various class imbalance degrees. Analyzing the test results, it is found that there is a convex correlation between the class imbalance rate of data set and classification accuracy [14].

Lee team on C4 The classification results of the decision tree under the improved ROC curve show that the area of the decision tree is the largest than that of the unbalanced decision tree, and the classification results of the improved ROC tree 5 better decision tree [11]. Liu *et al.* designed an integrated classifier based on SVM algorithm, in which sampling bagging is used to form a subset to train multiple base learners. Simulation test results show that the classification effect of this algorithm is better than that of classical SVM algorithm [13].

Hang's research team found that most of the faults during motor operation are related to bearings, and most of the collected motor fault data sets have serious label category imbalance problems. Therefore, they designed an improved clustering algorithm to improve the processing effect of a few oversampling techniques on category imbalance data sets, and designed simulation experiments,

The improved oversampling technology is combined with the classical machine learning algorithm to form a classification model to verify the effectiveness of this improvement. In order to increase the reliability of the conclusion, the experiment is repeated for many times. The results show that, The classification accuracy of the classifier combined with the improved clustering algorithm is significantly higher than that of the non improved classifier model [6].

From the above research results, it can be seen that on the one hand, the feature dimensionality reduction process is of great significance for processing data sets with redundant information, and its processing effect directly affects the performance of subsequent algorithms in classification or regression tasks. On the other hand, in addition to selecting reasonable and excellent feature dimensionality reduction methods, dealing with the category imbalance of the data set can also improve the working stability and performance of the model.

These two points are particularly important for the wireless network information detection model with serious data imbalance and a lot of redundant information, However, the research on using appropriate methods to deal with wireless network information and build intrusion detection model is still quite rare. Therefore, this research focuses on applying the improved deep learning and machine learning methods to wireless network information detection, in order to provide a certain reference direction for subsequent research.

3 Design of Network Intrusion Detection Model Integrating Improved Ladder Network and Improved Cascade Classifier

3.1 Design of Feature Extraction Algorithm Based on Stepped Self Encoder Network

Considering the characteristics of wireless network intrusion data, such as high redundancy and unbalanced categories, the wireless network intrusion detection model based on improved machine learning method designed in this study is mainly composed of three parts: data preprocessing, stepped self coding network and single classification SVM classifier, as shown in Figure 1.

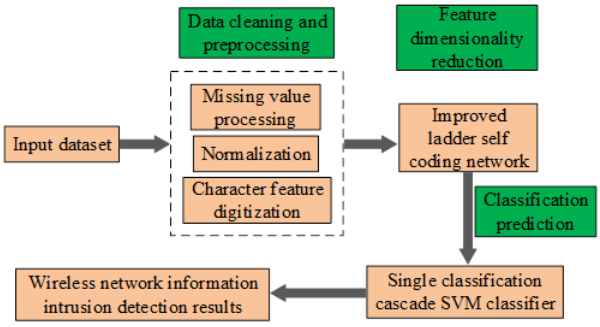


Figure 1: Schematic diagram of wireless network intrusion detection model based on improved machine learning method

As shown in Figure 1, the function of the data preprocessing module is to clean and process the messy original data into a form that can be recognized by the algorithm, and then input the feature extraction module to reduce the dimension of the huge data with a large amount of redundant information, so as to reduce the overall running time of the model and improve the accuracy of intrusion data monitoring, Then input the reduced dimension data into the cascade classifier based on single classification SVM for intrusion classification and detection of the data, and finally output the intrusion classification results of the original data. The specific content of data preprocessing is related to the characteristics of the data itself. It is introduced in the simulation experiment part. Here, the second part, feature dimensionality reduction, is designed.

Whether the scientific and reasonable feature dimensionality reduction of data can have a significant impact on the operation performance of network intrusion detection system. The data set with high core information retention and low feature redundancy can greatly improve the classification effect of intrusion detection classifier [9]. Considering the factors of redundant information and large correlation among features in network intrusion data, stepped self coding neural network is selected for feature extraction in this study. The classical ladder self coding network structure consists of supervised and unsupervised parts, as shown in Figure 2.

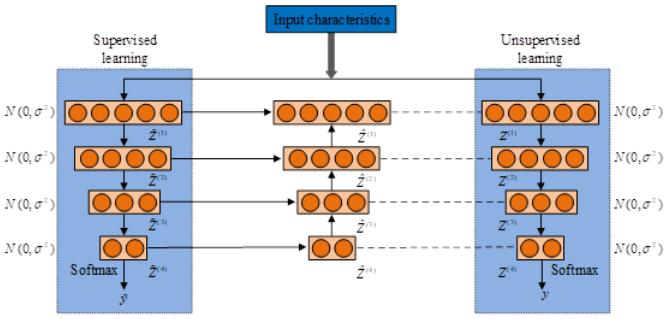


Figure 2: Classical ladder self coding network structure

It can be seen from Figure 2 that the inputs of the two parts of the classical ladder self coding network are completely consistent, but the unsupervised part does not use the data classification label, and the two parts share a set of parameters $W^{(l)}$. The coding feedforward sequence and decoding sequence of the supervised part are $\widetilde{Z}^{(1)} \rightarrow \widetilde{Z}^{(2)} \rightarrow \widetilde{Z}^{(3)} \rightarrow \widetilde{Z}^{(4)} \rightarrow \widetilde{y}$, $\hat{Z}^{(1)} \rightarrow \hat{Z}^{(2)} \rightarrow \hat{Z}^{(3)} \rightarrow \hat{Z}^{(4)}$, $\widetilde{Z}^{(l)}$ and $\hat{Z}^{(l)}$ respectively, representing the data after l layers of coding and decoding, and $\widetilde{y}$ is the prediction label. Moreover, random noise is added to each coding layer, and the original data is reconstructed in the decoding layer to improve the robustness of the system. The intrusion classifier is connected in the last coding layer to obtain $\widetilde{y}$ of the data, and the loss function of the model is the cross entropy function of $\widetilde{y}$ and the real label y^*. The feedforward order of the unsupervised part is $Z^{(1)} \rightarrow Z^{(2)} \rightarrow Z^{(3)} \rightarrow Z^{(4)} \rightarrow y$ without adding random noise. The Euclidean distance function value generated by the original data reconstructed by each layer of noise decoder is used as the loss function of this part. Therefore, the total loss function of stepped self coding network is as shown in the following formula:

$$Cos(t) = -\sum_{n=1}^{N} \log P(\widetilde{y_n} = y_n^* | X_n) + \sum_{n=1}^{N} \sum_{l=1}^{L} \lambda_l (Z_n^{(l)} - \hat{Z}_n{}^{(l)})^2$$

where N is the number of samples, L is the number of layers of the network, X_n is the eigenvector of sample n, and λ_l is the weight coefficient of the regular term. $Z_n^{(l)}$ and $\hat{Z}_n{}^{(l)}$ are the unsupervised output and decoded output of sample n at layer l, and the activation function before output is sigmoid function.

However, there are some deficiencies in the direct application of stepped self coding network to wireless network intrusion detection, so the stepped self coding network is improved. Firstly, the correlation between the features of wireless network data sets is complex, and the data changes in various ways, so the training model needs to

have stronger generalization ability. In this study, the sparse penalty term is added to the optimization function of the unsupervised part, so that the network can extract more sparse feature expressions in the unsupervised learning stage, so as to improve the generalization ability of the model. The selected sparse penalty term is KL (Kullback Leibler) divergence, and its calculation method is shown in Formula (1):

$$\varphi(t) = (1-\rho)\log\frac{1-\rho}{1-t} + \rho\log\frac{\rho}{t} \tag{1}$$

In Equation (1), $\varphi(t)$ is the KL divergence, ρ is the super parameter representing the sparsity of the model, $t = \frac{1}{n}\sum_{i=1}^{n} h_j^{(i)}$ represents the average output value of hidden layer neuron j on n training samples, and $h_j^{(i)}$ is the output of the j^{th} hidden layer neuron to sample i. The partial loss function of supervised learning with KL divergence sparse penalty term is shown in Equation (2):

$$Cos(t) = -\sum_{n=1}^{N}\log P(\widetilde{y_n} = y_n^*|X_n) + \sum_{n=1}^{N}\sum_{l=1}^{L}\lambda_l(Z_n^{(l)} - \hat{Z}_n{}^{(l)})^2 + \lambda\varphi \tag{2}$$

Secondly, the classical ladder self coding network has poor learning ability for difficult samples due to its own variation characteristics of softmax loss function, which leads to the low discrimination ability of the model between camouflage attack and normal behavior. To solve this problem, the loss function in the supervised stage is replaced by focal loss function L_{fl}, and its calculation method is shown in Formula (3):

$$L_{fl} = \begin{cases} -(y')^{\gamma}\log(1-y') & y=0 \\ -(1-y')^{\gamma}\log y' & y=1 \end{cases} \tag{3}$$

In Equation (3), y' is the probability that the sample is predicted to be the specified category, and γ is the super parameter to adjust the classification effect of difficult samples. The larger its value is, the greater the contribution of difficult samples to the loss value is, that is, the classification effect of the classifier on these samples is better. The total loss function of self coding network after replacing the supervised partial loss function with focal loss function is shown in Formula (4):

$$Cos(t) = L_{fl} + \sum_{n=1}^{N}\sum_{l=1}^{L}\lambda_l(Z_n^{(l)} - \hat{Z}_n{}^{(l)})^2 + \lambda\varphi \tag{4}$$

3.2 Cascade Classifier Design Based on Single Classification SVM Algorithm

After completing the design of feature extraction algorithm, the classifier of network intrusion data is designed. Because network intrusion detection belongs to multi classification task, and the correlation between normal behavior data and network attack data is complex and difficult to be described by linear relationship, mature SVM algorithm is selected to build cascaded SVM as the classifier of network intrusion detection model, and its structure is shown in Figure 3.

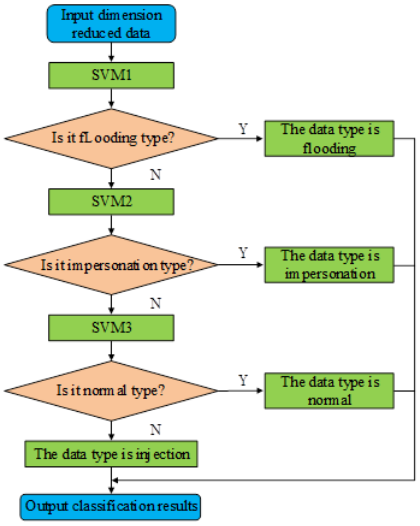


Figure 3: Structure diagram of cascaded SVM classifier

As shown in Figure 3, for the N-classification problem, only n-1 SVM classifiers need to be nested, and the algorithm complexity is low. Because the data set AWID-CLS used in the validation of this study has four types of labels (each classification label is flooding, impersonation, normal and injection), three SVM need to be set for the cascade classifier. The workflow of cascade classifier is that the data after feature dimensionality reduction is input into SVM1. If it is judged that the data is the record of flooding attack, it is marked as 0 and output, and the other data is marked as 1 and input into SVM2. SVM2 classifies and labels the impersonation data in the input as 0 and outputs it, and the other data is marked as 1 and input to svm3. Svm3 classifies the data into normal and injection. The former is marked as 0 and the latter is marked as 1.

In practical application, the data to be detected in the network intrusion data detection model often has serious category imbalance. For example, the ratio of normal data to offensive behavior data in the original data is usually greater than 10:1, even if the original data is input into the cascade classifier after data cleaning and feature dimensionality reduction, The upper SVM classifier in the model needs to treat all data except specific types as the same type, and the category imbalance is still serious [1]. Therefore, this time, the cascade classifier with the structure shown in Figure 3 is improved. The SVM 1 and SVM 2 basic classifiers in the model are replaced by single classification SVM, which is integrated into unsupervised classification learning to solve the problem of class imbalance in the data set, and other components and structures of the cascade classifier remain unchanged [7]. The workflow of the improved classifier is as follows. The data after feature dimensionality reduction is input into the single classification SVM classifier S1. Because the single clas-

Table 1: Data set label distribution before and after adjustment

Label	AWID-CLS-R-Trn	AWID-CLS-R-Tst	N-AWID-CLS-R-Trn	N-AWID-CLS-R-Tst
Flooding	48484	8097	48484	8097
Impersonation	48522	20079	48522	20079
Injection	65379	16682	65379	16682
Normal	1633190	530785	65328	21231

sification SVM algorithm is used to process unsupervised tasks, only the flooding attack data will be input into the cascade classifier as S1 for training S1, and this part does not need labels, Other data is used as the input of another single classification SVM classifier S2, and S2 will take the impersonation data in the remaining data as the training set, and other data will be output to the classical SVM basic classifier S3. Finally, S3 will train to divide the remaining data into normal data and injection data. Since the overall structure of the improved cascade classifier based on single classification SVM has not changed, the structure diagram of the classifier will not be drawn here.

4 Simulation Experiment Analysis of Improving Network Intrusion Detection Model

4.1 Model Building and Parameter Optimization

In this study, in order to test the performance of the designed network intrusion data detection model, the whole model is simulated. The data set used in the simulation experiment is the data subset AWID-CLS in AWID (Aegean Sea WiFi intrusion dataset). Most of the data in this data set are WiFi connection records obtained by various mobile devices at various times in a specific geographical range. There are four classification labels in the data set, namely, flooding, impersonation, injection and normal. The AWID-CLS-R-Trn and AWID-CLS-R-Tst data subsets in AWID-CLS are used as the training set and test set of the model respectively. See Table 1 for the distribution of various label data of the two.

It can be seen from table 1 that the sample distribution of the original training set and test set is extremely unbalanced, and the ratio of normal samples to network intrusion samples is about 10:1, which will lead to the detection network extracting more features of normal samples, thus affecting the operation results of the model. Therefore, combined with the operation characteristics of each basic classifier in the cascade classifier, 4% of the samples are extracted from the normal samples to form a new training set and test set N-AWID-CLS-R-Trn and N-AWID-CLS-R-Tst. The data distribution of the two sets is also listed in Table 1. Then, the original data are preprocessed by character feature digitization, missing value processing, normalization and other data processing. These are conventional processing methods, which will not be described in detail this time.

When the simulation detection model is built according to the design scheme, the computer environment processor is Intel (R) core i7-7700, the memory is 8GB, the hard disk is 2TB, the operating system is windows7 professional edition, and the programming language environment is Python 3 0 and its extension library. See Table 2 for the core parameter settings of the model.

4.2 Simulation Results of Improved Network Intrusion Detection Model

Firstly, the data processing effect of the ladder self coding network in the mobile network intrusion detection model designed in this study is verified. The network is selected followed by the cascade SVM classifier as the detection model (referred to as "LN + NSVM"), and then the common machine learning algorithms random forest, AdaBoost, naive Bayes XGBoost and the well-known deep learning trestle self coding network (SAE for short, designed as a two-layer structure with better effect, and the excitation function is prelu function) and resnext-50 are used as the comparison models. The preprocessed AWID-CLS data set of each model is trained and tested, and the statistical results of classification accuracy of each algorithm are obtained, as shown in Figure 4.

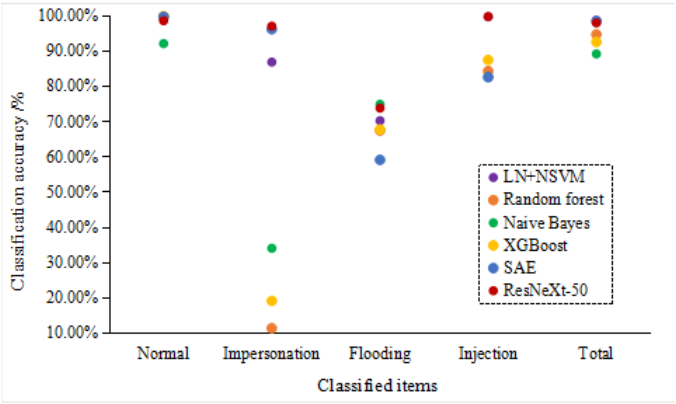


Figure 4: Classification accuracy of LN + NSVM model and comparison models

Table 2: Core parameters of simulation detection model

Parameter name	Explain	Set value or value rule	Setting basis
θ	Random Gaussian noise coefficient	0.012	Optimization
β	Neuron bias vector	Initialize to 0	Optimization
W_{ij}	Neuron weight vector	Xavier method initialization	Ensure that the variance of neuron input and output is the same
L_r	Training and learning rate of model	Initial to 0.006, then adjusted according to the training results of each round	After debugging for many times
Batch size	Number of single training samples	256	Optimization
Epoch	Number of iterations	13	Optimization
Hidden layer structure of self encoder network	/	95:70:35:4	Optimization
ρ	Sparse penalty coefficient	0.8	Optimization

It can be seen from Figure 4 that compared with the classical machine learning model, the LN + NSVM model has significantly higher detection accuracy for impersonation attack types, and the detection effect of normal type is slightly different, but the detection accuracy of flooding type is low. Compared with deep learning model, LN + NSVM model has poor detection effect on impression type, and the detection effect on other types of information is at the best or better level. On the whole, the classification accuracy of LN + NSVM model is the highest among all comparison algorithms, which is 98.77%. It shows that the improved ladder self coding network designed in the research can effectively extract and reduce the feature information in the original information and improve the detection ability of the model. Then compare the training speed of the model, as shown in Figure 5 Note that since the classification effect of the selected machine learning algorithm is significantly worse, only the deep learning model is selected for comparison, and in order to reasonably simplify the drawing of graphics, the model is sampled every 5 iterations.

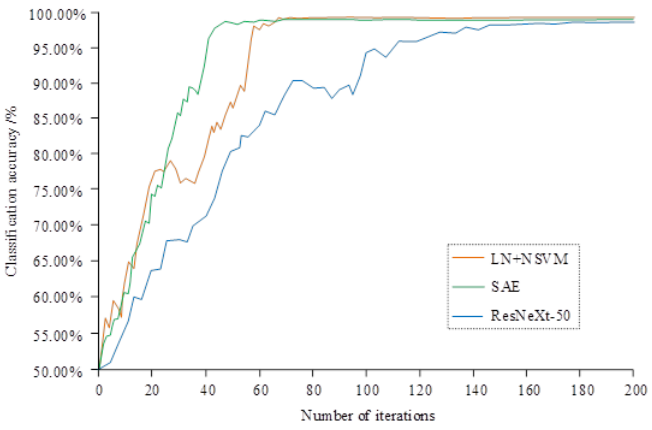


Figure 5: Training process of classification accuracy of LN + NSVM model and comparative deep learning model

It can be seen from Figure 5 that SAE model, LN + NSVM model and resnext-50 model begin to converge when the number of iterations reaches about 48, 67 and 175 respectively. The SAE model with the simplest network structure has the fastest training speed, followed by LN + NSVM model, but the difference is small. Then verify the impact of the improved single classification SVM cascade classifier on the classification effect of the detection model. Compare the LN + nsvm model with the complete improved classification and detection model (LN + NSSVM for short) designed in the research, and count the accuracy index comparison results of the two, as shown in Figure 6. In addition, in order to improve

the reliability of statistical results, each test scheme was carried out ten times in subsequent experiments.

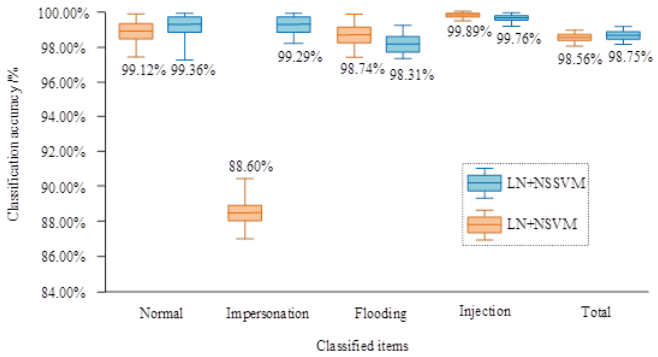


Figure 6: Comparison of classification accuracy between LN + NSVM model and LN + NSSVM model

It can be seen from Figure 6 that after using the single classification SVM cascade classifier, the median classification accuracy of the model in the type of camouflage attack is greatly improved from 88.60% to 99.29%, 12.07%, and there is little change in the recognition accuracy of other types of data. Take another look at the statistical results of the recall rate of the two models, as shown in Figure 7.

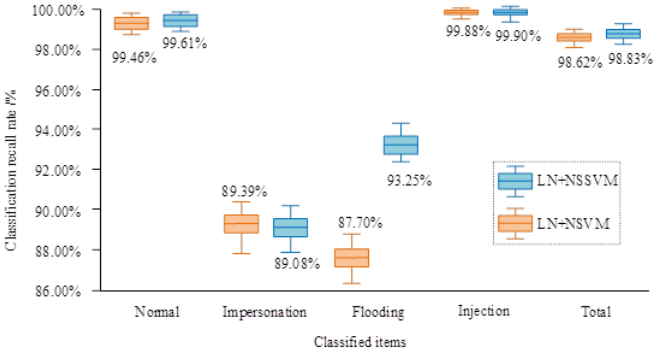


Figure 7: Comparison of classification recall rate between LN + NSVM model and LN + NSSVM model

According to Figure 7, the median recall rate of LN + NSSVM model for flooding attack detection is 93.25%, which is significantly higher than that of LN + NSVM model by 6.33%. There is little difference between the median recall rates of the two models in other information types, and the overall median recall rate of LN + NSSVM model is 98.83%, which is also higher than that of LN + NSVM model. Finally, the F1 index of the two models is analyzed.

It can be seen from the analysis of Figure 8 that the F1 values of LN + NSSVM model and LN + NSVM model in various types of information are slightly different, but the F1 average of the former in the overall data is 98.81%, which is higher than that of the latter. According to

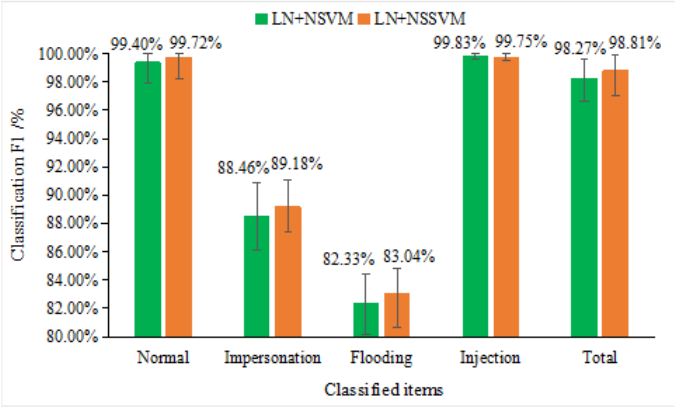


Figure 8: Comparison of classification F1 indicators between LN + NSVM model and LN + NSSVM model

Figures 6, 7 and 8 and their analysis contents, the use of cascade classifier based on single classification SVM is helpful to improve the information classification accuracy of the detection model.

5 Conclusion

Aiming at the problem that wireless networks are more vulnerable to intrusion than traditional wired networks, a wireless network intrusion detection model based on improved ladder self coding network and single classification SVM cascade classifier is designed. The simulation results show that the ladder self coding network makes the overall detection accuracy of the model to attack information better than the traditional machine learning model and the cutting-edge deep learning model, and the convergence speed of the model is faster. At the same time, on the basis of feature dimensionality reduction using stepped self coding network, the overall accuracy, recall and F1 indexes of the improved model with single classification SVM cascade classifier and the model with two classification SVM cascade classifier are 98.75%, 98.83%, 98.81% and 98.56%, 98.62% and 98.27% respectively. The former is better than the latter. The simulation results show that the detection model can effectively improve the detection accuracy of attack information in wireless networks.

References

[1] T. Alam, C. F. Ahmed, S. A. Zahin, M. A. Khan, M. T. Islam, "An effective recursive technique for multi-class classification and regression for imbalanced data," *IEEE Access*, vol. PP, no. 99, pp. 1-1, 2019.

[2] A. R. Anwary, H. Yu, M. Vassallo, "Optimal foot location for placing wearable IMU sensors and automatic feature extraction for gait analysis," *IEEE Sensors Journal*, vol. 2018, pp. 2555-2567, 2018.

[3] J. Cai, J. Luo, S. Wang, S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, no. jul.26, pp. 70-79, 2018.

[4] M. Christ, N. Braun, J. Neuffer, A. W. Kempa-Liehr, "Time series feature extraction on basis of scalable hypothesis tests (tsfresh – A Python package)," *Neurocomputing*, vol. 307, pp. 72-77, 2018.

[5] Y. Guo, R. Wei, Y. Liu, "Weighted gradient feature extraction based on multiscale sub-blocks for 3D facial recognition in bimodal images," *Information (Switzerland)*, vol. 9, no. 3, pp. 48-63, 2018.

[6] Q. Hang, J. Yang, L. Xing, "Diagnosis of rolling bearing based on classification for high dimensional unbalanced data," *IEEE Access*, vol. 7, no. 99, pp. 79159-79172, 2019.

[7] Y. Hou, L. Li, B. Li, J. Liu, "An anti-noise ensemble algorithm for imbalance classification," *Intelligent Data Analysis*, vol. 23, no. 6, pp. 1205-1217, 2019.

[8] N. Jia, S. Victor, C. T. Li, "On view-invariant gait recognition: a feature selection solution," *IET Biometrics*, vol. 7, no. 4, pp. 287-295, 2018.

[9] M. Koziarski, B. Krawczyk, M. Wozniak, "Radial-based undersampling for imbalanced data classification," *Neurocomputing*, vol. 343, no. MAY 28, pp. 19-33, 2019.

[10] M. Lango, J. Stefanowski, "Multi-class and feature selection extensions of roughly balanced bagging for imbalanced data," *Journal of Intelligent Information Systems*, vol. 50, no. 1, pp. 97-127, 2018.

[11] J. S. Lee, "AUC4.5: AUC-based C4.5 decision tree algorithm for imbalanced data classification," *IEEE Access*, vol. 7, no. 7, pp. 106034-106042, 2019.

[12] P. Li, L. Yin, B. Zhao, Y. Sun, "Virtual screening of drug proteins based on imbalance data mining," *Mathematical Problems in Engineering*, vol. 2021, no. 16, pp. 1-10, 2021.

[13] H. Liu, Z. Liu, W. Jia, D. Zhang, J. Tan, "A novel imbalanced data classification method based on weakly supervised learning for fault diagnosis," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1-1, 2021.

[14] F. Thabtah, S. Hammoud, F. Kamalov, A. Gonsalves, "Data imbalance in classification: Experimental evaluation - ScienceDirect," *Information Sciences*, vol. 513, no. 3, pp. 429-441, 2020.

[15] L. Zhou, C. Zhang, Z. Wang, Y. Wang, Z. Lu, "Hierarchical palmprint feature extraction and recognition based on multi-wavelets and complex network," *IET Image Processing*, vol. 12, no. 6, pp. 985-992, 2018.

Biography

Yan Jian, born in Tianmen, Hubei, China, has graduated from Northeastern University in 2008 and gained the postgraduate degree. Now she works in Henan Polytechnic. She is a lecturer. She is interested in network security and intrusion detection.

Liang Jian, born in Tianmen, Hubei, China, has graduated from Zhengzhou University of Aeronautics in 2017 and gained the postgraduate degree. Now he works in Zhengzhou Vocational University Information and Technology. He is a teaching assistant. He is interested in advanced manufacturing.

Xiaoyang Dong, born in Luoyang, Henan, China, has graduated from Zhengzhou University of Aeronautics in 2017 and gained the postgraduate degree. Now she works in Henan Logistics Vocational College. She is a teaching assistant. She is interested in big data and mathematical modeling.

Research on the Trusted Online Examination Systems

Anthony Y. H. Liao[1], Yu-Ying Hsieh[2], Cheng-Ying Yang[3], and Min-Shiang Hwang[1,4]
(Corresponding author: Min-Shiang Hwang)

Department of M-Commerce and Multimedia Applications, Asia University[1]
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Rd., Taichung 41354, Taiwan (R.O.C.)
Department of Computer Science, University of Taipei[3]
Taipei 10048, Taiwan (R.O.C.)
Department of Medical Research, China Medical University Hospital, China Medical University[4]
No. 91, Xueshi Rd., Taichung 40402, Taiwan (R.O.C.)
Email: mshwang@asia.edu.tw
(Received Sept. 22, 2020; Revised and Accepted Apr. 12, 2022; First Online Apr. 30, 2022)

Abstract

In recent years, due to the threat of the new crown pneumonia (Covid-19), to avoid cluster infections, the way of online teaching has rapidly formed a trend. To maintain the authenticity and fairness of exams, teachers in many colleges and universities have formulated various solutions for students cheating in online exams. Therefore, cheating methods and proctoring techniques have become the two most important issues in online teaching. This paper collects and analyzes relevant literature on online cheating and online proctoring techniques from 2015 to 2022. We concluded that personal and environmental factors mainly influenced why students cheated. Most types of cheating are plagiarism, plagiarism, collusion, and imposter. Teachers do their best to prevent students from cheating. Electronic monitoring, authentication, and change assessment methods are the most common method. However, no matter which method is used, it cannot obtain satisfactory results. Other academics object to using technology or methods to control student exams. Return to the essence of education and cultivate talents who can manage themselves. Such arguments are not an immediate solution to the current problem of cheating on online exams. This paper synthesizes the opinions and practices of various works of literature and argues that adopting multiple evaluation methods is the closest approach to fairness and effectiveness. The essence of education is to guide value creation, cultivate ethical thinking, and acquire knowledge and ability. It is also necessary to rely on the advancement of information technology to improve the design of learning management systems (LMS) to break through the blind spots of current online exam cheating and proctoring techniques.

Keywords: Learning Management Systems (LMS); Online Examination; Online Proctoring Techniques

1 Introduction

Exams are a practice necessary to understand learning outcomes. Unfortunately, the exam is unfair due to students cheating during the online exam process [21]. However, with the advancement of information technology, more and more people use online teaching methods. Because online teaching has many advantages that traditional classrooms do not have, the implementation of online teaching has become a symbol of progress in the corporate world and educational institutions [28]. Especially since the 2019 Covid-19 pandemic, higher education institutions worldwide have moved to teach online. Online teaching has become an inevitable trend. But the ensuing problems have aroused public attention and discussions among scholars. The focus is on a fair and accurate assessment of student performance [14].

Cheating on exams can lead to false assessments of learning outcomes, raising questions about the value of online courses [2] and the credibility of institutions [3]. And waste a lot of time and resources on the purpose of quality education [4]. Moreover, it has a significant impact on the future development of individuals and schools. Therefore, many scholars have devoted themselves to studying the influencing factors of student cheating and finding ways to deal with it.

1.1 Reasons Why Students Cheat

The first job in addressing cheating is understanding why students cheat, including analyzing students' attitudes and perceptions. The reasons why students cheat on exams are very complex. Some scholars have pointed

Table 1: Reasons for cheating in online exams

Scholar	Reasons for cheating on online exams
Crown & Spiller [17]	1. Personal factors: personality traits, attitudes, ideas. 2. Environmental factors: It is easy to use information equipment to cheat, be influenced by others, have high-grade pressure, and lack invigilation skills.
Yang *et al.* [37]	1. Not interested in the subject. 2. Not ready. 3. The feeling of rampant cheating. 4. No punishment even if found.
Becker *et al.* [8]	The fraud triangle: Pressure, opportunity, self-rationalization.
Dendir & Maxwell [18]	Students find it easier to cheat online than in brick-and-mortar classes. Justify cheating with "it didn't hurt anyone."
Mellar *et al.* [30]	Procrastination, laziness, and reluctance to work hard.
Amigud *et al.* [3], Ghizlane *et al.* [22], Gamage *et al.* [20]	Fear of failure, ability, cultural background

out that the factors that cause students to cheat can be divided into personal and environmental factors. Individual factors refer to personality traits, attitudes, and beliefs. Environmental factors include ease of cheating, being influenced by others, grade pressure, poor proctoring skills, lack of interest or preparation for the subject, the perception that cheating is rampant and not punished—the concept of punishment [17]. From a corporate perspective, Becker *et al.* [8] use the fraud triangle proposed by Cressey [15] to explain students' cheating behavior: pressure, opportunity, and self-rationalization are all three factors that motivate cheating behavior, and all induce cheating behavior in students [8]. This view is also consistent with the arguments of the literature mentioned above. Dendir and Maxwell stated that students find it easier to cheat in online exams than in physics courses [18]. Most of them have some dishonesty during the online exam. They justified their cheating by saying they "did not harm in any way". Some scholars believe that students' procrastination and laziness are also the reasons for cheating [30]. Other factors, such as fear of failure [22], ability [3], and cultural background [20], also influence students' decisions to cheat. The reasons for cheating in online exams are shown in Table 1.

From the viewpoints of literatures and observing the current practical situation, it is confident that cheating in online exams will continue to occur in the short term. Therefore, understanding the cheating methods commonly used by students and formulating strategies to eliminate cheating behaviors is the direction of the current online examination invigilation technology.

1.2 Common Cheating Methods in Online Exams

There is no fixed pattern of cheating patterns among students, and it often varies with the external environment. It is more accessible to cheating, especially in online exams with insufficient or no proctoring skills. Based on Garga & Goel's research on this issue, five categories of cheating are proposed, including impersonation, prohibited aids, collusion, plagiarism, and game systems [21]. Peled *et al.* also pointed out that looking for online resources, communicating with others, and taking exams for others are the most common ways of cheating [33]. Other scholars have pointed out that identity misrepresentation [25], the use of unauthorized resources [16], collusion [6], and plagiarism [34] are also commonly used cheating methods by students.

The availability of the internet provides students with multiple opportunities for cheating. Students collaborate through apps such as Line, WhatsApp, Email, and more to find answers on the internet. Even interact with dedicated subject experts [29]. Students use to cheat, including desktops, laptops, tablets, and cell phones. Among them, smartphones are the most common. Based on the research results of scholars, the standard cheating methods in online exams are listed as shown in Table 2.

1.3 Evaluation of Anti-Fraud Technology of Safe Online Examination System

Invigilation techniques to prevent or eliminate cheating in online exams have become part of online teaching. More and more technology and equipment are being put into proctoring strategies for online exams. Many scholars have researched the technical issues of online proctoring and put forward their views. Although it can achieve part of the anti-fraud effect, it has the shortcomings of taking care of one and the other.

Garga & Goel researched which strategies are used to tackle cheating on online exams. There are seven categories: examination method, integrity strategy, computer lock, identity verification tool, author identification, proc-

Table 2: Common cheating methods in online exams

Scholar	Common cheating methods in online exams
Garga & Goel [21]	Impersonation, Prohibited Aids, Collusion, Plagiarism, and Gaming Systems.
Peled *et al.* [33]	Find online resources, communicate with others, and even test for others.
Mungai and Huang [31]	Identity misrepresentation
Hylton. *et al.* [25]	Use unauthorized resources
Crook and Nixon [16]	Complicity
Awasthi [6] & Husain *et al.* [24]	Plagiarism
Rogerson & McCarthy [34]	Collaborate through social networks like Line, WhatsApp, and apps like email, find answers on the Internet and interact with dedicated subject matter experts.

toring, and data analysis [21]. The study pointed out that online proctoring can be divided into manual, fully automatic, and semi-automatic [29]. Manual proctoring refers to monitoring the exam process by an invigilator watching, in real-time or on video. Fully automated proctoring utilizes IT automation technology to analyze students during exams to detect cheating. For example, using facial recognition to authenticate students and estimate where they are looking is fully automated monitoring [5]. Finally, semi-automated proctoring combines the detection of automated methods with manual confirmation by the proctor. For example, some online exams use Secure Exam Browser (SEB) software that prevents students from searching or sharing answers during the exam. However, it does not provide detection capabilities, and students must still submit answers to the Learning Management System (LMS). But other proctoring software uses Artificial Intelligence (AI) and machines to identify suspicious behavior when examining online test records [13]. While teaching institutions find these benefits of online proctoring very appealing, students often complain about the uncomfortable feeling of being watched, and their privacy invaded [23]. It's also important to note that as online proctoring software improves, students find new ways to circumvent surveillance by such platforms [10].

During the Covid-19 pandemic, a South Korean university drew up and introduced a "Student Honor Code" to slow down online cheating [28]. And require all students to sign the code at the beginning of each semester. Students promise that they will not cheat on exams or engage in any academic dishonesty through this practice. At the same time, teaching institutions used the invigilation system to record, and they found that the university alleviated the cheating problem to a certain extent in the subsequent semesters [27]. Another study by Trezise *et al.* used an unsupervised clustering method to identify writing patterns to distinguish between students' work or work copied from other sources. Machine learning algorithms (MLA) are also used to detect other forms of cheating [36].

By sorting the above literature, we can find that different invigilation method prevent fraud, but each has its shortcomings. Based on the analysis of Garga & Goel [21], this paper organizes the papers published after sorting out the literature and organizes the main fraud prevention methods, as shown in Table 3.

1.4 Research on Cheating and Proctoring Techniques in Online Exams

Scholars have never stopped researching online exam cheating behaviors and proctoring techniques. However, there are not many related papers published. Until the Covid-19 pandemic quickly shifted the traditional face-to-face teaching method to online, online cheating by students has caused concern among schools and teachers. Therefore, many scholars began to invest in research on related topics. In order to understand the research situation of scholars, this article collects relevant literature as much as possible through journals, seminar result books, collections of papers, books, research reports, and Internet materials. Nine studies from 2020 to 2022 were selected as primary literature. For the convenience of future reference, they are arranged in the order of publication time, as shown in Table 4.

1.5 The Organizational Structure of this Article

The issues discussed in this article are related to online exam cheating behavior and cheating strategies. To understand the relevant issues' background facts, theoretical developments, and future research directions, we will discuss that. First of all, we collect relevant domestic and foreign literature in order to explore scholars' views and research on related issues. Then, use the literature analysis method to carry out an objective analysis and presentation and infer its impact on the whole issue. The literature is organized into three key points and discussed separately: the causes of students' cheating in online exams, the common cheating methods in online exams, and the strategies for preventing cheating and invigilation techniques. In addition, in order to keep the data consistent with the actual situation, the data collected in this paper are mainly papers and research reports after

Table 3: Comparison of anti-fraud techniques for secure online examination systems

Fraud prevention strategy	Mode of operation
Examinations	Randomized questions, instant responses, exam question banks, group assignments, oral presentations, progressive assignments, open-book exams, strict submission deadlines, and feedback delays.
Integrity Policy	Explain what cheating constitutes, how it is monitored, and the consequences, and develop an effective integrity policy, such as Honor Code, Integrity Commitment, and Advocacy for students to sign.
Computer Lock	Lock the browser, keyboard shortcuts (copy, paste, print, and screenshot), and access other applications. Including messaging, screen sharing, virtual machines, and remote desktops are all prohibited.
Authentication Tool	Authentication is securing a student's identity by validating their credentials to prevent misrepresentation. There are three ways to verify passwords, challenge questions and biometrics.
Authorship Tool	Confirm that students do what they claim to do. It is divided into three methods: plagiarism detection tools, teacher verification, and behavioral biometrics.
Online Proctoring	1. Manual invigilation: The invigilator will watch the real-time or recorded video of the examination process. 2. Fully automatic invigilation: Using automated technologies such as machine learning, Analyze students to detect cheating, such as facial recognition. 3. Semi-automatic invigilation: Combines the detection of automated methods and the further hands-on invigilators to confirm.
Data Analysis	Leverage machine learning methods to analyze student interactions with online learning environments, including platforms, content, peers, and teachers. And generate a large amount of data. For example, through analysis, you can obtain time records of questions, responses, submissions, etc., and can also analyze IP addresses and similar answers.

Table 4: Important research on cheating and proctoring techniques in online exams

Year	Author	Research topic
2020	Dendir & Maxwell [18]	Cheating in online courses: Evidence from online proctoring
2020	Gamage *et al.* [20]	Online delivery and assessment during COVID-19: safeguarding academic integrity
2021	Coghlan *et al.* [14]	Good proctor or 'big brother? Ethics of online exam supervision technologies
2021	Li *et al.* [29]	A visual analytics approach to facilitate the proctoring of online exams
2021	Hubler [23]	Keeping online testing honest? Or an Orwellian overreach?
2022	Garga & Goel [21]	A systematic literature review on online assessment security: Current challenges and integrity strategies
2022	Lee & Fanguy [27]	Online exam proctoring technologies: Educational innovation or deterioration?
2022	Schneider *et al.* [35]	Towards trustworthy autograding of short, multi lingual, multi type answers
2022	Jiang & Huang [26]	Effective and efficient strategies and their technological implementations to reduce plagiarism and collusions in non-proctored online exams

the outbreak of the epidemic in 2019 and refer to previous relevant literature. Therefore, the data are divided into thesis writings, research reports, and network data. After sorting and analyzing and comparing its advantages and disadvantages (the architecture is shown in Figure 1), a conclusion is finally made.

2 Discussion on Related Research

Given the issues to be discussed in this article, four new papers published in 2022 are selected from Table 4. Further discussion and analysis are made with these articles' viewpoints and suggested specific practices.

2.1 Analysis of the Reasons for Cheating in Online Exams

In Garga & Goel's literature [21], the reasons that affect online cheating behavior are divided into two categories: personal factors and environmental factors. Personal factors include individual characteristics and motivations unique to each student, such as different personality traits, conscientiousness, emotional stability, extroversion, self-discipline, and imitation of relevant experiences. In addition, according to Garga & Goel, citing research results of other scholars 1, it is believed that the fear of failure and personal ability also influence students' decision to cheat. According to their observations, many factors related to the curriculum include excessive workload, challenging tasks, strict time requirements, poor curriculum design, lack of teacher-student interaction, lack of awareness of the school's integrity policy, and the convenience of the Internet etc. Therefore, it may be the reason why students cheat. In the research results, Lee & Fanguy believed that students' cheating was because universities and teachers were under enormous pressure, and the management method of online examinations was not well-prepared [27]. In addition, factors such as using the same tools as physical teaching, etc., led to students' cheating increase in number. After analyzing the literature, it is believed that academic dishonesty can occur for various reasons, including disinterest in the subject, unpreparedness, a sense that cheating is rampant, and the notion that such behavior will not be punished if detected.

Becker *et al.* originally applied the fraud triangle theory from the business domain to explain the motivation, incentive, opportunity, and rationalization of cheating behavior [8]. Many studies have pointed out that motivation results from internal and external pressure. For example, expectations from others, challenging classes, and heavy workloads can all induce incentives to cheat. Opportunity refers to the occurrence of student cheating due to insufficient mechanisms. For example, lack of proctoring skills, lack of clear exam rules, and penalties. The final factor, rationalization, refers to students' belief that dishonesty does not violate their moral values. Schneider *et al.* believe that the imperfect design and scoring of exams is one of the reasons for student cheating [35]. The shortcomings of machinery and surveillance technology and the independence of the environment provide students with convenient opportunities for cheating. In addition, society has always evaluated students based on the merits of their grades, resulting in the pressure of competition for grades, which is also a factor that triggers cheating. Jiang & Huang believe that the design of relevant software, the planning and management of examination methods, and the scoring method will all lead to students' cheating behavior [26].

2.2 Discussion on the Types of Cheating Behaviors

Regarding the ways of online cheating, Garga & Goel identified impersonation, prohibited aids, collusion, plagiarism, and game systems as the five most common ways [21]. The so-called impersonation means pretending to be someone else's identity or taking the exam on someone else's behalf. Prohibited aids refer to students referencing various unauthorized references, including notes, books, etc., or using unapproved technical tools during the exam—for example, cell phones, calculators, and headphones. Collusion means cooperation, which means students use cell phones, phone calls, instant messages, or emails to get answers. Plagiarism means that students plagiarize the content of an article by copying ideas, word substitution, grammar changes, reordering, paraphrasing, and spelling after searching for relevant answers on the Internet. The last one is the game system. Students are dishonest by exploiting the features of the Learning Management System in order to succeed in exams. This practice is called a gaming system. The methods used include instant feedback, prompts, multiple attempts, and multiple accounts. Jiang & Huang also pointed out that plagiarism and collusion in exams are the most common cheating methods used by students [26].

2.3 Discussion of Anti-fraud Strategies

Finally, we discuss the views of these four kinds of literature on fraud prevention. Garga & Goel's literature [21] proposed a solution to cheating in exams. The first is the technical aspect of test design, and it is believed that different test methods can minimize the chance of cheating in online tests. For example, randomization of questions [12] and responses [2]. Even exam question banks prevent students from sharing answers during the exam [1]. The literature also proposed using methods such as group assignments, oral presentations, progressive assignments, and open-book exams instead of traditional paper-based exams. For other types of assessments [33], it is considered difficult for students to cheat using these methods. The second is the web-page browser lock, the Secure Exam Browser (SEB) [12]. During the lockdown, various keyboard shortcuts such as copy, paste, screenshot, transfer, search, and other applications are

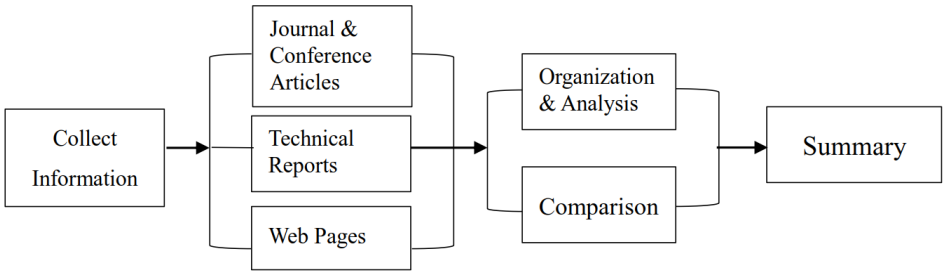


Figure 1: The structure of this study

disabled until the exam deadline. The third approach is the integrity policy [9]—which outlines what constitutes cheating, monitoring, and consequences. Having an effective integrity policy and raising awareness about it can prevent cheating from happening in the first place. The fourth method is authentication and author identification [22]. Ensure student identity by verifying student credentials. Numerous studies have used a variety of biological feature identification methods. For example: Face recognition [22], speech recognition [30], and fingerprint recognition [30] to verify student identity. The last one is data analysis [11]. They analyze student interactions with the platform, peers, and teachers throughout the process, generating massive amounts of data. We can analyze this data to draw clear conclusions and serve as the basis for cheat detection.

Lee & Fanguy studied the online exam questions of a university in South Korea and found that teachers used monitors, SEB, and physiological recognition systems to prevent students from cheating and achieved good results [27]. Many teachers and students report a dramatic reduction in cheating. They were delighted with the results of online proctoring. But some teachers feel that using these proctoring systems can cause students to feel uncomfortable being watched and suspected. Schneider *et al.* did not put forward a specific point of view on the invigilation system [35]. However, they believed that in the form of short, multi-language, multi-type answers, with the assistance of artificial intelligence, using an automatic scoring system to detect students' high-level answers can make the correct test fair. Azad *et al.* investigated the manual way to compensate for the inadequacy of automatic scoring during the actual exam [7]. Their approach is to have students try multiple times to reduce the error rate of automatic grading. Regarding how to prevent students from cheating in online exams, Jiang & Huang pointed out in the paper some practical strategies and techniques to reduce plagiarism and collusion in unproctored online exams that effective deployment, exam management, answer retrieval, and automatic scoring Such strategies should be sufficient to eliminate plagiarism and collusion [26]. The online examination strategies they proposed are: Adopting an asynchronous examination method, distributing examination papers with different contents to students, strictly limiting the submission of answers within the shortest time, and prohibiting returning and modifying the submitted answers to reduce the desire of students to plagiarize or reduce the chance of collaboration.

3 Analysis and Comparison

3.1 Analysis of the Related Works

From the above four works of literature and research data, it is found that maintaining the fairness of the test and the correctness of the results is the goal of teachers and the expectations of students. Comprehensively sorting out the content of each literature, summarizing the reasons for students cheating in online exams and the methods of cheating are similar. However, the strategies adopted by teachers and schools to prevent fraud are different.

Garga & Goel proposed seven prevention strategies and advocated that schools should start from the design of examination methods [21]. For example, methods such as randomization of questions, progressive assignments, immediate responses or oral presentations, and strategies for integrity (such as integrity policies, which promote a code of honor for students, etc.), emphasis on the nature of education, and de-emphasis on grades, will naturally Reduce cheating.

We also found that Lee *et al.* have different attitudes towards online proctoring [27, 28]. They believe that the root of the online exam proctoring system is the education in question, and it is a teacher-centered authoritarian education method. It causes the dualization of teachers and students and harms the teaching relationship and educational achievements. They use Foucault's theory of discipline to analyze the reasons for students' cheating [19]. He points to encouragement, opportunity, and self-rationalization as motivations for cheating. Therefore, schools should formulate effective policies, design a well-designed examination environment, and reduce the pressure on student performance is the fundamental way to eliminate cheating.

Schneider *et al.* mainly analyze the short use of multilingual and multi-type answers. They emphasize using simple logistic regression models for automatic grading and automatic scoring. Finally, manual inspection is used to reduce the error rate of scoring. They utilize multilin-

gual versions for bidirectional encoding. Use the k-means clustering algorithm to cluster the answers, and then use the natural language processing (NLP) of AI technology to score automatically.

Jiang & Huang argue that active advocacy aims to defeat potential student plagiarism or collusion [26]. They propose to do this in an unproctored way. They propose asynchronous examination and sub-item answering and strictly allocated answering time, effective deployment, examination management, answer retrieval, and scoring mechanism.

3.2 Comparison of the Related Works

After analyzing the central claims of the above four works of literature, compare their advantages and disadvantages, as shown in Table 5.

The following points are summarized: Although Garga & Goel specifically reveals students' diverse cheating methods [21], it is helpful to understand the loopholes in preventing cheating. It is believed that schools and teachers should establish a perfect anti-cheating mechanism and give students an excuse to rationalize their cheating behavior. Lee believes that students' test scores are not the only measure of learning effectiveness [28]. Society's expectations for students should return to the nature and purpose of education. Eliminate exam cheating with sound policies. This point of view directly points out the society's distortion of the meaning of education, but educating students until they don't cheat and society no longer pays attention to test scores is an ideal that requires long-term evolution and is challenging to achieve in the short term.

Schneider *et al.* focus almost exclusively on how to score, so that test scores are fair [35]. Although the use of advanced machine technology can significantly reduce grading error, it ignores the meaning of education. Some encourage teachers to establish a grade-based education direction but lack constructive education and learning quality suggestions. It is the most significant disadvantage. Jiang & Huang put forward many specific methods from the design of the test method and the scoring mechanism [26]. Although these anti-cheating methods can effectively defeat plagiarism and collusion cheating and promote the actual fairness of the test results, like Schneider and others' performance-oriented viewpoints, they ignore the value of humanistic thinking and education [35].

4 Future Research Topics

This article explores online exam cheating, the types of cheating, and anti-cheating strategies using literature analysis. In order to maintain the authenticity of the information and the current educational situation, and in line with the current background factors, we discarded many precious documents with the reference value in the process of selecting documents. After a detailed reading of all the collected literature, although most scholars study the problems of online exams, the discussion focuses on how to prevent or detect cheating through various effective techniques. But this technology is not ideal. An ideal trusted online exam system should meet the following requirements:

1) Security: Prevent impersonation and illegal means to obtain answers.

2) Convenience: No additional complicated equipment is required.

3) User Friendly: Easy to use and operate.

In order to satisfy the above requirements, we propose the following future research:

Topic 1 - Dynamic Biometric Authentication:
Remote identification is required to prevent impersonation. It is easy for an imposter to substitute a password or certificate (such as a smart card) for their identity. A student's identity can only be ensured by identifying the student through biometrics (such as fingerprints, face, eye prints, etc.). Fingerprints are not suitable for remote identification. Eyeprint devices are too complicated. At this stage, face recognition is the leading remote identification. But faces can easily be replaced by photos or models and can be tricked by verification — dynamic biometric authentication, which requires random facial expressions to ensure student identity.

Topic 2 - Effective Surveillance Technology:
Although locking the browser and keyboard can prevent students from sending messages online, students can still send messages through other devices (such as mobile phones or other computers).

Topic 3 - Unforgeable Evidence of Cheating:
Accusing a student of cheating requires evidence. Therefore, ensuring that evidence is not falsified is an important research topic.

5 Conclusion

The threat of Covid-19 persists, and online teaching is still the most popular way to teach. Although the methods proposed in various works of literature can eliminate some of the problems of online examinations, they cannot entirely and effectively solve all the various problems existing in the examinations. The current policies and technologies are necessary until educational institutions and teachers can find better solutions. But these are only temporary solutions. The type of online teaching will not change in the short term, and the behavior of cheating in online exams will not disappear, which is more likely to force students to develop more ways to avoid proctoring.

Table 5: Comparison of literature on online exams

Author	Main content	Advantage	Shortcoming
Garga & Goel [21]	The body reveals the diverse ways of cheating among students. Therefore, it is believed that schools and teachers should establish a perfect anti-fraud mechanism.	It helps to understand the loopholes that prevent fraud. In addition, there are references to provide fraud prevention techniques.	Feelings of rationalizing cheating may mislead students about cheating.
Lee & Fanguy [27, 28]	It is believed that students' test scores are not the only measure of learning effectiveness. Therefore, society's expectations for students should return to the nature and purpose of education.	This point of view directly points to society's distortion of the meaning of education. It helps to establish a correct concept of the value and purpose of education.	The change of concept is an ideal that requires long-term evolution. It is difficult to achieve in the short term and cannot solve the current problem.
Schneider *et al.* [35]	The focus is almost entirely on how to grade, so that test scores are fair and reasonable. Emphasize the correctness of the rating.	Using advanced machine technology can significantly reduce errors in scoring.	Teachers are encouraged to establish a grade-based approach—lack constructive advice on the quality of education and learning.
Jiang & Huang [26]	The design of the test method and the scoring mechanism proposes progress and specific strategies such as effective deployment, test management, answer retrieval, and scoring mechanism.	It can effectively prevent plagiarism and collusion cheating and promote the fundamental fairness and justice of the test results.	Encouraging a performance-oriented perspective ignores human-centered thinking and the actual value of education.

Cheating is not just a superficial exam problem but an issue that needs to be reviewed for the entire educational policy and educational concept. Schools or teachers should not spend a lot of energy and money exploring the problems of cheating and invigilation but ignore the root causes of these problems. Instead, it should be a student-centered structure based on educational theory, integrating textbook design, teaching methods, roll call modules, online testing, and educational environment planning. And through professional training to enhance the teaching effectiveness of teachers so that teaching can meet the learning needs of students. On the other hand, teaching situations should be based on people-oriented thinking, establish interpersonal relationships of mutual trust and mutual respect, use multiple assessment methods to test students' learning effects, and use incentive and enhancement technology to improve Students' motivation to learn.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 109-2221-E-468-011-MY3, MOST 108-2410-H-468-023, and MOST 108-2622-8-468-001-TM1.

References

[1] H. M. Alessio, N. Malay, K. Maurer, A. J. Bailer, B. Rubin, "Interaction of proctoring and student major on online test performance," *The International Review of Research in Open and Distributed Learning*, vol. 19, no. 5, pp. 166–185, 2018.

[2] G. Alexandron, J. A. Ruip´erez-Valiente, Z. Chen, P. J. ˜Muñoz-Merino, D. E. Pritchard, "Copying@Scale: ˜Using harvesting accounts for collecting correct answers in a MOOC," *Computers & Education*, vol. 108, pp. 96–114, 2017.

[3] A. Amigud, J. Arnedo-Moreno, T. Daradoumis, A. E. Guerrero-Roldan, "An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives," *Computers & Security*, vol. 76, pp. 50–70, 2018.

[4] I. J. M. Arnold, "Cheating at online formative tests: does it pay off?," *The Internet and Higher Education*, vol. 29, pp. 98–106, 2016.

[5] H. S. G. Asep, Y. Bandung, "A design of continuous user verification for online exam proctoring on M-learning," in *Proceedings of the International Conference on Electrical Engineering and Informatics*, pp. 284–289, 2019.

[6] S. Awasthi, "Plagiarism and academic misconduct: A systematic review," *DESIDOC Journal of Library & Information Technology*, vol. 39, no. 2, pp. 94-100, 2019.

[7] S. Azad, B. Chen, M. Fowler, M. West, C. Zilles, "Strategies for deploying unreliable AI graders in high-transparency high-stakes exams," in *International Conference on Artificial Intelligence in Education, Lecture Notes in Computer Science*, vol. 12163, Springer, 2020.

[8] D. Becker, J. Connolly, P. Lentz, J. Morrison, "Using the business fraud triangle to predict academic dishonesty among business students," *Academy of Educational Leadership Journal*, vol. 10, no. 1, pp. 37–54, 2006.

[9] L. Benson, K. Rodier, R. Enstr¨om, E. Bocatto, "Developing a university-wide academic integrity e-learning tutorial: A Canadian case," *International Journal for Educational Integrity*, vol. 15, no. 1, pp. 1–23, 2019.

[10] J. Binstein, "How to cheat with proctortrack, examity, and the rest," *Jake Binstein*, 2015. (https://jakebinstein.com/blog/on-knuckle-scanners-and-cheating-how-to-bypass-proctortrack/)

[11] J. Chauhan, A. Goel, "An analysis of quiz in MOOC," in *Proceedings of the 9th International Conference on Contemporary Computing*, IEEE, pp. 1-6, 2016.

[12] S. S. Chua, J. B. Bondad, Z. R. Lumapas, J. D. Garcia, "Online examination system with cheating prevention using question bank randomization and tab locking," in *Proceedings of the 4th International Conference on Information Technology: Encompassing Intelligent Technology and Innovation Towards the New Era of Human Life*, pp. 126–131, 2019.

[13] C. Y. Chuang, S. D. Craig, J. Femiani, "Detecting probable cheating during online assessments based on time delay and head pose," *Higher Education Research & Development*, vol. 36, no. 6, pp. 1123–1137, 2017.

[14] S. Coghlan, T. Miller, J. Paterson, "Good proctor or 'big brother'? Ethics of online exam supervision technologies," *Philosophy & Technology*, vol. 34, pp. 1581–1606, 2021.

[15] D. R. Cressey, *Other People's Money: A Study of the Social Psychology of Embezzlement*, Glencoe, IL: Free Press, 1953.

[16] C. Crook, E. Nixon, "The social anatomy of 'collusion," *British Educational Research Journal*, vol. 45, no. 2, pp. 388–406, 2019.

[17] D. F. Crown, M. S. Spiller, "Learning from the literature on collegiate cheating: A review of empirical research," *Journal of Business Ethics*, vol. 17, no. 6, pp. 683–700, 1998.

[18] S. Dendir, R. S. Maxwell, "Cheating in online courses: evidence from online proctoring," *Computers in Human Behavior Reports*, vol. 2, 100033, 2020.

[19] M. Foucault, *Discipline and Punish: The Birth of the Prison*, Vintage, 2012.

[20] K. A. A. Gamage, E. K. De Silva, N. Gunawardhana, "Online delivery and assessment during COVID-19: Safeguarding academic integrity," *Education Sciences*, vol. 10, no. 11, pp. 1– 24, 2020.

[21] M. Garga, A. Goel, "A systematic literature review on online assessment security: Current challenges and integrity strategies," *Computers & Security*, Vol. 113, Feb. 2022.

[22] M. Ghizlane, B. Hicham, F. H. Reda, "A new model of automatic and continuous online exam monitoring," in *Proceedings of the 4th International Conference on Systems of Collaboration, Big Data, Internet of Things and Security*, pp. 1–5, 2019.

[23] S. Hubler, "Keeping online testing honest? Or an Orwellian overreach?," *The New York Times*, May 10, 2020. (https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html)

[24] F. M. Husain, G. K. S. Al-Shaibani, O. H. A. Mahfoodh, "Perceptions of and attitudes toward plagiarism and factors contributing to plagiarism: a review of studies," *Journal of Academic Ethics*, vol. 15, no. 2, pp. 167–195, 2017.

[25] K. Hylton, Y. Levy, L. P. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," *Computers & Education*, vol. 92, pp. 53–63, 2016.

[26] Z. Jiang, J. Huang, "Effective and efficient strategies and their technological implementations to reduce plagiarism and collusions in non-proctored online exams," *IEEE Transactions on Learning Technologies*, 2022. (https://ieeexplore.ieee.org/document/9724115)

[27] K. Lee, M. Fanguy, "Online exam proctoring technologies: Educational innovation or deterioration?," *British Journal of Education*, 2022. (DOI:10.1111/bjet.13182)

[28] K. Lee, M. Fanguy, X. S. Lu, B. Bligh, "Student learning during COVID-19: It was not as bad as we feared," *Distance Education*, vol. 42, no. 1, pp. 1–8, 2020.

[29] H. Li, M. Xu, Y. Wang, H. Wei, H. Qu, "A visual analytics approach to facilitate the proctoring of online exams," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021.

[30] H. Mellar, R. Peytcheva-Forsyth, S. Kocdar, A. Karadeniz, B. Yovkova, "Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives," *International Journal for Educational Integrity*, vol. 14, no. 1, 2018.

[31] P. K. Mungai, R. Huang, "Using keystroke dynamics in a multi-level architecture to protect online examinations from impersonation," in *Proceedings of the IEEE 2nd International Conference on Big Data Analysis*, pp. 622–627, 2017.

[32] J. G. Nguyen, K. J. Keuseman, J. J. Humston, "Minimize online cheating for online assessments during COVID-19 pandemic," *Journal of Chemical Education*, vol. 97, no. 9, pp. 3429-3435, 2020.

[33] Y. Peled, Y. Eshet, C. Barczyk, K. Grinautski, "Predictors of academic dishonesty among undergraduate

students in online and face-to-face courses," *Computers & Education*, vol. 131, pp. 49–59, 2019.

[34] A. M. Rogerson, G. McCarthy, "Using Internet based paraphrasing tools: Original work, patchwriting or facilitated plagiarism?," *International Journal for Educational Integrity*, vol. 13, no. 1, 2017.

[35] J. Schneider, R. Richner, M. Riser, "Towards trustworthy autoGrading of short, multi-lingual, multi-type answers," *International Journal of Artif-cial Intelligence in Education*, 2022. (https://doi.org/10.1007/s40593-022-00289-z)

[36] K. Trezise, T. Ryan, P. de Barba, G. Kennedy, "Detecting contract cheating using learning analytics," *Journal of Learning Analytics*, vol. 6, no. 3, pp. 90–104, 2019.

[37] S. C. Yang, C. L. Huang, A. S. Chen, "An investigation of college students' perceptions of academic dishonesty, reasons for dishonesty, achievement goals and willingness to report dishonest behavior," *Ethics & Behavior*, vol. 23, no. 6, pp. 501–522, 2013.

Biography

Anthony Y. H. Liao received his M.S. degree in computer science and the Ph.D. degree in computer science and engineering both from the University of Louisville, Louisville, Kentucky, USA. He is currently an associate professor and the Chairman of the Department of M-Commerce and Multimedia Applications, Asia University, Taiwan. Dr. Liao is a senior member of IEEE, and a member of ACM. His research interests include artificial intelligence, image processing, pattern recognition, data mining, e-learning, management information systems, enterprise resource planning, e-commerce, smart manufacturing, and software engineering.

Yu-Ying Hsieh received the Bachelor of Education in National Taiwan Normal University in 1983 and received an M.S. of Social Welfare in Providence University, Taiwan, in 2003. She served as a kindergarten teacher and principal from 1982 to 2005. She has repeatedly won the Kindergarten Model Award and Social Welfare Service Award issued by government agencies from 1996 to 2003. She was currently studying for a Ph.D. in the Department of Computer Science and Information Engineering of Asia University. Her research interests include applying information technology in-game and event design, etc.

Cheng-Ying Yang received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as a Professor at Department of Computer Science, University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing and computer security.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a distinguished professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

Research on Network Security Intrusion Identification and Defense Against Malicious Network Damage in a Cloud Environment

Yong Zhang

(Corresponding author: Yong Zhang)

Information Technology Department, Shandong Academy of Governance,
Jinan, Shandong 250000, China
Email: yo97ak@126.com

(Received Sept. 22, 2020; Revised and Accepted Apr. 12, 2022; First Online Apr. 30, 2022)

Abstract

The network security issue of edge computing has received more extensive attention in the cloud environment. This paper designed a network security intrusion identification method based on an extreme learning machine (ELM). In order to further reduce the computation on edge computing, the ELM was improved in terms of the selection of training samples. The improved ELM algorithm was used to recognize intrusion. Based on the game theory, attacker and defender models were established. How to select the defense strategy in the face of malicious network damage was designed. It was found that the improved ELM algorithm had a short training time and the highest accuracy rate (99.84%) for intrusion identification. In terms of defense against malicious network damage, the proposed method could effectively find the most suitable strategy to defend the network. The results demonstrate the reliability of the proposed method. The proposed method can be further applied in practical edge computing.

Keywords: Cloud Environment; Defense Method; Edge Computing; Intrusion Identification; Network Security

1 Introduction

In the cloud environment, with the rapid development of the network, network security issues have become more and more prominent. After accessing various network devices, the network environment becomes more complex, problems such as insufficient bandwidth and high energy consumption are frequent, and user privacy protection is more and more difficult. In order to solve the above problems, edge computing has been increasingly discussed [1]. Edge computing uses the edge of the network to compute and store data [2], which reduces network delay [3], saves network bandwidth, facilitates better decision making and protects privacy [4].

Edge computing plays a very important role in the fields of smart home [5] and vehicle networking. In terms of network security, traditional identification and defense techniques are targeted and passive; however, they are not applicable for the environment of edge computing, where networks usually face new and unknown security threats [6]. Moreover, due to limited resources in the edge computing network, guaranteeing network security becomes more and more difficult [7].

Rathore *et al.* [8] designed a soft hesitation fuzzy rough set (SHFRS) approach to handle multiple security services that dynamically change with user requirements and conducted an experiment on the approach.

Xu *et al.* [9] proposed a microservice security agent to protect user privacy, combined edge computing with application programming interface (API) gateway technology to provide a secure authentication mechanism, and verified the usability of the method by evaluating the round-trip time.

Han *et al.* [10] used one-time association multitasking proofs to authenticate local identities to realize access control under edge computing and found through experiments that the method was flexible.

Sang *et al.* [11] combined edge computing with an optimized annealing algorithm for relay protection in smart substations and found through experiments that the method consumed a short time in computing and had a positive effect on the safe shunting of power relays.

This paper mainly studied the network security of edge computing in a cloud environment, designed methods based on extreme learning machine (ELM) and game theory, and made experimental analysis on the methods to verify their reliability. This work provides some new methods to improve the security of edge computing networks, which is helpful to further promote the development and application of edge computing.

2 Extreme Learning Machine-Based Network Security Intrusion Identification Method

Intrusion in the network refers to all actions that may threaten data confidentiality and system reliability [12], including port scanning, denial of service, etc. Network security intrusion identification in edge computing refers to identifying data in edge nodes and determining illegal intrusions from them. Considering the complexity of the edge nodes and the limited resources, this paper chooses ELM to identify intrusions. ELM is an algorithm with simple computation, few parameters, and fast learning [13], which has good applicability in edge computing.

Suppose there is a training sample (x_j, t_j), where $j = 1, 2, \cdots, N$, $x_j = [x_{j1}, x_{j2}, \cdots, x_{jn}]$ and $t_j = [t_{j1}, t_{j2}, \cdots, t_{jm}]$, and n and m are the lengths of input and output vectors; then, the objective function of ELM can be written as:

$$H\beta = T,$$

where H is the output of the hidden layer, β is the output weight, and T is the expected output. The specific equations are as follows:

$$\begin{aligned} H &= \begin{bmatrix} h(x_1) \\ h(x_2) \\ \cdots \\ h(x_N) \end{bmatrix} \\ h(x) &= g(wx + b), \\ T &= [t_1, t_2, \cdots, t_N], \\ \beta &= H^+ T, \end{aligned}$$

where w is the weight, b is the threshold value, $g(x)$ is the activation function, and H^+ refers to the Moore-Penrose generalized inverse of H.

In order to further reduce the training time of the algorithm, the ELM algorithm is improved in terms of the selection of training samples. First, total sample S_n on the edge node is divided into two groups, one as the training sample set ($S_{nf}^f = \{s_j^f = (x_j^f, y_j^f)\}_{j=1}^{nf}$) and the other as the alternative sample set ($S_{nc}^c = \{s_j^c = (x_j^c, y_j^c)\}_{j=1}^{nc}$), $S_{nf}^f \cup S_{nc}^c = S_n$, and $S_{nf}^f \cap S_{nc}^c = \phi$. The ELM algorithm learns based on S_{nf}^f to satisfy $J(w, b, \beta) \leq \sigma$, where $\sigma \in \min J(w, b, \beta)$, which is the pre-determined limit of network performance.

It is assumed that the combination of absolute values of differences between the actual output and the algorithm output is U^c, $U^c = \{u_j^c | u_j^c = |t_j^c - F(x_j^c, w, b, \beta)|\}_{j=1}^{nc}$, after the algorithm trains S_{nc}^c. Let the element in S_{nc}^c that corresponds to the maximum value element in U^c be S_z^c, $S_z^c = (x_m^c, y_m^c)$. The calculation process of the improved ELM algorithm is as follows.

1) The sample sets are initialized: $S_{nf}^f = \phi$, and $S_{nc}^c = S_n$. The parameters of the ELM algorithm are initialized: $w = \phi$, $b = \phi$, and $\beta = \phi$.
2) The output H of the hidden layer is calculated.
3) $J(w, b, \beta)$ and U^c are calculated.
4) β is updated by w and b obtained by calculations to make $J(w, b, \beta) = \sigma$.
5) S_{nf}^f, S_{nc}^c, w, b and β are continuously updated until $J(w, b, \beta) \leq \sigma$.

3 A Game-based Approach to Defending Against Malicious Network Damage

After the identification of network security intrusions using the improved ELM method, different measures need to be taken for defense in order to respond effectively to these malicious damages. A method for defending against malicious network damages is designed based on a game. The attack device and the defense device are considered as two parties of the game. The strategy set of the attack device is $W_a = \{x_1 = attack, x_2 = noattack\}$, and the strategy set of the defense device is $W_d = \{x_1 = defense, x_2 = nodefense\}$. The strategy space of the model is written as:

$$W = \{W_a, W_d\} = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2)\},$$

where (x_i, y_j) is a combined strategy. Let R_{ij} be the gain when device i selects strategy j, then the gain of the model is expressed as:

$$Q = \begin{Bmatrix} Q_a(R_{11}, R_{21}), Q_d(R_{11}, R_{21}) & Q_a(R_{11}, R_{22}), Q_d(R_{11}, R_{22}) \\ Q_a(R_{12}, R_{21}), Q_d(R_{12}, R_{21}) & Q_a(R_{12}, R_{22}), Q_d(R_{12}, R_{22}) \end{Bmatrix}$$

During the game, the defense device will try to defend the network to avoid malicious damage, but when the attack of the weak attack device is powerful and difficult to be defended successfully, the defense device will stop defense to minimize the defense cost.

The benefits for both parties can be divided into four categories as follows.

1) The attack device attacks, and the defense device defends.
   In this case, the gain of the attack device is:
   $$Q_a(R_{11}, R_{21}) = \frac{T - T'}{T}(z_0 Q_\alpha + z_1 Q_\beta) - z_2 \frac{T'}{T}$$
   The gain of the defense device is:
   $$Q_d(R_{11}, R_{21}) = a_0 Q_{p'} + a_1 \gamma - a_2 Q_{q'} - a_3 \lambda.$$
2) The attack device attacks, and the defense device does not defend.
   In this case, the gain of the attack device is:
   $$Q_a(R_{11}, R_{22}) = z_0' Q_{\alpha'} + z_1' Q_{\beta'}$$
   The gain of the defense device is:
   $$Q_d(R_{11}, R_{22}) = Q_{\bar{p}}$$

3) The attack device does not attack, and the defense device defends.
In this case, the gain of the attack device is:

$$Q_a(R_{12}, R_{21}) = 0,$$

and the gain of the defense device is:

$$Q_d(R_{12}, R_{21}) = a_0' Q_p - a_1' \lambda - a_2' Q_q$$

4) The attack device does not attack, and the defense device does not defend.
In this case, the gain of the attack device is:

$$Q_a(R_{12}, R_{22}) = 0,$$

and the benefit of the defense device is:

$$Q_d(R_{12}, R_{22}) = Q_{\hat{p}}$$

The designed parameters and corresponding meanings in the above cases are shown in Table 1.

Table 1: Parameters

Parameters	Meaning
T	Attack time
T'	Penalty time of the attack device after the defense of the defense device
Q_α	The average bandwidth consumed after an attack when the defense device defends
Q_β	The normal packet loss rate after an attack when the defense device defends
$Q_{\alpha'}$	Average bandwidth consumed after an attack when the defense device does not defend
$Q_{\beta'}$	Normal packet loss rate after an attack when the defense device does not defend
$Q_{p'}$	Average bandwidth consumed by normal devices when the defense device defends
γ	Number of attacks defended by the defense device
$Q_{q'}$	Resources consumed for defense
λ	Number of normal devices affected after defense
$Q_{\bar{p}}$	Average bandwidth consumed by normal devices when the attack device attacks but the defense device does not defend
Q_p	Average bandwidth consumed by normal equipment
Q_q	Energy consumed after the defense of the defense device
$Q_{\hat{p}}$	Average bandwidth consumed by normal devices when neither the attack device nor the defense device takes action

Under edge computing, due to the many edge devices and complex network environment, there may be a situation where the gain of defense is less than the gain of no defense, at which time the defense device may choose not to defend. In order to improve the defense effect, this paper combines the mean-field game theory with the above model. It is assumed that the game time is $[0, T]$. The mean-field game (MFG) model for attack and defense can be written as:

$$MFG = \{N, A, D, Q_a, Q_d\}$$

where N is the set of all devices under edge computing, A and D are the optional attack and defense behaviors, and Q_a and Q_d are the gains of the attack device and defense device.

A mean-field coupling function is established to determine the effect of a single decision on the overall defense of edge computing. The Hamiltonian-Jacobian-Bellman (HJB) equation is written as:

$$\omega_i(m,t) = -\vartheta_t w_i^*(m,t) - \sigma_i \Delta(m,t) + H[i, \vartheta_t w_i^*(m,t)],$$

where w_i^* is the optimal defense strategy for a single device, m is the defense error mass distribution, and t is the decision time.

The Fokker-Planck-Kolmogorow (FPK) equation is written as:

$$\vartheta_t m - \frac{\sigma_i^2}{2} \Delta m - div\{mH[i, \vartheta_t w_i^*(m,t)]\} = 0.$$

The optimal game strategy can be obtained by solving the system of HJB-FPK coupled equations using the reinforcement learning-based Actor-Critic-Mass (ACM) algorithm [14].

4 Experimental Analysis

First, the improved ELM-based intrusion identification method was analyzed using the KDD CUP99 data set [15], which includes 39 intrusion types and is a common data set used in intrusion detection experiments. Twenty thousand training samples and 10,000 test samples were selected from the KDDCUP99 data set for experiments. The improved ELM algorithm was compared with the ELM algorithm, the support vector machine (SVM) algorithm, and the back-propagation neural network (BPNN) algorithm on the KDD CUP99 data set. First, the training time of the algorithms under different amounts of data is shown in Table 2.

It was seen from Table 2 that as the amount of training data increased, the training time of the algorithms increased, the ELM algorithm ¡ the improved ELM algorithm ¡ the SVM algorithm ¡ the BPNN algorithm. When the amount of training data was 5,000, the training time of the improved ELM algorithm was 0.12 s, which was 0.01 s longer than the ELM algorithm, 3.84 s shorter than the SVM algorithm, and 6.65 s shorter than the BPNN algorithm. When the amount of training data was 20,000, the training time of the improved ELM algorithm was 4.01 s, which was 0.04 s longer than the ELM algorithm, but

Table 2: Comparison of training time between algorithms (unit: s)

Algorithms	5000	10000	15000	20000
The improved ELM algorithm	0.12	1.97	2.12	4.01
The ELM algorithm	0.11	1.95	2.09	3.97
The SVM algorithm	3.96	7.82	12.33	16.32
The BPNN algorithm	6.77	10.34	20.78	30.77

Table 3: The set of attack behaviors

Attack Behaviors	Number	Attack Level	Cost of Attack
Installing Trojan horse virus	a_1	Low	20
Port scan	a_2	Low	10
Shutting down the database server	a_3	High	30
Code injection	a_4	High	20

Table 4: The set of defense behaviors

Defense Behaviors	Number	Defense Level	Cost of Defense
Repairing the database	d_1	Low	20
Deleting suspicious accounts	d_2	Low	10
Uninstalling Trojan horse virus	d_3	High	20
Installing patch program	d_4	High	30

significantly shorter than SVM and BPNN algorithms. When the amount of training data was 15,000, the training time of SVM and BPNN algorithms has exceeded 10 s, while the training time of improved ELM and ELM algorithms remained around 2 s. The above results suggested that the ELM algorithm took the shortest time in training, and the increase in computational complexity due to the step of sample selection in the improved ELM algorithm was small and did not have much impact on the efficiency of the algorithm. In conclusion, the improved ELM algorithm was reliable and could finish training in a short time for intrusion identification.

The accuracy of different algorithms in identifying intrusions was compared using the testing data, and the results are shown in Figure 1.

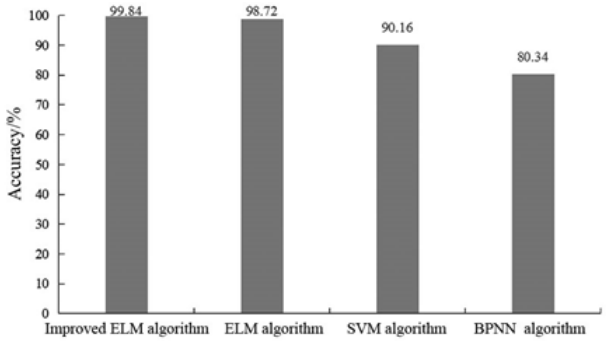


Figure 1: Comparison of accuracy between algorithms

It was seen from Figure 1 that the improved ELM algorithm had the highest accuracy, 99.84%, followed by the ELM algorithm (98.72%), the SVM algorithm (90.16%) and the BPNN algorithm (80.34%). The accuracy of ELM, SVM and BPNN algorithms was 1.12%, 9.68% and 19.5% lower than that of the improved ELM algorithm. The results of intrusion identification verified that the improved ELM algorithm had high accuracy. Overall, the improved ELM algorithm could identify intrusions in edge computing networks well and fast.

Then, the game-based network malicious damage defense method was analyzed. According to studies of Kayode *et al.* [16] and Gordon *et al.* [17], the set of attack behaviors used in the experiments is shown in Table 3, and the set of defense behaviors is shown in Table 4.

It was assumed that the attack strategy adopted by the attack device was $A_1\{a_1, a_3\}$, and the defense strategy adopted by the defense device was low-level strategy $D_1\{d_1, d_2\}$ or high-level strategy $D_2\{d_3, d_4\}$. In such a game, the gains of both parties were analyzed. The performance of the edge computing network was determined by taking the service delay time (SDT) as the standard, and the results are shown in Table 5.

It was seen from Table 5 that in the face of the same attack, the higher the level of the defense strategy was, the higher the gain of the defense device was, and the shorter the SDT was, i.e., the performance of the edge computing network was better under higher-level defense strat-

Table 5: Attack and defense game results

Attack Strategy	Defense Strategy	SDT/ms	Gain of the Attack Device	Gain of the Defense Device
a_1	d_1	282	233	128
a_1	d_2	197	287	165
a_3	d_1	144	136	121
a_3	d_2	113	155	136
a_1	d_3	74	146	251
a_1	d_4	42	171	280
a_3	d_3	39	115	151
a_3	d_4	34	126	181

egy. Moreover, regardless of whether the attack strategy was a_1 or a_3, selecting defense strategy d_4 could obtain the best result. When the attack strategy was a_1 and the defense strategy was d_4, the SDT of the edge computing network was 42 ms; when the attack strategy was a_3 and the defense strategy was d_4, the SDT of the edge computing network was 34 ms, which was much lower than that of the other choices. The results showed that adopting the game-based network malicious damage defense method could effectively identify the most appropriate strategy to defend the network against malicious damage.

5 Conclusion

This paper studied the edge computing network in a cloud environment. An improved ELM algorithm-based intrusion identification method and a game theory-based malicious damage defense method were designed. It was found through experiments that the intrusion identification method could complete training in a short time and had a high identification accuracy, and the defense method could accurately find out the appropriate defense strategy. The two methods can be further applied in practice. This work provides some theoretical bases for better implementation of network security of edge computing.

References

[1] M. Nijim, H. Albataineh, "Secure-Stor: A novel hybrid storage system architecture to enhance security and performance in edge computing," *IEEE Access*, vol. 9, pp. 92446 - 92459, 2021.

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016.

[3] Y. Yu, "Mobile edge computing towards 5G: Vision, recent progress, and open challenges," *China Communications*, vol. 13, no. Supplement2, pp. 89-99, 2016.

[4] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30-39, 2017.

[5] C. Vallati, A. Virdis, E. Mingozzi, G. Stea, "Mobile-edge computing come home connecting things in future smart homes using LTE device-to-device communications," *IEEE Consumer Electronics*, vol. 5, no. 4, pp. 77-83, 2016.

[6] P. Zhang, C. Jiang, X. Pang, Y. Qian, "STEC-IoT: A security tactic by virtualizing edge computing on IoT," *IEEE Internet of Things*, vol. 8, no. 4, pp. 2459-2467, 2021.

[7] R. Rapuzzi, M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model," *Future Generation Computer Systems*, vol. 85, no. AUG., pp. 235-249, 2018.

[8] S. Rathore, P. K. Sharma, A. K. Sangaiah, J. J. Park, "A hesitant fuzzy based security approach for fog and mobile-edge computing," *IEEE Access*, vol. 6, pp. 688-701, 2017.

[9] R. Xu, W. Jin, D. Kim, "Microservice security agent based on api gateway in edge computing," *Sensors*, vol. 19, no. 22, pp. 4905, 2019.

[10] D. Han, X. Du, Y. Lu, "Trustworthiness and a zero leakage OTMP-P2L scheme based on NP problems for edge security access," *Sensors*, vol. 20, no. 8, pp. 2231, 2020.

[11] Z. Sang, K. Yang, R. Zhang, "A security technology of power relay using edge computing," *PLoS ONE*, vol. 16, no. 9, pp. e0253428, 2021.

[12] J. Jiang, J. Li, J. Chen, "Research on edge computing security defense of information energy system," *IOP Conference Series: Earth and Environmental Science*, vol. 784, no. 1, pp. 012014 (5pp), 2021.

[13] J. Tang, C. Deng, G. B. Huang, "Extreme learning machine for multilayer perceptron," *IEEE Transactions on Neural Networks & Learning Systems*, pp. 809-821, 2017.

[14] Z. Zhou, H. Xu, "A novel mean-field-game-type optimal control for very large-scale multiagent systems," *IEEE Transactions on Cybernetics*, vol. PP, no. 99, pp. 1-1, 2020.

[15] S. Choudhary, N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Procedia Computer Science*, vol. 167, pp. 1561-1573, 2020.

[16] A. B. Kayode, I. G. Babatunde, H. D. Israel, "DGM approach to network attacker and defender strategies," in *IEEE Third International Conference on Information Science and Technology (ICIST'13)*, pp. 313-320, 2013.

[17] L. A. Gordon, M. P. Loeb, W. Lucyshyn, R. Richardson, "2004 CSI/FBI computer crime and security survey," *Computer Security Journal*, vol. 20, no. 3, pp. 33-51, 2004.

Biography

Yong Zhang has received the master's degree on electronic communication engineering. He is the deputy director and associate professor of Information Technology Department in Shandong Academy of Governance. His research interests include wireless communication, Internet security, and big data analytics. He has published more than 5 technical papers and 2 books in Chinese and international journals.

Browser Forensics: Extracting Evidence from Browser Using Kali Linux and Parrot OS Forensics Tools

Sirajuddin Qureshi[1], Jingsha He[1], Saima Tunio[1], Nafei Zhu[1], Faheem Akhtar[2], Faheem Ullah[1], Ahsan Nazir[1], and Ahsan Wajahat[1]

(Corresponding author: Nafei Zhu)

Faculty of Information Technology, Beijing University of Technology[1]
Beijing 100124, China
Email: znf@bjut.edu.cn
Department of Computer Science, Sukkur IBA University, Sukkur 65200, Pakistan[2]

(Received May 4, 2021; Revised and Accepted Apr. 3, 2022; First Online Apr. 30, 2022)

Abstract

In today's digitalized world, a lot of information is getting online, and the size of online data is getting huge day by day; thus, the field of data science emerged. Questions arise when there is so much massive size of data. It also makes it vulnerable to people who have malicious intentions. The gateway for surfing the internet is the web browser. Whether people use that for fair means or foul, some data is precious and sensitive. In this research, a related study about web browser forensics specifies its importance in digital forensics. These studies mention the techniques and tools for web browser forensics, investigating the Android platform as different web browsers provide their web applications. Considering all these studies, the authors go in various directions to extract evidence from the browser. This research will utilize tools like dumpzilla (based on python script), Bulk extractor, and SQLite to extract the details of evidence like history URLs, Cookies, Add-ons, and web Sessions and saved passwords in the cloud storage of the browser. For this, A scenario in the virtual environment is created that the victim browser could be exploited. Forensics tools run on two different platforms, Kali Linux and Parrot Security OS. Two other platforms are used to authenticate and verify shreds of evidence collected. There are limitations of tools. While running on different platforms, they missed capturing some shreds of evidence. After gathering the data from the victim machine, the web browser activities were predicted. There are limitations, and research offers future scope by improving the tools' performance—this requires sound knowledge of python, access control, and system architecture.

Keywords: Browser Forensics; Extracting Evidence; Forensics Tools; Kali Linux; Parrot OS

1 Introduction

Digital forensics is used in auditing and investigating whenever criminal activities were reported. DF is the preservation of the artifacts collected. In this process, there are four steps. The first step is the identification of cybercrime activity what happened. Next is the extraction and preservation of pieces of evidence collected from the crime scene. Then there is the thorough analysis of all the facts and shreds of evidence contained. The last step is the documentation of the whole case and forwards it to further proceedings. In Digital Forensics, BF is the central part as any activity starts through the browser. Many obstacles come in this research as there is volatile data, and challenging to recover the browsing history. In background study, the work of previous authors mainly consists of focusing on the artifacts that are emails, browser history, and images. In this research, cookies are focused and are to be extracted using the forensics tools of Kali Linux. Cookies can save plenty of information like the web page's language, websites we visit online shopping, details, passwords, and most importantly it maps would be very helpful in predicting the real cyber culprit who exploited the browser. Man in the Browser (MITB) is the type of cyber threat in which the hacker uses the browser by identifying and hitting on its vulnerabilities. The primary victim of MITB is online banking transactions. The hacker can alter the transactions and launch a DoS on the bank server, making it unavailable to its legitimate users. With such types of threats, it becomes necessary to secure web browsing. Still, when it was exploited, digital forensics investigators must find out the cause of the cyber-attack and make room for the future and overcome the vulnerability that the attacker exploits.

Private browsing is one of the major issues highlighted by [5]. Many browsers nowadays provide privacy modes

like google incognito, where browsing history was not mapped. That's one of the significant issues. Suppose forensics cannot find out what is surfed on the browser. It will create problems in leading the investigation—their research identifies the possible hidden privacy modes in a web browser. Phishing attacks are common these days. Most of the people receive emails scams like a Nigerian widow is offering her seven hundred thousand dollars with the link provided or youngsters mainly targeted by the emails in which some company (which does not exist in reality) offering them a job with a handsome amount of salary and many more like this. So [6] elaborated on these email scams and studied how to avoid malware/spyware phished into your system.

In this discipline of web browsers, forensics legal and technical aspects must be considered while conducting a forensics investigation. A digital forensics investigator must know about these legal aspects to filing a solid case [24] contributed to digital forensics technical development by answering can browser forensics detect a criminal tendency?, What are the legal aspects of conducting web browser forensics? Software tools make our lives easy, but there is still a need for expertise to utilize these tools efficiently for this hands-on tool BrowStExplus studied by [16] for web browser forensics. This tool is used to map the storage of web browser details and helps in extracting the pieces of evidence. WBF is one of the major domains in digital forensics as dependency on the internet increases, thus increasing its vulnerability. Deleted web data, private browsing modes, denial of service DoS attackman in the browser all exploit the web browser and become catastrophic for the online business and e-commerce industry. One of the main obstacles that refrain digital forensics investigators from leading the investigation is the deleted history and using private browsing modes. In this research, the main focus would be on internet cookies that save many things, including online shopping details, saved passwords, and one of the most important things they mapped the browsing activity, which is the key in web browser forensics investigation. For example, an internal malicious user exploited the web browser in an organization and leaked the company's private information on the internet. The problem arises when the investigators reach the IP address from where the information is leaked, but after reaching that device, all the data is vanished and is wiped out from the browser.

This addresses the main problem statement of this project: **"In an organization, an internal malicious user leaked the confidential information on the web by exploiting the browser and deleted all their footprints. For that purpose, a forensics investigation needs to extract all the pieces of evidence like history, cookies, and saved passwords from the cloud space provided by the browser."**
This research follows by utilizing digital forensics tools on the victim's device. The main tools that were used in this project are "Dumpzilla" and "SQLite".

1.1 Research Questions

As mentioned about the browser forensics earlier, the main criminal activity starts from here and it may lead to botnets and denial of service attacks. The main question of this research arises as follow: **Is it possible to run a successful digital forensic investigation in the circumstances when all the browsing data is vanished after being exploited?** Following this question and to barrier the research gaps, this research raises some questions that would lead to the solution of the problem statement to solve the issue of browser cloud forensics investigation.

- **What would be the suitable technique to conduct browser forensic investigation and avoid the chance of losing important shreds of evidence?** Browser data is sensitive and volatile. It is difficult to prevent the data loss that would help lead the investigation. It is also essential for the organization to be equipped with evidence collection methods and techniques.
- **How to extract and predict the culprit?** Here comes the difficult part of the investigation. First, in this research, the shreds of evidence are preserved following the procedures of digital forensics investigation and compiling the report. Finally, the prediction of browser activity to find the real culprit.

The sub-questions help the investigators in leading the research. First of all, the researcher will extract the shreds of evidence from the browser cloud by utilizing the tools of Kali Linux. Some problem arises in experimental analysis while conducting the research this would be later discussed in this paper.

1.2 Paper Structure

Start with part one. The introduction briefly explained the overall concept of research to be conducted and the main hindrances that arise in investigation. It provides the background about how other authors work on this investigation and how it will overcome the gaps. In the next part, the literature would explain the researches of previous authors in this regard, then the thesis would come towards the research methodology, which would elaborate the research scenario of how the research is being conducted in the environment when all the browsing data has vanished. Then the experimental analysis gives the simulations of the tools conducting the investigation. After that comes towards the findings the problem arises in the research then comes towards the conclusion and future aspects of this research.

2 Literature Review

In the cyber world every day there are countless numbers of crimes reported each day which breached many

gigabytes of online data. As the world is digitalizing, the demand of securing the IT industry is a demanding topic these days. Here comes the need for digital forensics and investigation all the criminal activity. There are tools available that need the expertise to capture the malicious activity. Earlier this research, many authors work on this problem as today's world information is digitalized. All your banking and financial details, health reports, and personal credentials are online, making them vulnerable. The beauty of the internet facilitates the users by coping with any type of device connected to it. But in making the architecture of the internet, the layers of TCP, the main focus was on functionality. As time passed, security becomes a loophole for the attacker and cyber criminals to exploit the information.

The work of previous authors mainly centred on the analysis of artifacts related to browser history, emails, and images or videos are discovered or not. This research is a step forward to find the cookies based on that the behaviour of the malicious user on the browser can be determined, and this can be compared with the history and cookies of employees of the organization to find out the real culprit.

In this project, we assume a case study in which a malicious internal user of an organization exploits sensitive information by leaking it on the internet. Someone from the organization found the information randomly on the internet and report it to the IT department. They immediately call the digital forensics investigator. With some initial investigation, the investigators found the PC's IP address from where the information leaked. Now they find out that all the browsing history is deleted, and there is no trace of malicious activity. First, they have to do some research for such type of investigation problem, and with the help of a digital forensics tool, the required shreds of evidence will be extracted.

2.1 Related Study

Heading towards the research, we have to study the brief idea of digital forensics, its significance in cyber security, and the necessary investigation processes. What are the main obstacles that arises and how to overcome these issues smartly and bypass the obstacles that come in the investigation? In understanding the main process, firstly, let's discuss the work of authors in this field.

The field of cyber security moves in both ways defense and attack one can be on the defensive and attacking side. The combination of both is efficiently elaborated by [17]. They combine steganography and forensics with running a security check and overcoming a vulnerability in transferring information between users. In reviewing and leading the digital forensics investigation as studied by [3]. Their framework consists of two steps or phases. The first phase maps all are artifacts and shreds of evidence collected from the crime scene during the investigation. The next phase is the step-by-step and semi-automatic way of investigating a cyber threat despite its intensity. In this phase, first of all, there is the selection of CKC. Then comes the identification by comparing the found CKCs with the organization of the proposed artifacts. Then find the correlation between the CKCs and the artifacts presented. Then there is the construction of the chain of artifacts CoA. After there is analysis of CoA.

Ensuring the quality of investigation and avoiding the flaws and false shreds of evidence [4] gives the QA for the DF investigation. Many practitioners or investigators face challenges while investigating when they came across mismanaged shreds of evidence. Like without proper preservations and proper documentation of the artifacts that can be utilized to solve the case. In this regard, the authors proposed the mechanism of "Verification of Digital Evidences" which helps practitioners keeping track of all the artifacts and proper documentation of sensitive evidences; without proper records, it would be troublesome to lead the investigation. This research is also getting motivation concerning the work of [25]. They set up a virtual environment, exploited IoT devices with Kali Linux Tools, and conducted digital forensics experiments. This research following the same footsteps in experimental learning.

Same in a virtual environment, a web browser is exploited. A web browser forensic investigation is run to extract the shreds of evidence from the browser in a virtual setup and about the forensics tools, FTK imager is also very beneficial in getting all the desired evidence from the web browser studied and implemented [22]. The author gives a detailed study about capturing the user activity on a web browser by utilizing the FTK imager. Also [15] provides the detailed research, tools, and techniques for forensics analysis of shreds of evidence collected from the web browser. The work of previous authors mainly centred on the analysis of artifacts related to browser history, emails, and images or videos are discovered or not. This research is a step forward to find the cookies because the behavior of the malicious user on the browser can be determined. This can be compared with the history and cookies of employees of the organization to find out the real culprit. There is also a study [12] in which the authors discussed the compatibility and efficiency of tools utilized for the Firefox browser.

Internet starts with the search engine, the web browser, and the first thing that comes in search is URLs (uniform resource locator). Data about data or Metadata need to be grabbed when locating or mapping extensive search activities. This research provides the framework for grasping the malicious browser activity like hate content or leaking of sensitive information on social sites by examining and mapping URLs activities to guess the browsing activity. It may help in guessing the browsing activity of the particular user in case of an internal threat or case when an internal malicious user exploits the system. This approach is utilized in this search, but the target will be to extract the cookies. Logging is one of the best ways to keep the record or directory as in [7] authors discussed logging with the help of it a user activity on the browser

can be mapped. A log file helps to collect information about the malicious internal user. All windows systems have log files that keep the arbitrary data. It is called index.dat, which keeps all the data of websites visited from the computer. Also, trace the log file [1], which gives the techniques to identify and locate the log files of the browser. Also contributed to analyzing the gathered information to find out the malicious activity.

Phishing is one of the major attacks that exploit computers and mobile devices. Phishing emails are mostly used in which a user receives an email of a job offering or any marketing scam to overcome such spam. In phishing, there is mostly the negligence of employees who do not timely report any such incident. In a study by [11] they discussed social cognitive theory (SCT) and cyber risk beliefs in SCT. Their major contribution is to give detailed study about the careless attitude from the employees and give awareness for cybersecurity. To secure the browser from such intriguing mails a study by [9] conducted an activity in which 985 participants take place. Their data collected and analyzed have proposed a model for predicting spam and phishing emails. Also, there is a need for user awareness for securing their web browser from phishing because you have applied the most advanced system for security in an enterprise.

Still, there is the negligence of unaware employees that puts the whole enterprise at risk. So [21] studied the behaviour of users and reactions when they received warnings from the browser. Their results would help in improving the browser's security features. Authors (Peter Snyder, 2018) give a cost-benefit approach to secure the browser. They have made a simple extension to avoid the CVE exploits that are available open-source. Another study by [23] in which the proposed system is doing deep scanning of emails and sorting them out in different categories like spam, important, etc. For securing the web browser, one should be aware of the security configuration features of the web browser. A study by [18] studied more than a thousand configuration options for three major web browsers. Out of that, they have found 13 useful features for secure web browsing. A private web browser that was continuously relocating the IP also makes it difficult in a forensics investigation, like Tor Browser. These browsers camouflage the IPs and make it difficult to detect and map the exact location of criminal/malicious activity. Regarding this issue [8] discussed about the forensic of a tor browser. While discussing their design considerations, the project is focused on expanding the previous research to find out that there is an existence of the Tor browser in windows 10. They're also a case study on "Epic" which is a private browser [14]. There is a study about the harsh impact of usage of epic browsers for illegal activities like drug dealing and human trafficking. They run live forensics on an epic browser to capture the exact location of the desired shreds of evidence. Secondly, by capturing the RAM they find out the digital artifacts provided by the Tor browser. The malicious activity can also be done through the android device as the browsers provide the full compatibility in smartphones as well. To run the forensics on the browser in a smartphone [20]. In their framework, they extract the information from the device like serial no, root access, or any sort of encrypted files in the device. Then moved towards checking the root access in the device.

They found the device is rooted, and then it will further process for web browser forensics. Then another module checks and calculates the artefacts and shreds of evidence collected; then there is a thorough analysis of artefacts and shreds of evidence collected.

There is also an issue of resource abuse studies by [2] that there is a covert use of resources of machines for crypto mining or crypto-jacking. Hackers made their transactions in cryptocurrency for that they need the heavily resource-rich device for this purpose. They use botnets to exploit the machines and abuse their resources. Authors have designed an algorithm to guard and protect the browser if botnets exploit resources for crypto mining. To secure the web browser, a fingerprinting method was proposed by [10, 11] in which there is a transaction on identity method imposed. Users with high likely hood and based on their extracted features, they have generated an identity. Every time they browse on the internet, they have to provide that ID for searching. Also, the US patent [19] recommends the authentication factors for secure web browsing. This related study is summarized in Table 1.

2.2 Summarized Literature Review

In summarizing all the related studies mentioned above, it gives the significance of browser forensics in DF as the browser is just like the motherboard of connecting devices to the internet world. Any activity on the internet starts with surfing on the browser. It may be good and maybe sometimes exploited by any malicious user from inside the organization. Sometimes, it becomes cumbersome for the DF investigators when all the browsing history were deleted and someone is using a private browser like Tors. Many browsers offer the private browsing mode or camouflage the IPs of the devices, which makes it challenging to map the browsing activity, leading to the malicious user that exploits the browser.

Prior authors have discussed web browser forensics in this arena. The main focus was on extracting the artifacts and collecting the shreds of evidence. They are going with extracting log files in the windows, utilizing a tool like BrowStExplus. They were also utilizing android toolkits for forensics and running algorithms for identifying phishing attacks via email forensics. While conducting the digital forensics investigation, it is compulsory to consider the legal and technical aspects mentioned in the related study. This research will extract cookies from the browser and save passwords by utilizing the forensics tool dumpzilla and SQLite in the OS Kali Linux.

An experimental learning environment is set up to run a digital forensics investigation on the exploited browser

in the research scenario. By extracting the artifacts like cookies, save passwords in the cloud environment provided by the browser.

The abbrevations used in Table 1 will be discussed in appendix section at the end of this paper. The main research objectives are as follow:

- Conduct a forensic investigation on browser cloud;
- Utilize tool to collect the artifacts and evidences;
- Bypass the hindrance of deleted browsing activities;
- Focused on extracting the cookies of the browser which contains many information related to browsing activity;
- Analyzing all the evidences to capture the malicious internal user.

In concluding all the related studies, it's elaborated the importance of browser forensics in the world of digital forensics. Many authors researched it by utilizing different tools and techniques for the investigations. Also, the legal and technical aspects are mentioned as a digital forensics investigator must be aware of these aspects. Comparison to all the research mentioned in the related study, and after studying their approaches, this research will extract cookies from the browser. These cookies contain many sensitive and volatile data that are very precious for investigators. Most of the investigations got stuck without proper handling of the artifacts and after losing the volatile data. This research utilizes the tool dumpzilla. Dumpzilla is the digital forensics tool developed in python that provides many utilities in conducting the digital forensics investigation on the browser. It helps extract the volatile data and sensitive shreds of evidence that would be a gem for investigators. Getting required traces of evidence in the vital step investigations and after that, there is also need to preserve these documents.

Table 1: Summarized related study

Reference Work	Basics in DF	VoE	DF Tools	HE and SB	Phishing, UB	PB	RA	Remarks
[3, 4, 25]	Discussed	Discussed						CKC, Mechanism for VoDE
[7, 12, 15]		Discussed	Discussed					FTK imager, Firefox forensic tool
[1, 11, 13]	Discussed		Discussed	Discussed				A proposed method to penetrate log files
[9, 21]					Discussed		Discussed	Methodology to mitigate a phishing attack
[8, 18]					Discussed			cybersecurity awarenes
[2, 14, 20]		Discussed		Discussed		Discussed		Methods to extract pieces of evidence in PB
[10]				Discussed				Live Forensics of RAM capturing
[19]						Discussed	Discussed	Resource abuse mitigation algorithm

3 Research Methodology

Describing the qualitative investigation goals is understanding, explaining, discovering, and making theoretical approaches and hypothetical information. Qualitative is flexible structured it can be modified according to the facts collected and gathered. Data collection in qualitative the researcher is the main instrument for gathering and processing the data. This qualitative data can be obtained from various sources like conducting interviews of relevant people of the field, focus groups analyzing and studying the research topics on the basis of their findings and observations. After that, the thorough and intensive study of existing documents of the relevant field. Describe here the three chapters from the book qualitative research (Dawn Goodwin, 2019). It's a difficult task to assess and assure the validity and quality of qualitative research because of its diversity. They mentioned six methods: triangulation, respondent validation, clear

exposition of data collection methods, reflexivity, attention to negative cases, and fair dealing. The theory has an essential role in leading qualitative research. Some considerations underpin the research strategy. They also explained ontology in which is concerned with the questions. Also, epistemology is concerned with the theories of knowledge.

The quantitative is mainly concerned with the statistical and numeric data, logic, and an objective stance. It is a systematic and empirical investigation of observable phenomena via statistical and mathematical techniques. It consists of large numerical data. After that, they conduct data analysis that to find correlations. It involves the generation of data in a quantitative form which can be subjected to rigorous quantitative analysis formally and rigidly. While in mixed methods, there is a hybrid of both qualitative and quantitative to research three different ways. In the first type, the quantitative data are collected first and then the qualitative data. In this process, the qualitative data were served to explain processed quantitative data in contributing to the research. The next type of research is in which first there is qualitative then comes the quantitative for justification of qualitative data collected earlier. The last type is the combined effect of both qualitative and quantitative.

3.1 Research Design

It is moving towards the research design to identify the purpose of this research and its outcomes. About the book chapter (Woodrow, 2014), the first part of the research design is to identify the research purpose. Following this regard, the focus of this research is on web browser forensics. Any activity on the internet starts with surfing on web browse, whether for the searching purpose or exploiting the legitimate resources of any enterprise. It becomes challenging for the investigators to capture the volatile data and manage sensitive shreds of evidence in the environment of the exploited web browser. In this regard, the purpose of this research would become:

"Extracting evidences with the approach of capturing the cookies in the browser which contains plenty of precious data that would lead the digital forensics investigation in right direction"

The next step is identifying the variables, whether it is an independent variable (IV) that impacts the outcome of the dependent variable (DV), that is, the outcome itself. In this research, the impact of extracting the cookies, passwords, add-ons, sessions, etc. (independent variable) with the help of forensics tools (independent variable) to run the browser forensics. From that, the variables are measured. Then decide how these variables will be measured, it is by extracting cookies with the help of dumpzilla and checking the browser details with the help of SQLite. After that analyze all the variables, our main target is to find the internal malicious user. This can be done by setting up a virtual environment in which a digital forensic investigation is run to collect all the cookies and then it's analyzed. As mentioned in the proposal, we are assuming that we have found out the machine that is exploited to leak the data on the internet. Now data from all the devices in that department is analyzed. After that, the data collected from the exploited machine was compared with the collected data of all other department's machines. After that, the report was compiled, and the process is as Figure 1.

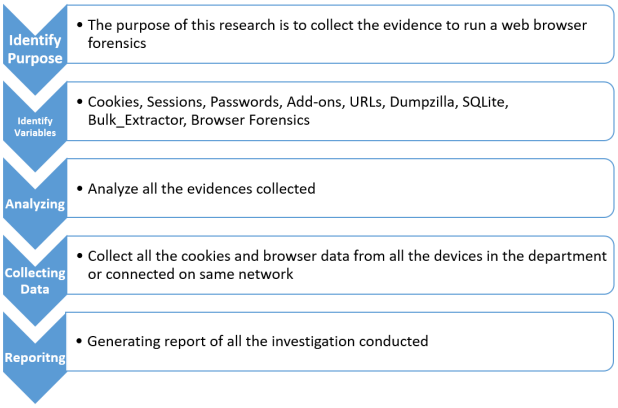


Figure 1: Research design

3.2 Choosing Research Method

They discuss all the related studies work in digital forensics, specifically in web browser forensics. Most of the authors use logging like keeping the record files of all the browsing activity. Some are capturing the RAM file using disk image forensics to get all the activity during web surfing. There is also the discussion of legal and technical aspects of digital forensics research. A DF investigator must be aware of all the legal and technical aspects of the investigation.

In this research, following the research design, the approach collects the shreds of evidence from the web cookies. These cookies are basically the messages that a web server sends to your web browser when you visit internet sites. It's a term of a UNIX program that is Fortune Cookie which contains all the browsing activity information. This research aims to get these cookies pulled out from the browser and start the investigation. The method chosen in this search is the hybrid of qualitative and quantitative analysis. The mixed methodology is in which first the related researches are thoroughly studied and run an experiment of extracting artifacts from the victim machine and concluding the results.

After cookies, we must move towards other data and the saved passwords of different sites that an internal malicious user used for various sites, which could be a gem in extracting more details and making the investigation more concise. Sessions are also important evidence in guessing and predicting the malicious activity along with the Add-ons and all the important URLs we can extract by utilizing our tools in the environment or lab we set up for the investigation.

4 Investigation and Analysis

Getting started with the investigation, we have to set up an environment to conduct the investigation, set up all the necessary tools, and fulfill all the dependencies. Move with the assumption that the investigation has traced the IP addresses of the machines that are being exploited. As they reached that machine, investigators found out that all the browsing activity had vanished, creating a big hurdle in their investigation. They need to extract out all the sensitive shreds of evidence, including sessions, cookies, add-ons, passwords, etc. First, we have set up a forensics environment. We have setup Kali Linux, an operating system providing a platform for penetration testing and digital forensics.

Similarly, another competitor operating system for penetration testing and forensics is used which "Parrot". Using two operating systems makes the investigation more precise and authentic as there is cross-check of results from two different platforms. Experimental analyses are the most critical part of any research, which decides the contributions of the author. Here either you have reached the desired results and contribute by suggesting the gateway toward the solution of the identified problem. On the other way around, after so much intensive work, the desired outcomes are not achieved and, in the end, the research is not going the way you anticipated. In such a case, the author's contribution is that he/she has done so much study to identify the problem and formulate a hypothesis to get the solution. After conducting the intensive series of experiments and calculations when the anticipated method did not lead to the desired solution, the author saved the time of many researchers. The contribution is his or her wide range of study to save the time for literature review and guide the researchers that the anticipated method does not lead towards solution it is either stuck at the end.

4.1 Project Implementation

Following the methodology of the project. The implemented technique or method here is the mixed methodology the combination of qualitative and quantitative research. First, a detailed study has been conducted for the problem identification in which the researches of various authors are mentioned in the detailed study section. This study includes digital forensics' legal and technical aspects to extracting artifacts, sensitive shreds of evidence, and volatile data. These authors work on separate identities like email forensics to detect and prevent phishing attacks. Then some are using log-based analysis to get the log files of saved browsing activities. Some are using image extracting tools to recover the browser's log files in the hard disk image. Also the method of capturing RAM to access the volatile data of the browser.

All these researches and experimental analyses are leading towards extracting as much data as it makes the investigation more authentic and more precise. But there

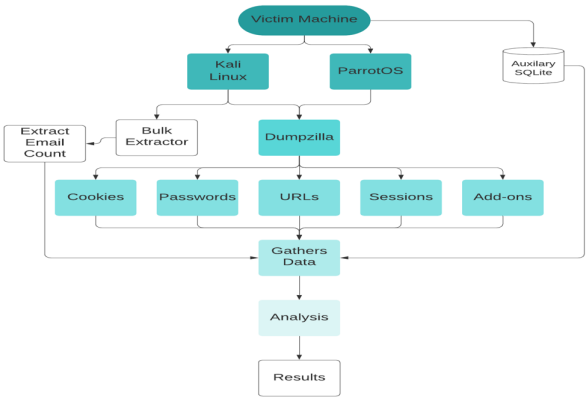


Figure 2: Project implementation

are a lot of methods to pull the same shreds of evidence. This research shows all the shreds of evidence, including the most critical cookies, sessions, passwords, Add-ons, etc. by utilizing "Dumpzilla" and "Bulk Extractor". There is the setup of the virtual environment in which as per assumption the victim machine is found out which is used in the exploitation of the browser. On this machine, investigators installed two operating systems "Kali Linux" and "ParrotOS" which extract the necessary data nd shreds of evidence. The project implementation is illustrated in Figure 2.

4.2 Experimental Enviornment

Coming towards our digital forensics lab where the investigation will capture the cyber culprit/internal malicious user who has exploited the browser and tries to hack into XYZ organization's database to get the sensitive information. Moving with the assumption that forensics experts have traced the IP address of the victim machine, but on reaching that machine, they have found out that all the data has vanished, here comes the hurdle and basis of this research.

There is a need to extract all the data from the browser, including sessions, Add-ons, cookies, and saved passwords. In our lab, we have setup KL and POS in which we are utilizing forensics tools like dumpzilla and bulk extractor, and auxiliary SQLite information of history. The same experimental analysis on two OS makes the research more precise and authentic when verification from more than one source. So moving towards the investigation.

4.3 Investigation in Kali Linux

First, we are extracting the shreds of evidence in the kali Linux lab the required shreds evidence. Let's start with extracting the history of the browser by running the dumpzilla. Starting with dumpzilla

From Figure 3, we can see the interface of dumpzilla and how it makes our work easy. To get the best use of these tools in investigation, an investigator must acquire

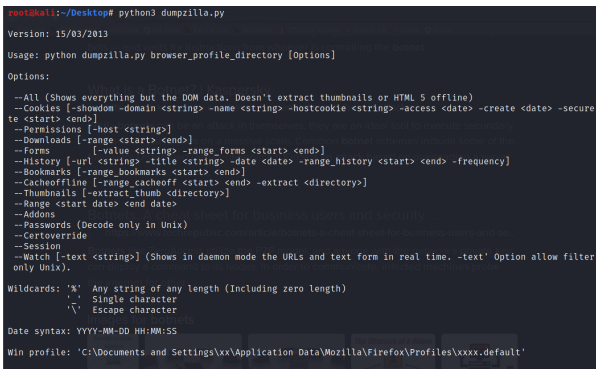


Figure 3: CLI view of Dumpzilla

Figure 4: Mozilla profile

the sound knowledge and hands-on command on Linux usage. Linux gives many utilities over windows, but this is not the discussion of this research. In the interface, it has been seen that the tools instruct extracting the data. Starting with history extraction, we have to locate the browser default file hidden in the system then run that file on forensics investigation. In Figure 4, we get into the directory to locate the default file of the browser.

By running some simple commands on Linux, the investigator's life becomes more accessible and he gets into the default file of the browser from the victim machine. Now, this critical file is to be used in leading the investigation towards predicting the browsing activity of the malicious user.

By getting the comprehensive data, we run the command –All to get complete information about the browser then get step by step into it. The process is shown in Figure 5.

Summarizing the above-collected data information we have got the overall scenario of how much the browser is exploited. So, in Table 2 have a summary of gathered

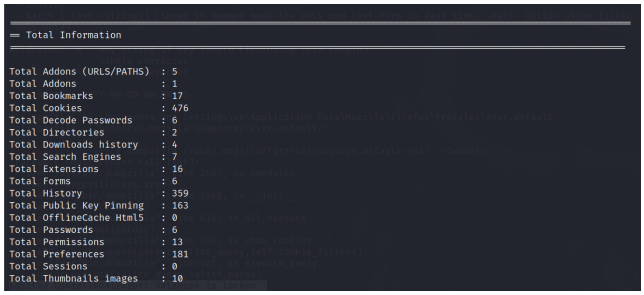


Figure 5: Summary of fetched data

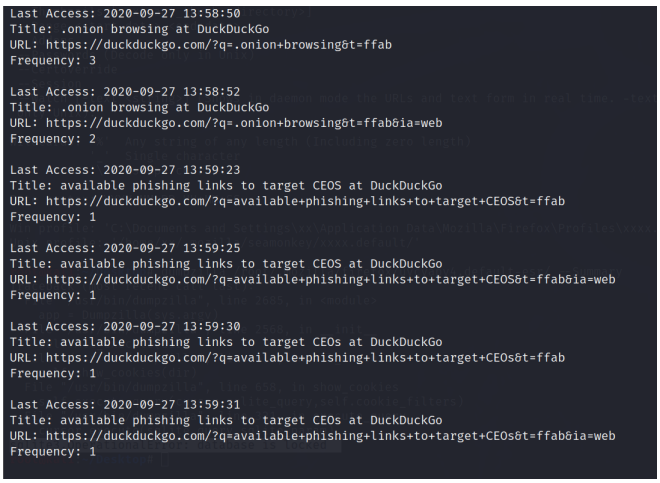


Figure 6: Extracted history

information.

Table 2: Summarized extracted data

Evidence	Frequency of Data
Cookies	290
Passwords Decode	0 (no Saved Passwords)
URLs	116 saved URLs
Sessions	0
Add-ons	0
Bookmarks	10

Now we have moved towards the step-by-step extraction of all the shreds of evidence collected. From above, the frequency of traces of evidence collected now by looking deep into that, the required piece of data is sorted out in coming steps. Moving towards history first. An extracted record is shown in Figure 6.

The figures mentioned above contain all the details about browser history, after deeply analyzing the history details gathered from previous suspicious activities, it has been found that the malicious internal user has tried to make identity anonymous by using Tor browsing and tries to learn about the phishing attacks to trap the company's CEO (mostly they are non-technical people and seldom care about such things). Also, he is continuously surfing to find out ways of accessing the dark web that might exploit the department's PCs for unfair means and activities. Summarizing the history details in Table 3.

From the above tabular data of historical details, the internal malicious user continuously searches the malicious things dark web, phishing, and techniques to install malware and Trojans. On the basis of these searches found from the victim machine, the same data was extracted from the other PCs of the department, and after that, we will compare and analyze to find out who is the real culprit who used someone else computer to exploit the data and for malicious and illegal activities. From cap-

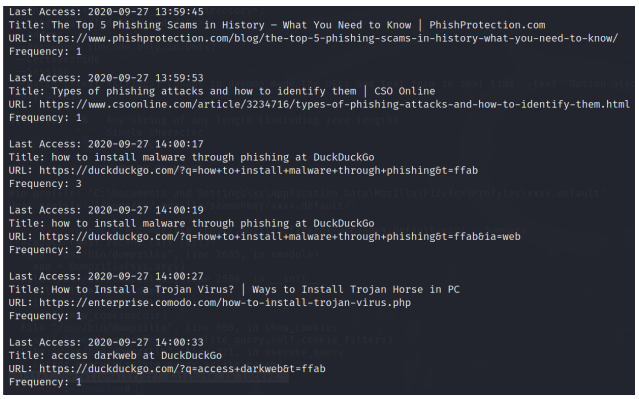


Figure 7: Extracted cookies

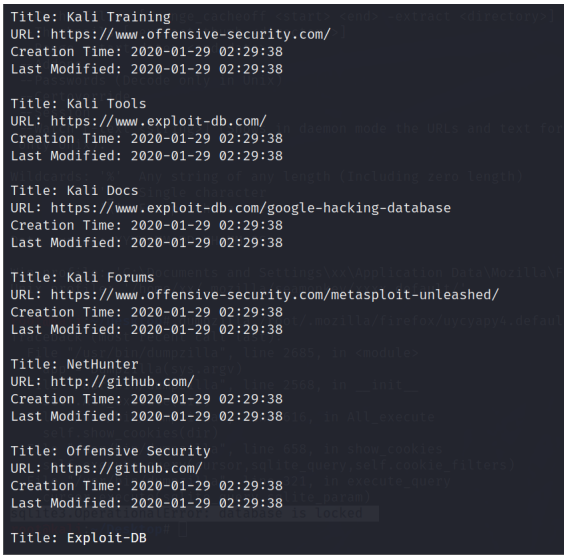


Figure 8: Extracted bookmarks

turing the Tor browser access from the history, it's been confirmed that the malicious user has actions on "Dark Web"; otherwise, nobody needs a Tor browser for any fair method. It has been concluded that he might be selling enterprise's sensitive data to some black hat hackers on the Dark Web. But this can be done when the culprit is being caught then police and investigation agencies will take care of it. Now let's move towards the cookies extraction in Figure 7.

From cookies extraction, it gives us the complete details about the browser activity. It provides the details about the sessions created, domain name, hostname, expiry whether it HTTP or HTTPS its value and all this information from the vanished computer helps a lot in leading the research and closing the case for final analysis now moving towards the bookmarks saved. Extracting and summarizing bookmarks in Figure 8.

It can see the bookmark's details that the malicious user has activities on the tor browser. Now it's sure that he has some linkages on the dark web and might be selling companies sensitive on illegal websites. To further verify shreds of evidence collected and count the emails present

Figure 9: Extracted add-ons

Figure 10: Extracted sessions

in the browser, another tool, "Bulk Extractor" is used for further investigation.

Now moving towards the Addons, Passwords, Thumbnails and further data extraction is shown in Figures 9, 10, & 11.

Now for the Bulk extractor, it can use in terminal mode, and it also provides GUI for the extraction of data. First, let's launch the Bulk extractor, which is shown in Figure 12.

Here adopting the methods of experts, the tool is utilized in the terminal and command line to run the investigation. In this tool, there are utilities in which it creates a whole folder for the directories and all the shreds of evidence it has collected from the victim machine. Starting with Bulk extractor shown in Figure 13.

Here the data extracted from the browser is saved in the folder created by the Bulk extractor (see Figure 14). This tool provides the extracted data from the file directory and keeps it in a folder created. It can also scan the image files, but here in this research, the approach is to get the file directory for investigation. The above also concluded that it has been found from vanished data that 491 Email features were present there. Here the folder created "Case-1-internal_threat", which contains all the data collected from the file directory, and it also has SQLite auxiliary file for further verification of shreds of evidence. The given snapshot gives details about the files created

Table 3: History details

Title	URL	Date and Time	Frequency
.onion browsing at DuckDuckGo	https://duckduckgo.com/?q=.onion+browsingt=ffab	2020-09-27 13:58:50	3
phishing links to target CEOs	https://duckduckgo.com/?q=available+phishing+links+to+target+CEOSt=ffab	2020-09-27 13:59:23	1
Top 5 Phishing Scams in History	https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/	2020-09-27 13:59:45	1
how to install malware	https://duckduckgo.com/?q=how+to+install+malware+through+phishingt=ffab	2020-09-27 14:00:17	3
How to Install a Trojan Virus?	https://enterprise.comodo.com/how-to-install-trojan-virus.php	2020-09-27 14:00:27	1
access darkweb	https://duckduckgo.com/?q=access+darkwebt=ffab	2020-09-27 14:00:33	1

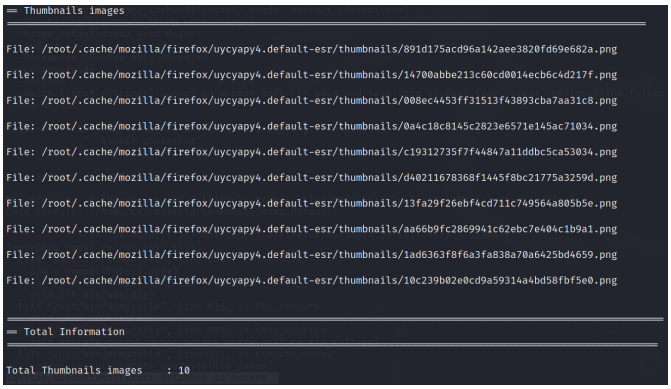


Figure 11: Extracted bookmarks

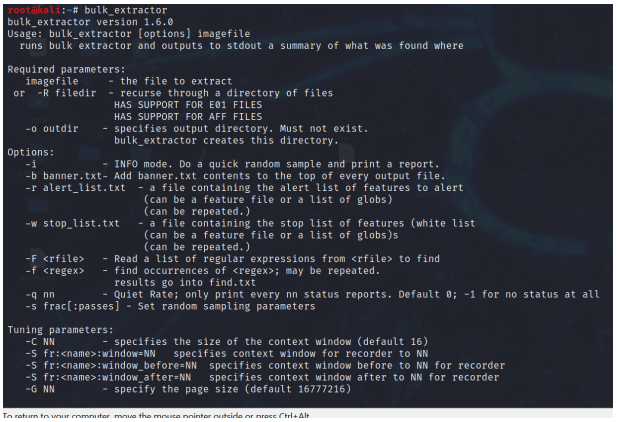


Figure 12: Bulk extractor CLI view

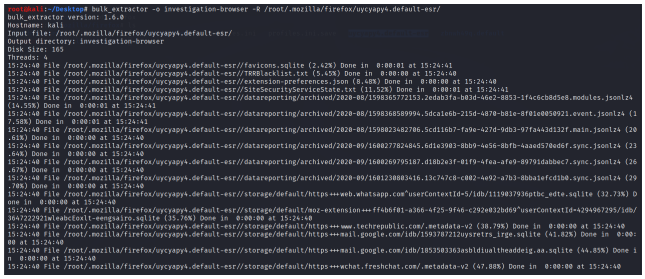


Figure 13: Bulk extractor performing data extraction

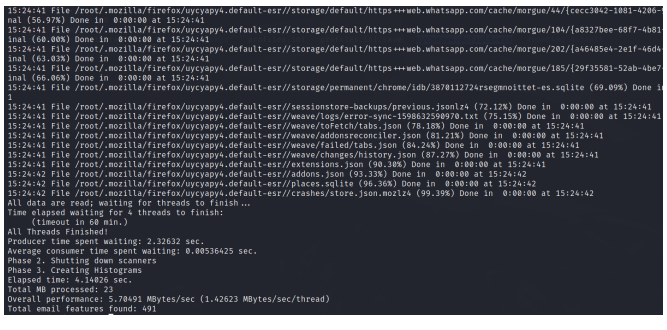


Figure 14: Bulk extractor data

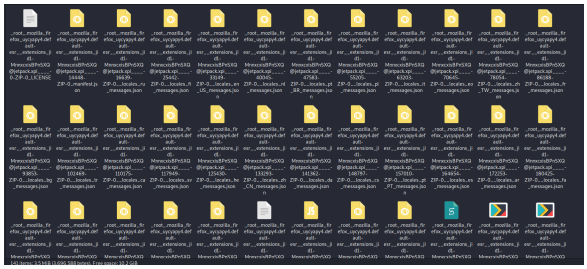


Figure 15: Folder created by bulk extractor

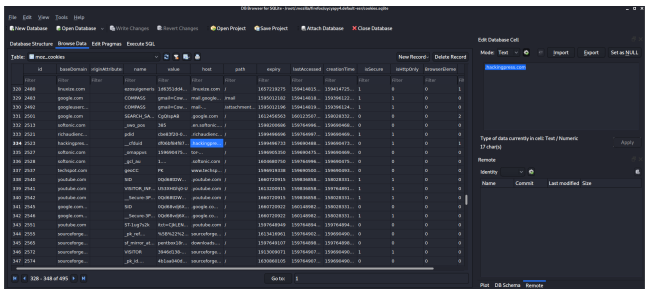


Figure 16: Data of SQLite DB

in folders shown in Figure 15.

Here from the above screenshot, it can be seen that there is the extension (add-ons) of the privacy modes of web browser that is been missed by the dumpzilla. Also with this tool, the shreds of evidence are authenticated and provide us all the details, and helps in compiling all the data. Now with auxiliary SQLite DB browser, we get some information as Bulk extractor also saves data in the files of SQLite database, shown in Figure 16.

By seeing the details on the database created by the SQLite, it gives all the necessary information which was created by the Bulk extractor. Here as focusing on the cookies in Figure 17, many of them are captured for leading the investigation.

The dumpzilla missed this extension information, but the auxiliary database of SQLite is recovered. Ending this discussion here that in the forensic lab setup different tools are utilized to get the data identified from the related study. First dumpzilla is utilized to collect the important evidences and mentioned above. Then Bulk extractor is used to get the information that the dumpzilla

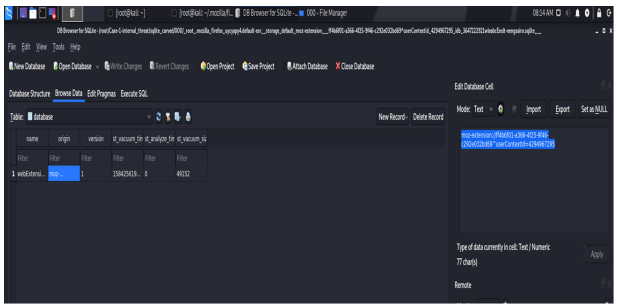


Figure 17: Data analytics from SQLite DB

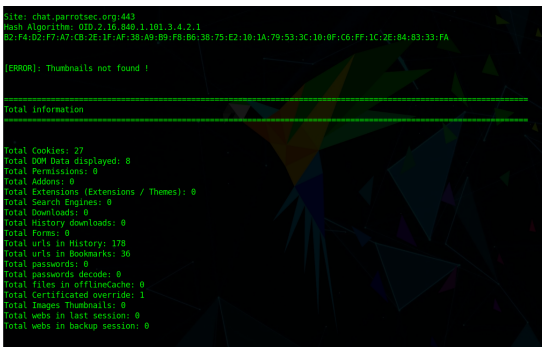


Figure 18: Total information gathered in Parrot OS

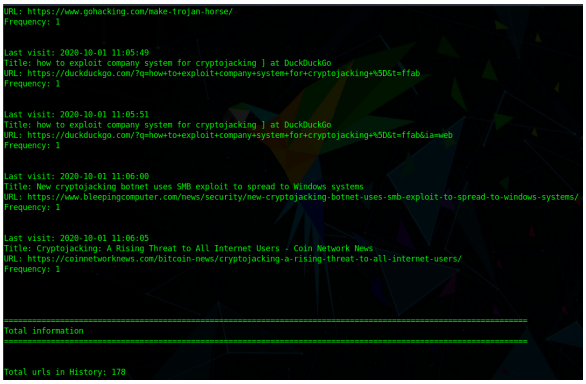


Figure 19: History extraction in Parrot

cannot trace. It not only extract the evidence but also gives the log data in the folder. Then SQLite data base is utilized to get the details about the cookies and the extension that missed by dumpzilla.

As far as the precious information is gathered from utilizing the tools of digital forensics in the previous section. Now comes the part of analysis and authentication of these factors and evidence. For making the investigation precise, the same tools and techniques are run on another operating system, the "Parrot". Parrot Security OS is also a compatible system for penetration testing and digital forensics research. It's the competitor of Kali Linux here in this research it is utilized to get authentication of all the gathered data and evidences. The same investigation is run on parrot OS.

4.4 Investigation in Parrot OS

Starting with the Parrot OS, it's also linux system that has debian system. Provides many tools for ethical hacking as well as digital forensics. The same dumpzilla is run on Parrot to get the results and compare with the results of Kali to verify the evidence collected. Staring with the extraction of history and then compare the results for authentication. Attaching the history snapshot from parrot OS in Figure 18.

As mentioned above in Figure 19, Parrot extracts the same results from the Kali Linux by the dumpzilla. Now summarize the results from both Kali Linux and Parrot

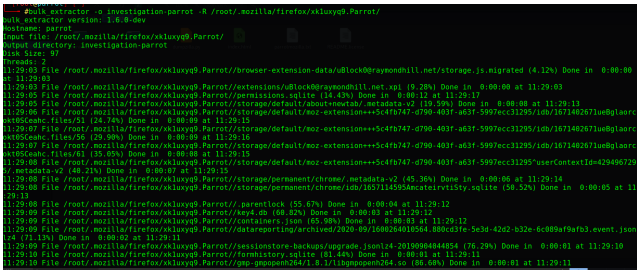


Figure 20: Bulk extractor CLI view in Parrot

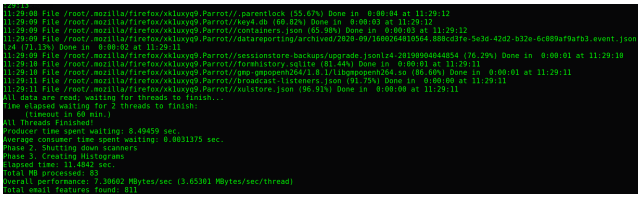


Figure 21: Bulk extractor data extraction

is as in Table 4.

Table 4: Analysis of evidence extraction from both OS

Kali Linux	Parrot Security OS
.onion routing	Trojan Horse Installation
tor browser	Exploiting enterprise Database
Phishing attacks to target company CEOs	Access Dark web with tor browser
Malware installation	Phishing attacks to target company CEOs
Exploit company machine	Cryptojacking
Darkweb	Tor browser

From the above comparative analysis, it shows that the results are almost the same. Duplicate history titles have been extracted from both Kali Linux and Parrot Security OS. After getting the same effect of accessing Tor browser and exploiting enterprise databases and botnets. It has been confirmed that the internal malicious user has some connections with dark web users and tries to sell the company's sensitive data on the dark web. Now dumpzilla comparison is verified, moving towards the comparison of bulk extractor results. The same Bulk extractor tool is run on Parrot to find out the email features that were missed from the dumpzilla. In Figures 20 and 21 shows the result of Bulk extractor.

Analyzing the above, it's found out that there might be some glitch in dumpzilla running on Kali Linux because it has missed the count of verified emails from here. Now check the folder that is the key feature of Bulk extractor that it creates a folder and log all the files of the directory. The attached snip of Figure 22, the folder created by the Bulk extractor in Parrot:

Here it can be seen that the Bulk extractor in Parrot might have missed the extensions that it has captured

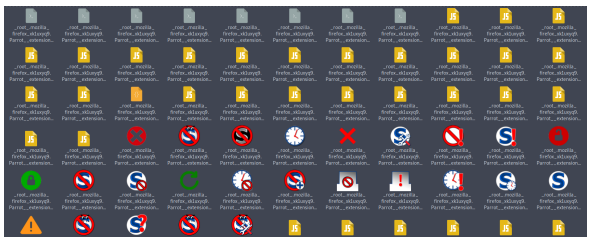


Figure 22: Folder created by Bulk extractor

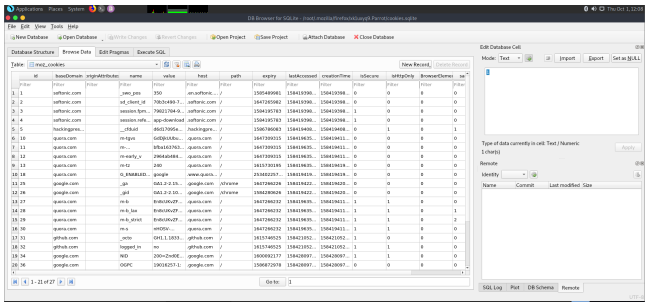


Figure 23: SQLite DB browser data

in Kali Linux. Comparing both and getting verified step by step, some glitches in running tools on the different operating systems are missing evidence. But running the same tool on different platforms gives us the advantage of covering each other's drawbacks. Like if dumpzilla missed any evidence Bulk extractor captured it, and so on. Now the last step is to get the auxiliary information of the SQLite database browser, which keeps the log of all files of the browser is shown in Figure 23.

It can be seen that SQLite Db in Parrot did not capture all the cookies as it logs the details of cookies so here, Kali Linux overcomes the Parrot gives verified details of the Cookies, which helps in leading the investigation.

In concluding the experimental analysis chapter, there is a need to mention the importance of web browser forensics in digital forensics again. Every cyber-criminal activity starts with the web browser because it is the gateway to get anywhere on the internet, especially in the dark web. From the related study, the authors are going in various directions. In contrast, after a thorough study, it is found that these different skills might be a problem for investigators as most of them are not experienced in programming. So, this research adopts the approach of utilizing digital forensics tools to get the identified outcome or variables. Then comes the problem of authentication and verification of tools results. For this purpose, the same tools run on two different platforms in Kali Linux and in Parrot OS. In analyzing and comparing the results, some things are missed by tools in Kali that are overcome by the same tool when it runs on Parrot and vice versa. In the end the experiment becomes successful in extracting data Cookies, URLs, history details, etc. The same information is gathered from the other computers of the department is extracted, and results are compared if the browsing activity of computer slangs been matched, then

the culprit is caught in the virtual scenario who have exploited the browser.

5 Observations and Key Findings

In light of all the results from the experimental analysis, it's been observed that malicious users exploited the browser. By following the history extracted from the victim machine, it's been observed that the user continuously tried to access the dark web from inside the department. Based on these browsing activities it can easily be observed the malicious intentions of the user. The script of dumpzilla written on python is designed on the basis of access control. There is different access of different features and directories of machine. If there are rights from admin, only superuser or admin can add or delete if there is user login on the machine than user cannot install or delete program inside the machine. A US patent (United States Patent No. US10579995B2, 2020) Elaborated about the access control in which the device's utility is extended by allowing the user to get full access of the device. This can become the reason of exploitation because the system administrator allows the maximum access to increase the utilities and boost up the performance of work from the employee. But this also questions the security of the system. If the administrator allows some of its access rights to the users or employees, it jeopardizes the security. No mechanism can find the malicious intentions of the user. In this case, this maximum access control becomes the vulnerability of the system's security, and the user exploited the browser exploiting his full access to the sites. The SA should harden the system according to the standard operation of procedures (SOPs) by the vendor whose devices are being used by the enterprise. If the department is using windows server 2016 than the system administrator should follow all the SoPs for hardening of server as provided by Microsoft (Microsoft, 2017). In most digital forensics cases, it's been coming out in the investigation that there is no following of the SoPs for hardening the system administrator system. Thus, this carelessness most of the time from IT department becomes a vulnerability. This, when being exploited by someone inside becomes the risk and ends up in losing a lot of sensitive data and private information. As discussed by the (Zang, 2019), machine learning-based systems detect suspicious behaviour from internal users based on denoising autoencoders. As this is not the domain of this research but giving this suggestion based on related study and from the experimental analysis, the main reason that leads towards the exploitation of web browser is not following the SoPs for the hardening of the system.

Digital forensics comes at the part of auditing and investigating of the systems and databases. As this research is conducted on the virtual environment in which browser is being exploited and investigation is conducted to find out the evidence which is being analyzed to predict the linkages of malicious user in the dark web, this finding leads to further investigation to the malicious user. In light of related study and results from the experimental analysis, the key findings are being summarized as follow:

- The major finding is the weakness in the systems. In many enterprises most of the systems are not properly hardened which leads vulnerability and after that it is exploited by the internal malicious user.
- The script of Dumpzilla is written in python, which focused on the access control techniques. Although there is logging of all the browsing activity data in the system hard drive which can be extracted by utilizing disk image extractor method or by getting files through directories.
- Disk image method may fails when the disk is damaged. But here in this research directory of file gives the advantage as it locates the exact position of data stored in the hard drive to extract the evidences like history URLs, cookies, extensions, add-ons despite the fact that the web browser data is being vanished.
- There might be some data that is being missed by the Dumpzilla so another tool bulk extractor is used in assistance of main tool.
- Bulk extractor tool not only provides the utility of extracting evidences but also it makes the case folder in which it saves all the evidences.
- Than SQLite browser that saves all the browsing gives some auxiliary information about the evidences.
- For checking the authenticity and verification of the evidences collected, the same tools are run on two different platforms Kali Linux and Parrot Security OS.

It's been found out that both platforms provide different utilities, while comparing the data gathered it almost the same but there are some limitations that Bulk extractor missed some files in running on Parrot as compare to Kali.

6 Conclusion and Discussion

In the process of this research, first, we did the theoretical implementation. Relevant papers, articles, book sections that are readily available on the internet is studied to identify the research problem. In this qualitative part of the research, previous studies' findings include email forensics that gives information about phishing attacks. This phishing was exploiting the user machine by using it resources. There is a discussion on web browser forensics that most authors extract artefacts and evidence with different techniques, as mentioned in the related study portion. These studies provide the various ways of extracting the same data, collecting data from previous research, and analyzing the details; this research goes with finding the

simple method for extracting the evidence. Also, there is a discussion of legal and technical aspects of digital forensics that an investigator must be aware off.

After identifying the research problem in an organization, an internal malicious user leaked the confidential information on the web by exploiting the browser and deleted all his/her footprints. For that purpose, a forensics investigation needs to extract all the evidence like history, cookies and saved passwords from the cloud space provided by the browser. So, an experimental setup is being arranged in a virtual environment. The lab is set up in two different Kali Linux and Parrot Security OS platforms for the quantitative part. The forensics tools like dumpzilla and bulk extractors are used. SQLite database is used in auxiliary with these tools to get the required information. The target data to capture is History, URLs, Cookies, Sessions, Add-ons, Extensions, etc. Two different platforms were used to verify the authenticity of the evidence collected. The dumpzilla is missing some data and bulk extractor in Kali, and some is missed when the same tools run on Parrot OS. So in this way both platforms fills each other's gaps that arise in research. After that the mixed method research is completely conducted when the data from the victim machine is being matched with another machine and the user of that machine is being captured for further investigation

6.1 Contributions of Research

As discussed earlier in chapter three that research can go in both ways. Either it leads to the solution of identified problem via procedural steps (may be qualitative or quantitative or both). In this type the solution acquired from the study or experimental results is the contribution of the research. In other words, after identifying the problem when the procedural steps, tools and suggested techniques do not lead towards the required solution. It still considers contribution because the authors saved the time of other researchers by giving a vast literature review and guide about the path to save the time of other researchers.

This research is being adopted and going with the mixed method. The main contribution is providing the path for leading the digital forensics investigation with the help of tools including dumpzilla, Bulk extractor, and SQLite database browser. After identifying the problem with the related study, it's been said that the browser is the gateway for the whole internet. Where you want to go on the internet, the gate is from the web browser. So browser is the most vulnerable part it needs to be secured. A virtual environment is set up in which a scenario is created where a machine's browser exploits malicious activity. To verify results were generated from the experimental analysis, the same tools are running on two different platforms, and the results are analyzed. The major contribution is finding out the carelessness of enterprises that they do not follow the standard operational procedures for hardening systems. Summarizing the contributions as in Table 5.

Table 5: Contributions of research

Contributions	Type of Study
Enterprise not following the SoPs for system hardening	Qualitative and Quantitative
Dumpzilla script focused to get the root access in the system	Quantitative
Providing solution with utilizing tools of digital forensics	Qualitative
Authenticating evidences by running tools on different platforms	Quantitative

6.2 Conclusion

In concluding all the research discussed in the research, it is supposed that web browser forensics has sound importance in digital forensics research. As mentioned in a related study, discussing work on authors is from using browser forensic tool, running browser forensics on the android toolkit, and suggesting techniques on avoiding phishing attacks via emails to the legal and technical aspects of digital forensics research. All this done in the qualitative part of the research identifies the importance of browser forensics and identifies the problems in running an investigation. After a thorough study of the related articles, this research approach utilizing digital forensics tools dumpzilla, Bulk extractor and SQLite were selected for analysis. In the quantitative part, a virtual environment was set up, moving with the assumption that the investigators traced the victim machine's IP while reaching that machine. The web-browser data is vanished by the malicious user. Then investigation runs on two different platforms including Kali Linux and Parrot Security OS to authenticate the evidence collected from the experimental analyses. The data collected from all the devices in the department then it's compared. The culprit is caught when the victim machine's data was matched with the PC in the department, and the user is caught for further investigation. It has also been found out that the main vulnerability is the enterprise not following the standard operating procedures for system hardening.

6.3 Limitations of Study

Every research has limitations, in this research so far it has achieved the targets of extraction of data from the web browser. But the tools has its limitations like in conducting the investigation dumpzilla has missed the extensions saved in the browsers. Although these extensions get extracted by the Bulk extractor, it still did not extract all the saved extensions. Also, the SQLite has missed some

URLs that being visited by the malicious user. Also, there are still many ways to get this research conducted as it can be more study of related articles.

6.4 Scope of Future Work

In the future study of this research, there is scope for good python programmers and computer experts who are aware of the software architecture and the architecture of operating systems. Also, research in access control is required as this research focuses on getting deep into the system to extract the evidence. A good python programmer makes the script of an existing tool more improved, plus the sound knowledge of operating systems and access control can penetrate deep into the systems. With the combination of all these, research can be conducted on the weaknesses of dumpzilla, and bulk extractors and new tools can be developed that can do similar tasks better.

References

[1] E. Akbal, F. Günes, A. Akbal, " Digital forensic analyses of web browser records," *Journal of Software*, vol. 11, no. 7, pp. 631—637, 2016.

[2] M. Asim, M. F. Amjad, W. Iqbal, H. Afzal, H. Abbas, Y. Zhang, "AndroKit: A toolkit for forensics analysis of web browsers on android platform," *Future Generation Computer Systems*, vol. 94, pp. 781-794, 2018.

[3] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, I. Mavridis, "D41 - Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, pp. 22-31, 2020.

[4] H. Graeme, " Part 1: Quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework," *Forensics Science International: Reports*, vol. 2, pp. 123-133, 2020.

[5] G. Horsman, B. Findlay, J. Edwick, A. Asquith, K. Swannell, D. Fisher, P. McKain, " A forensic examination of web browser privacy-modes," *Forensic Science International: Reports* , vol. 1, pp. 22-29, 2019.

[6] N. A. Hassan, "Web browser and e-mail forensics," in *Digital Forensics Basics*, pp. 247–289, 2019.

[7] M. R. Jadhav, B. B. Meshram, "Web browser forensics for detecting user activities," *International Research Journal of Engineering and Technology*, vol. 5, no. 7, pp. 273—279, 2018.

[8] A. A. Jillepalli, de Leon, D. Conte, S. Steiner, J. Alves-Foss, "Analysis of Web Browsing Security Configuration Options," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 12, pp. 6139—6160, 2018.

[9] K. Parsons, M. Butavicius, P. Delfabbro, M. Lillie, " Predicting susceptibility to social influence in phishing emails," *International Journal of Human-Computer Studies*, vol. 128, pp. 17—26, 2019.

[10] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, M. Bailey, "Outguard: Detecting in-browser covert cryptocurrency mining in the wild," in *The World Wide Web Conference*, pp. 840—852, 2019.

[11] Y. Kwak, S. Lee, A. Damiano, A. Vishwanath, "Why do users not report spear phishing emails?," *Telematics and Informatics*, vol, 48, 2020.

[12] S. Mahaju, T. Atkison, " Evaluation of firefox browser forensics tools," in *Proceedings of the South-East Conference* , pp. 5—12, 2017.

[13] N. Mays, C. Pope, "Quality in qualitative research," *Qualitative Research in Health Care*, Chap. 15. pp. 211-233, 2019. (`https://doi.org/10.1002/9781119410867.ch15`)

[14] M. Munir, P. Leimich, W. J. Buchanan, "A forensic audit of the tor browser bundle," *Digital Investigation*, vol. 29, pp. 118-128, 2019.

[15] A. Nalawade, S. Bharne, V. Mane, " Forensic analysis and evidence collection for web browser activity," in *International Conference on Automatic Control and Dynamic Optimization Techniques*, pp. 518—522, 2016.

[16] F. Paligu, A. Kumar, H. Cho, C. Varol, "BrowSt-Explus: A tool to aggregate IndexedDB artifacts for forensic analysis." *Journal of Forensics Science*, vol. 64, no. 5, pp. 1370—1378, 2019.

[17] R. Parkavi, S. Anitha, R. Gayathri, *Digital Steganography Security*, Critical Concepts, Standards, and Techniques in Cyber Forensics, *IGI Global*, pp. 33-41, 2020.

[18] C. Parulekar, " Minimize phishing attacks: Securing spear attacks," *International Research Journal of Engineering and Technology*, vol. 6, no. 6, pp. 3054-3058, 2019.

[19] J. S. Queiroz, E. L. Feitosa, "A web browser fingerprinting method based on web audio API," *The Computer Journal*, vol. 62, no. 8, pp. 1106—1120, 2019.

[20] A. Reed, M. Scanlon, N. An Le-Khac, " Private Web Browser Forensics: A Case Study of the Epic Privacy Browser," *arXiv preprint arXiv:1708.01732*, 2017.

[21] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, pp. 1—13, 2018.

[22] N. Shafqat, "Forensic investigation of user's web activity on google chrome," *International Journal of Computer Science and Network Security*, vol. 1, pp. 67-75, 2016.

[23] P. Snyder, C. Taylor, C. Kanich, "Most websites don't need to vibrate: A cost-benefit approach to improving browser security," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 179-194, 2018.

[24] Y. U. Sonmez, A. Varol, "Legal and technical aspects of web forensics," in *7th International Symposium on*

Digital Forensics and Security (ISDFS'19), pp. 1—7, 2019.

[25] X. Zhang, T. T. Yuen, K. K. R. Choo, "Experiential learning in digital forensics," in *Digital Forensic Education*, Springer, pp. 1–9, 2020.

Biography

Sirajuddin Qureshi received his bachelor's degree in Computer Sciences from Quaid-e-Awam University of Engineering, Science & Technology, Pakistan. Afterwards, he pursued his Master's in Information Technology from Sindh Agricultural University Tandojam, Pakistan. Currently he is pursuing PhD in Information Technology at Beijing University of Technology, China. He has nine research publications to his credit as main author and co-author, which featured national and international journals and conferences. Sirajuddin's research areas includes but not limited to Network Forensics Analysis, Digital Forensics, Cyber security, Computer Networks and Network Security.

Jingsha He received the bachelor's degree in computer science from Xi'an Jiaotong University, China, and the master's and Ph.D. degrees in computer engineering from the University of Maryland, College Park, MD, USA. He worked for several multinational companies in USA, including IBM Corp., MCI Communications Corp., and Fujitsu Laboratories. He is currently a Professor with the Faculty of Information Technology, Beijing University of Technology (BJUT), Beijing. He has published more than ten articles. He holds 12 U.S. patents. Since August 2003, he has been published over 300 papers in scholarly journals and international conferences. He also holds over 84 patents and 57 software copyrights in China and authored nine books. He was a principal investigator of more than 40 research and development projects. His research interests include information security, wireless networks, and digital forensics.

Saima Tunio received the BSIT (Hons) with gold medal from Sindh Agricture University Tandojam, Pakistan. Afterwards, she pursued her MSIT from Isra University Hyderabad, Pakistan. Currently she is pursuing PhD in Information Technology at Beijing University of Technology, China.She has more than five research publications to her credit as main author and co-author, which featured national and international journals and conferences. Saima's research areas includes but not limited to Information security.IoT security, Digital Forensics, Cyber security, Computer Networks.

Nafei Zhe received the B.S. and M.S. degrees from Central South University, China, in 2003 and 2006, respectively, and the Ph.D. degree in com- puter science and technology from the Beijing University of Technology, Beijing, China, in 2012. She was a Postdoctoral Research Fellow with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, from 2015 to 2017. She is currently an Associate Professor with the Faculty of Information Technology, Beijing University of Technology. She has published over 20 research papers in scholarly journals and international conferences. Her research interests include information security and privacy, wireless communications, and network measurement.

Faheem Akhtar received his Ph.D.degree from the Beijing University of Technology, China,in 2020.He is currently working as an Assistant Professor with the Department of Computer Science, Sukkur IBA University, Pakistan.He is the author of various SCI, EI, and Scopus indexed journals and international conferences.He is part of various indexed international conference at different positions and a Reviewer of various SCI, EI, and Scopus indexed journal. His research interests include data mining, machine learning, deep learning, information retrieval, privacy protection, Internet security, the Internet of Things, and big data.

Faheem Ullah received the M.S degrees from the Xian Jiaotong University, China,in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include information security, Blockchain and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.

Ahsan Nazir has received his M.Sc degree from University of Engineering and Technology Lahore in 2016. From September 2015 to August 2018 he worked as software Engineer at Dunya Media group Lahore since September 2018 he is doing PhD in Software Engineering from Beijing University of Technology , Beijing China. He has published more than 10 journals and conference papers.His area of research include eGovernment,IoT,Software Engineering and Machine learning applications.

Ahsan Wajahat received the B.S. and M.S degrees in information technology from the Sindh agriculture University, Pakistan, in 2012 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include machine learning, information security, forensic network and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.

Formal Security Analysis of OPC UA Protocol in Industrial Control System

Tao Feng, Zhuang-Yu Ma, and Jun-Li Fang
(Corresponding author: Zhuang-Yu Ma)

School of Computer and Communication, Lanzhou University of Technology
Lanzhou,Gansu 730000,China
Email: 530901638@qq.com

(Received Aug. 30, 2021; Revised and Accepted Apr. 3, 2022; First Online Apr. 23, 2022)

Abstract

The OPC UA is a protocol used in the interaction between factory equipment. It is also widely employed in the industrial Internet industry, where long-distance data sharing and transmission between devices, multi-device interconnection, etc., must be realized. Therefore, it is essential to study the security of industrial control system protocol. However, most previous research on industrial control protocols mainly focuses on realizing the security of the protocol itself, lacking formal modeling and security evaluation, leading to some research gaps. Based on the previous colored Petri net theory, combined with the Dolev-Yao attacker model, this paper tries to make targeted improvements to analyze the security of the OPC UA protocol. First, based on the colored Petri net theory and CPN Tools, the security mechanism of the protocol is verified for consistency. Then the Dolev-Yao attacker model is introduced to evaluate the security of the original model of the protocol. By analyzing the security mechanism of the protocol, some issues, including the security of random numbers in OPC UA protocol and the deceptive attack of identity authentication attributes, have been found. Besides, some corresponding improvement projects are given. Finally, we used CPN Tools to verify the security of the new project. We also found that adding the recipient's public key to the message and the key packaging mechanism can effectively prevent attacks against the protocol, improving the protocol's security.

Keywords: Colored Petri Nets; Formal Analysis; Key Packaging; OPC UA Protocol; Security Evaluation

1 Introduction

With the gradual integration of informatization, industrial control systems are widely employed in many fields in a country and have become the focus of many countries to improve their comprehensive national strength. The OPC UA protocol are widely used, providing communicative connections for both mutually independent factory equipment and platforms.Since the Stuxnet attack occurred in 2010, the global industrial control system attack incidents have shown a spurt of growth [25], Industrial control security has already become an issue that cannot be ignored by government agencies. The security of industrial control systems is related to national strategic security,to a certain extent.Therefore, security has become the top priority of OPC UA protocol to expand the scope of use.

Industrial control systems differ from other systems.Due to the long lifespan of equipment and having difficulty in repairing vulnerabilities, the security must be carefully checked before deploying protocols and standards.Igure [11] and Patel [20] and others emphasized the lack of formal verification of traditional industrial protocols,and pointed out that formal verification is very important for evaluating the security of the protocol and discovering the loopholes of the protocol.Therefore,it is significant for both the formal analysis of OPC UA protocol and the security of OPC UA protocol.

The main contributions of this article include three aspects:

1) Adopt a detection method based on the previous colored Petri net theory and the Dolev-Yao attacker model;

2) Because of the extreme importance of two subprotocols of the OPC UA handshake, including Open Secure Channel and Create Session, hierarchical colored Petri nets (HCPN) for formal modeling, they will be employed to make analysis and verify the consistency of the sub-protocol models. Introduce the Delov-Yao attacker model to evaluate the security of the sub-protocols, and discover attacks against the sub-protocols;

3) As to the attack on the sub-protocol, the author proposes a security enhancement scheme, where the recipient's public key to the message is added, a key wrapper mechanism to prevent the identity of the random number from being deceived and forged is used and the security the new scheme is verified.

2 Related Work and Theories

Most of the researches on the security of industrial control protocols is limited to the written norms of human language and the realization of its own security, lacking the use of formal methods to be verified. The methods of formal analysis of the protocol mainly include modal logic, theorem proof, type checking and model checking. Although the modal logic method adopted in the literature [14] can verify whether the protocol meets its security goals through a series of reasoning, the logic is too abstract, leading to covering the state information of the protocol, the message exchange and aggressive behavior of the protocol cannot be described in more detail. Literature [22] analyzed the advantage of the theorem proving method, namely, being able to analyze the operation of infinite subjects participating in the protocol. Besides, the disadvantage of the method is that the process cannot be fully automated and requires manual intervention.

Literature [7] pointed out that the type detection method can verify the security properties of the protocol, but cannot find out the aggressive path. Literature [4] pointed out that the model checking method can verify whether the protocol meets the security properties, but cannot verify the correctness of the protocol and it also causes the problem of state space explosion. In terms of theoretical research, the author introduced the security mechanism of OPC UA protocol in parts 2, 4 and 6 of the technical document of OPC unified architecture [12,13,17]; Literature [10] deeply interprets the security issues of OPC UA and proposes security optimization strategies; Literature [21] uses Proverif, an encryption protocol verification tool, to check the security properties of the OPC UA protocol; Literature [6] introduced remote authentication and hardware authentication-based encryption to OPC UA, improving the security of OPC UA client-server communication; Literature [16] studied the security status of OPC UA,improving the communication efficiency by improving the encryption efficiency.

Compared with the previous researches, based on the colored Petri net theory and an improved Dolev-Yao attacker model, a detection method is proposed to analyze the security of the protocol, verify the consistency of the protocol model, then introduce the attacker model to evaluate the security of the protocol, propose a targeted security enhancement scheme for the evaluative results, and finally verify the security of the new scheme.

2.1 Overview of OPC UA Protocol

OPC UA, namely, OPC unified architecture, is a new industrial control protocol based on Web services, which was extended in the basis of traditional OPC foundation. Besides, it has been widely employed in long-distance interaction between factory equipment and multi-device interconnection. It also has the functions of cross-platform, integrated address space, encapsulation of general service interfaces, and definition of security models [9,18]. What differs from the traditional OPC protocol is that the OPC UA protocol can realize the long-distance data exchange of various industrial systems and equipment through the Internet, realize the communication between the client and the server and meet the needs of data exchange at all levels of the industrial control system.

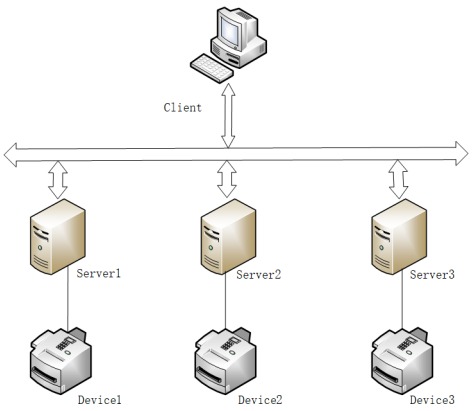


Figure 1: OPC UA communication mode

The communication mode of OPC UA agreement is shown in Figure 1 The client makes a service request, and the server receives the request from the client, performing a series of operations in the address space, and giving a response through the API. It can be seen that the communication method of OPC UA is closer to the modern communication method, which is more conducive to system management and application development.

2.2 Introduction to OPC UA Security Mechanism

Industrial Control System (ICS) not only needs to realize the real-time transmission of control data, but also ensure the safety of data during the transmission process. Therefore, in the application of OPC UA in the field of industrial control, security is of the extreme importance. OPC UA defines a security model in order to ensure the communication security of OPC UA, as is shown in Figure 2.

The OPC UA security model can be divided into three layers. The bottom is the transport layer, which is the basis for ensuring security communication, and is also one that is easier to be attacked, such as a denial of service attack; What is a bit higher than the transport layer is the communication layer where the secure channel can be established. The communication layer adopts asymmetric encryption, digital signature and other technologies to ensure the confidentiality and integrity of the channel. At the same time, identity authentication and authorization mechanisms are used to ensure the authenticity of communications; The top one is the application layer. Based on the secure channel, the client and server make a communication at the application layer through negotiation, which is used to transmit real-time data and operate in-

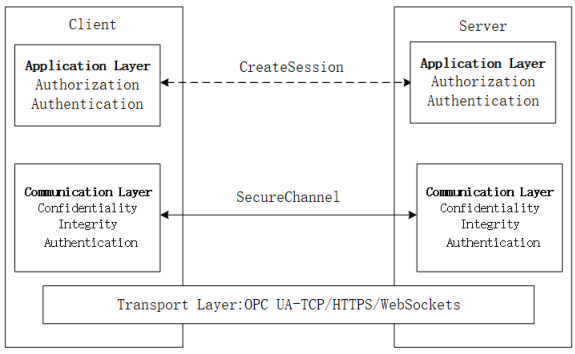


Figure 2: OPC UA security model

structions between devices. Making a communication can verify and authorize the client's identity.

This security model provides a certain foundation for the security of OPC UA, and provides guidance for analyzing the security of the two handshake sub-protocols of OPC UA.

2.3 Colored Petri nets and Modeling Tools

German scientist Carl Adam Petri first proposed the concept of Petri net and then many extensive concepts appeared, such as time Petri net, stochastic Petri net, CPN, etc. [1, 15, 24] Colored Petri Nets (Colored Petri Net, CPN) is an advanced form of traditional Petri Nets. Compared with Petri Nets which has no concept of types and modules, CPN has various advantages, including a variety of types, complicated operative data, rich and flexible color sets, definitive types of the function and the ability to describe hierarchical structures. Besides, it can provide the operative interface. These can be conducive to giving standardized definition of message flow models, which can be used to describe and analyze communication, distribution, and Protocols and systems with features such as synchronization and concurrency.

CPN Tools is a system modeling analysis tool developed by the Aarhus University team in Denmark. The model description language is composed of Petri net diagrams and CPN ML programming language. It uses good man-machine interface technology to perform graphical user interface (GUI) design. It also has functions of incremental syntax checking and code generation. It can be edited, simulated, used to analyze the state of space and other features of the model and can accurately locate errors in the model through the feedback mechanism, which ensures the correctness of the model to a certain extent. In addition, it also supports for time CPN and hierarchical CPN. With the help of CPN Tools, users can not only model easily, but also simulate and analyze parallel systems [2, 3].

3 OPC UA Sub-protocol Modeling

Faced with modeling large-scale and more complex protocols with Petri nets, it is more complicated to adopt the traditional CPN model. Therefore, at this time we need to adopt the idea of modular programming, namely, the concepts of substitution transitions and port places in CPN Tools. The network or protocol structure is divided into multiple modules and the network with substitution changes is a multi-level network. We can first establish a simplified network top-level model more broadly and then further refine the sub-pages through the substitution transitions in the top-level model. The layered modeling method can reduce model complexity and improve reusability. This paper divides the OpenSecureChannel and CreateSession sub-protocol modeling into three levels:top level, middle level and bottom level.

3.1 OpenSecureChannel Sub-protocol Message Flow Model

The OpenSecureChannel sub-protocol aims to achieve identity verification between the client and the server by exchanging two secret random numbers and derive a shared key for future communication. In addition, OPC UA has three security modes, including "None", "Signature" and "Signcryption" [19]. "None" shows that the secure channel is in an insecure state and the sub-protocol does not provide any security, but for compatibility. "Signature" means that the private key h(m)sk(x) associated with the OPC UA client certificate can be used for digital signature and the recipient can verify whether the transmitted message has been tampered with by a third party or not. The "signcryption" mode means that the transmitted message is not only signed, but also encrypted by the public key associated with the client certificate. Encryption is used to provide confidentiality for communication and signatures are used to provide authentication and integrity.

The message flow model of this sub-protocol is shown in Figure 3.

Step 1. The client needs to send a Get EndPoints request that asks information about the server;

Step 2. Discovery EndPoint uses the server's public key pk(S), security mode, security policy SP, and user policy UP to make a response, where both SP and UP are used to encrypt primitive negotiation;

Step 3. The client sends a request to OpenSecureChannel the client's public key pk(C), and a random number NC to the server, using the server's public key pk(S) to encrypt and using the client's private key sk(C) to sign;

Step 4. The server sends OSCRes, random numbers N_S, ST, TTL as a response, and uses pk(C) encryption

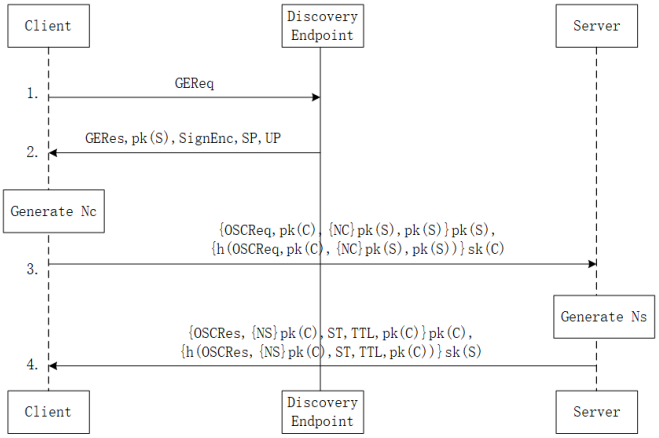


Figure 3: OpenSecureChannel sub-protocol message flow model

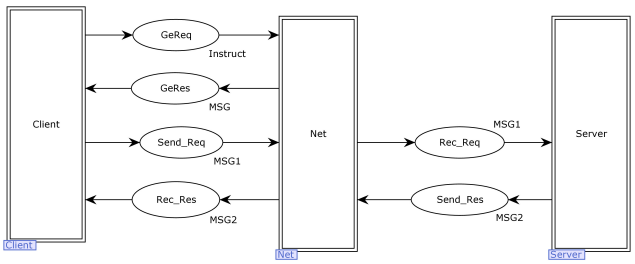


Figure 4: OpenSecureChannel sub-protocol top-level model

and sk(S) signature, where OSCRes stands for the response of the open secure channel, ST stands for the channel identifier, and TTL stands for its life cycle.

3.2 Establishment of OpenSecureChannel Sub-protocol CPN Model

This article is based on the OpenSecureChannl sub-protocol signcryption model of the message flow model for specific modeling.

The top-level CPN model of the OpenSecureChannel sub-protocol is shown in Figure 4, where the interaction process of the sub-protocol is abstractly described on the whole, including the client, server, communication network and transmitted messages of the protocol. In the top-level model of Figure 4, the double-line rectangle stands for the substitution transition and the ellipse stands for the message repository. The substitution transition Client on the left stands for the communication client, the substitution transition Net in the middle stands for the communication network and the substitution transition Server on the right stands for the server.

The middle model of this sub-protocol consists of 4 substitution transitions and 7 places which are shown in

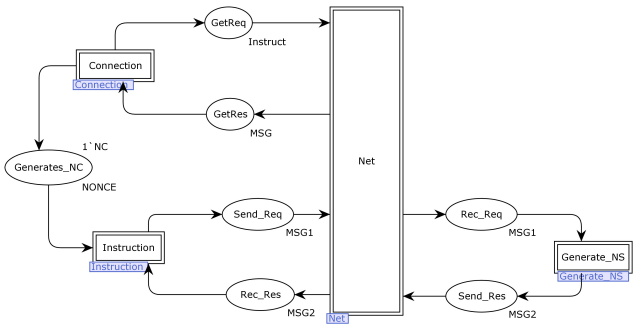


Figure 5: The middle layer model of the OpenSecureChannel sub-protocol

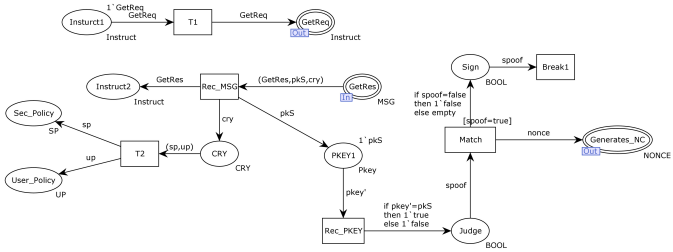


Figure 6: The internal model of the substitution transition Connection

Figure 5. The process of achieving connection information between the client and the server is represented by the substitution transition Connection; The process in which the client sends an OpenSecureChannel request instruction to the server is represented by the substitution transition Instruction; The process of generating random numbers from the server to the client is represented by the substitution transition Generate_NS.

The bottom model of this sub-protocol includes 4 parts. According to the order of interaction between the client and the server, the connection establishment, request instruction and random number generation will be introduced as fully as possible. The internal model of the substitution transition Connection is shown in Figure 6. Transition T1 is used to make a request for information from the server and the response message from the client is received by the place GetRes through the transition Rec MSG processing, the received server's public key pk(S) is received through the transition Rec_PKEY. It is verified by Transition Match. After the verification is correct, the storehouse GenerateNC generates a random number N_C. If the verification fails, the operation will be ended.

Figure 7 depicts the internal model of substitution transition Net. The transition DisEndPoint simulates the transmission path where the client sends a request to the server to obtain terminal description information, the transition OSCReq and OSCRes, respectively, simulate the transmission path of the client initiating the OpenSecureChannel makes a request for information to the server

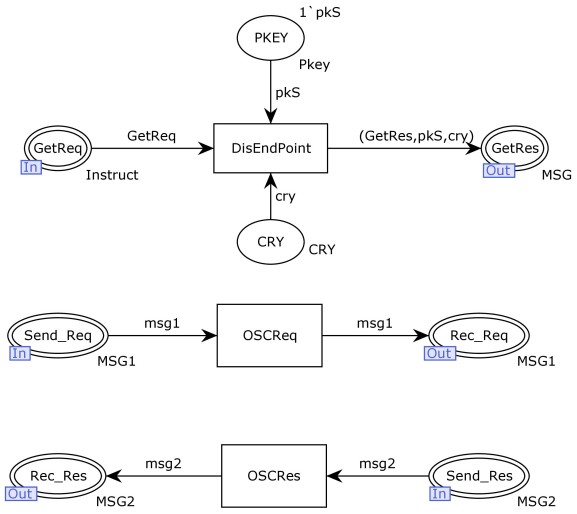


Figure 7: The internal model of the substitution transition Net

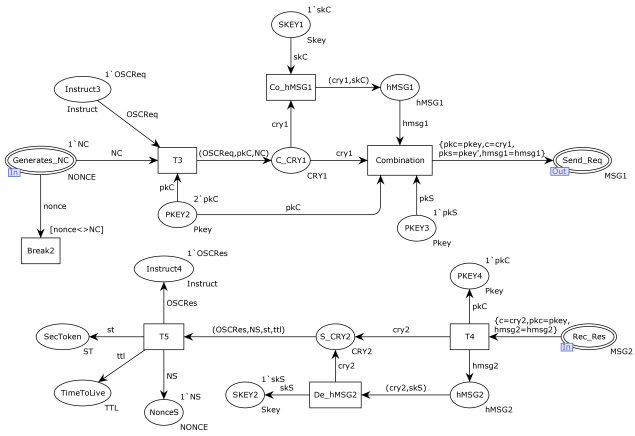


Figure 8: The internal model of the substitution transition Instruction

and the transmission path of the server in response to the request information to the client.

Figure 8 depicts the internal model of the Alternative Transition Instruction. Random number N_C is generated by the repository Generates_NC, transition T3 integrates the random number N_C that has been received, client public key pk(C) and request OSCReq. Transition Combination combines the signed information and encrypted information. Finally, this information is sent to the server through the repository Send_Req; transition Break2 means that the random number N_C has been received, verification failed to perform the termination operation, The place Rec_Res is used to receive the data information sent by the server. Transitions T4 and T5 decompose the received safety data.

Figure 9 depicts the internal model of the substitution transition Generate_NS. The place Rec_Req is employed to receive the data information sent by the client to the

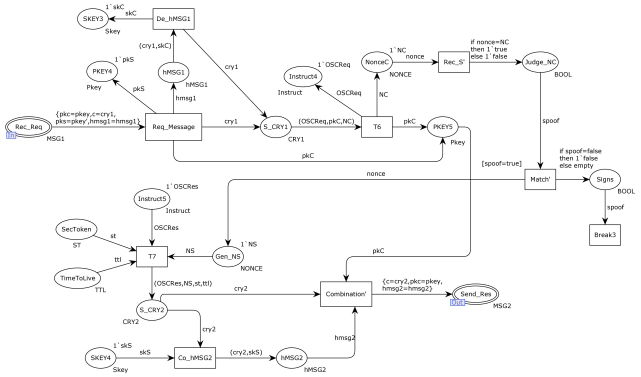


Figure 9: The internal model of the substitution transition Generate_NS

server, transition Req_Message decomposes the security data which have been received and transition Rec_S' verifies the random number N_C which have been received. After the verification is finished, the random number N_S will be generated by the place Gen_NS, If the verification fails, operation Break3 will be ended; Transition T7 integrates the response command OSCRes which have been received, identifiers and its life cycle; transition Combination' combines all the information which have been received; Finally, this information is sent to the client through the place Send_Res.

3.3 OpenSecureChannel Sub-protocol Model Consistency Verification

The analysis tool of state space in CPN Tools will be employed to verify the consistency of the original CPN model of the sub-protocol. We first give the expected results of the original model which was established. The model will successfully perform request, make a response and verify random number where operations are never ended in the process of the entire interaction.

Table 1 shows the results of state space in the original model of the sub-protocol. It can be clearly found that the number of state space nodes, directed arcs and strongly connected nodes and strongly connected arcs is equal, which shows that all state nodes of the original model that were established are reachable. In addition, there are no infinite loops and iterative behaviors in the state space. The number of main state nodes and active transitions are both 0, indicating that there is no reachable state in the original model, and there is no active transition in the active state; The existence of a dead node indicates that any transition under this node are not enabled; There are 3 dead transitions Break1, Break2 and Break3. the transition Break1 means that after the establishment of the connection the operation will be ended once it fails to verify pk(S).The transition Break2 shows the operation is ended because of the error of random number N_C, the transition Break3 stands for the ended operation that generates the failure of ver-

Table 1: State space analysis of the original model of OPC UA OpenSecureChannel sub-protocol

Categorys	Numbers	Name
State space node	30	/
Directed arc	59	/
Strongly connected node	30	/
Strongly connected arc	59	/
Master state node	0	/
Dead node	1	[30]
Death transition	3	Break1/Break2 /Break3
Live transition	0	/

ification of random number N_S. The existence of these three dead transitions reveals there is no failure of operation and verification for the original model and it accords with the expected results.

3.4 CreateSession Sub-protocol Message Flow Model

The clients are allowed to send credentials (username and password) through the secure channel established in the CreateSession sub-protocol.This sub-protocol follows the security model of sub-protocol that is used in the OpenSecureChannel and uses a derived symmetric key. Therefore, the signature will depend on the message authentication code (MAC) once symmetric encryption is used. The message flow model of this sub-protocol is shown in Figure 10. The message sent by the client is encrypted by KSC and signed by KSigcs, and the message sent by the server is encrypted by KSC and signed by KSigsc. Step 1: The client sends a CreateSession request, a random number N_C and the client's public key pk(C) to the server. After encrypting with KCS and signing by KSigcs, the client sends them to the server; Step 2: the server sends SigNc=pk(C),$N_C$sk(S), CreateSession response, random number N_S, server public key pk(S) through signcryption processing and sends it to the client as a response to make a conversation; Step 3: the client uses the signature SigNs of the random number N_S to send pk(C), ActivateSession request and user credentials through signcryption processing, and sends them to the server as a request to activate the conversation; Step 4: the server makes a response for ActivateSession and a fresh random number N_S2, which also undergoes sign cryption processing, as the client, changes the interrogate of the conversation and makes a response when the conversation exceeds the time limit.

3.5 Estabishment of CPN Model of CreateSession Sub-protocol

In this paper, the specific modeling is based on the message flow model of the signcryption mode of the CreateSession sub-protocol.The top-level CPN model of the CreateSession sub-protocol is shown in Figure 11, where the interaction process of the sub-protocol is abstractly described on the whole, including the client, server, communication network and transmitted messages of the protocol. The substitution transitions Client, Net, Server stand for client, communication network and server respectively.

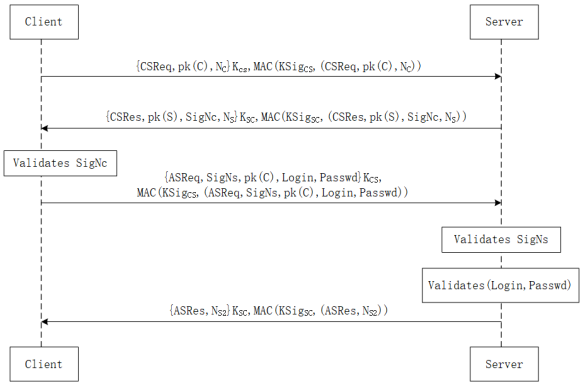


Figure 10: CreateSession sub-protocol signcryption mode message flow model

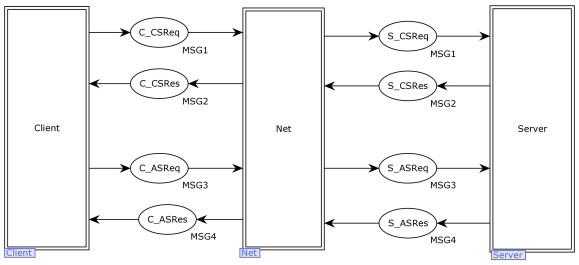


Figure 11: Top-level model of CreateSession sub-protocol

The middle model of this sub-protocol consists of 5 substitution transitions and 9 places which are shown in Figure 12. The process of achieving connection information between the client and the server is represented by the substitution transition CreateSession and CreateSession;The process of activating the session from the client to the server is represented by the substitution transitions ActivateSession and ActivateSession';The Net stands for communication network.

The bottom model of this sub-protocol includes 5 parts. The internal model of the substitution transition CreateSession is shown in Figure 13. Transition T1 integrates the received CSReq, pk(C), and N_C, and transition Combination1 merges all messages which has been received. Finally, it is sent to the server through the place S_CSReq; The place R_CSRes is used to receive the security information sent by the server and the transitions C_CSRes,T2 and T3 are used to decompose the security information which has been received; The transition Re_NC is used to verify the random number NC which has been received. If the verification succeeds,the

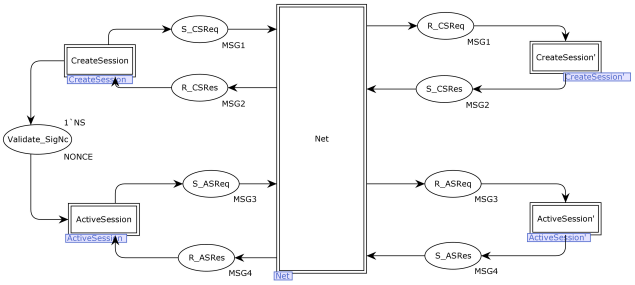


Figure 12: The middle layer model of CreateSession sub-protocol

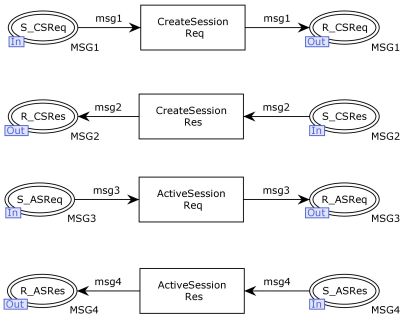


Figure 14: The internal model of substitution transition Net

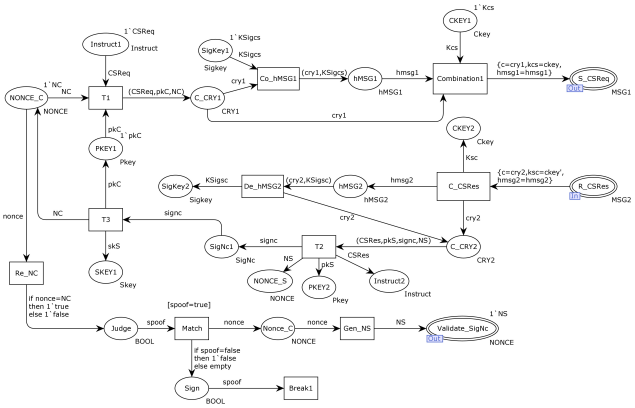


Figure 13: The internal model of substitution transition CreateSession

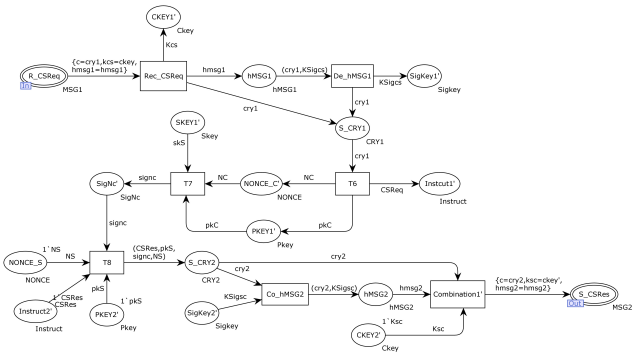


Figure 15: The internal model of substitution transition CreateSession'

Validate_SigNc will generate a random number NS. But if it fails, the operation will be ended.

Figure 14 depicts the internal model of substitution transition Net.The transitions CreateSessionReq and CreateSessionRes imitate the transmission path of the client and server to create the requests for session and response, the transitions ActivateSessionReq and ActivateSessionRes imitate the transmission path of the client and server to activate the session request and response activation respectively.

Figure 15 depicts the internal model of the substitution transition CreateSession'. The place R_CSReq is used to receive the message sent by the client and then it is decomposed by the transition Rec_CSReq, T6, and T7; Transition T8 integrates the random number N_S which has been generated, request for response CSRes, SigNc, and server public key pk(S); Transition Combination1' combines the received information and sends it to the client through the place S_CSRes.

Figure 16 depicts the internal model of the substitution transition ActivateSession. The place Validate_SigNc sends the random number NS that are generated to the transition C_SigNs and then integrates the received keys pk(S) and sk(C).Transition T4 integrates the received activation request ASReq, user credentials login, pwd, and key pk(C), Combination2 will merge all received messages and send them to the server through the place S_ASReq; The place R_ASRes is used to receive the response message sent by the server and it is decomposed by the transition S_ASRes and T5.

Figure 17 depicts the internal model of the substitution transition ActivateSession'. The repository R_ASReq is used to receive the request information sent by the client and decompose it through the transitions S_ASReq, T9, and S_SigNs, the places Vali_User and Vali_SigNs are used to verify user credentials (assuming the user name is "admin" and the password is "123456") and the random number N_S, respectively, If it is successfully verified, the random number N_S2 is generated through the transition Match_User. But if not, the operation Break2 is ended; The transition T10 integrates the received random number N_S2 and the activation response ASRes, merges them by the transition Combination2' and sends them to the client through the place S_ASRes.

3.6 Consistency Verification of CreateSession Sub-protocol Model

First of all, the authors give the expected results of the original model established. The model will successfully perform the request and make a response for session creation and activation and there is no interruption of operation in the process of the entire interaction. Table 2

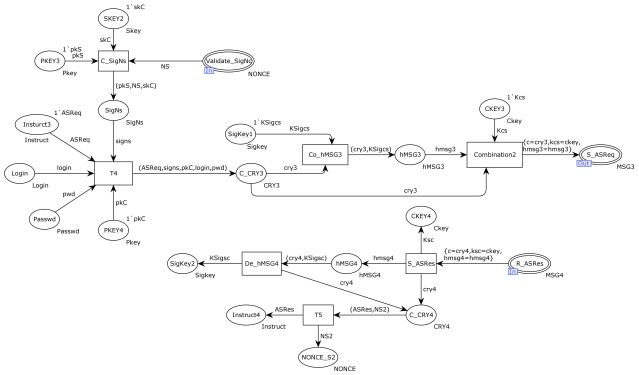


Figure 16: The internal model of substitution transition ActivateSession

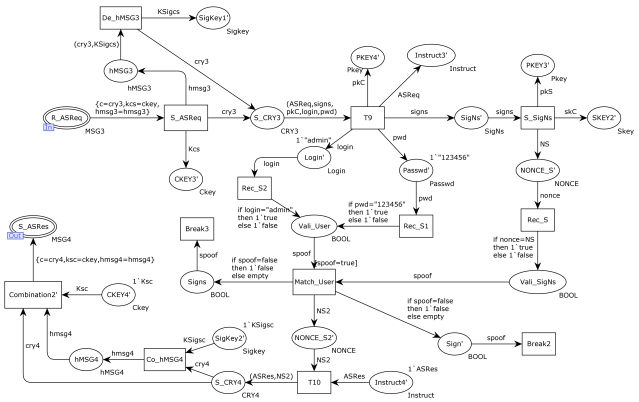


Figure 17: The internal model of substitution transition ActivateSession'

shows the results of state space in the original model of the sub-protocol, which is totally similar to Table 3. The number of state space nodes, directed arcs and strongly connected nodes, and strongly connected arcs is equal, All state nodes of the original model that are established are reachable, and there are no infinite loops and iterative behaviors in the state space; The number of main state nodes and the number of active transitions are both zero, indicating that there is no reachable state in the original model, and there is no active transition in the active state; The existence of a dead node indicates that any transition under this node are not enabled; There are 3 dead transitions Break1, Break2 and Break3.The transition Break1 means that the operation will be ended once the random number N_C verification fails during the creation of the session. The transitions Break2 and Break3 respectively represent the interruption of operation of the user credential and the random number N_S verification fails in the activation session, the existence of these three dead transitions show that the original model does not fail to pass the verification, which accords with the expected results.

4 Based on the Attacker's Security Assessment Model

Dolev and Yao published an important paper, which have a profound impact on the development of protocol security research [8]. The main contribution of this paper is to only analyze the security properties of the protocol itself based on the assumption that the cryptographic system is "perfect". At the same time, an attacker model with powerful computing power has been proposed, which can not only eavesdrop, intercept, tamper, and replay the messages interacted during the operation of the protocol, but also encrypt, decrypt, split and combine the information [5, 23]. In this way, we can concentrate on studying the inherent vulnerability and security of the protocol without caring about the security of the cryptographic algorithm.

Table 2: State space analysis of the original model of the OPC UA CreateSession sub-protocol

Categorys	Numbers	Name
State space node	64	/
Directed arc	168	/
Strongly connected node	64	/
Strongly connected arc	168	/
Master state node	0	/
Dead node	1	[64]
Death transition	3	Break1/Break2 /Break3
Live transition	0	/

Because the sub-protocol of OPC UA has a high degree of real-time performance and data frames are transmitted between the client and the server, this article attempts to add an attacker model to the network channel between the client and the server.

4.1 Introducing an Attacker's Security Assessment Model

According to the Dolev-Yao attacker model, the attacker has the powerful ability to initiate various man-in-the-middle attacks on network channels, Man-in-the-middle attacks of replay, spoofing and tampering are introduced to the network transport layer of the two sub-protocols of the OPC UA handshake.

As shown in Figures 18 and 19, man-in-the-middle attacks are added to the OpenSecureChannel and CreateSession sub-protocol network transport layers, including replay, tampering, and spoofing. Different color sets have different places and transitions functions. The red part of the places and transitions in the figure imitates a tampering attack, and the attacker attack and attack are introduced into the expression; The blue part of places and transitions in the figure imitates a replay attack. The transition TA intercepts the message of the initial operation of the sub-protocol that the attacker is going to split and is stored in the place DB, places CB1, CB2, CB3 store atomic information. The attacker's decomposition principle is adopted to decompose transition TC message; The message after the transition TD synthesizes the atomic

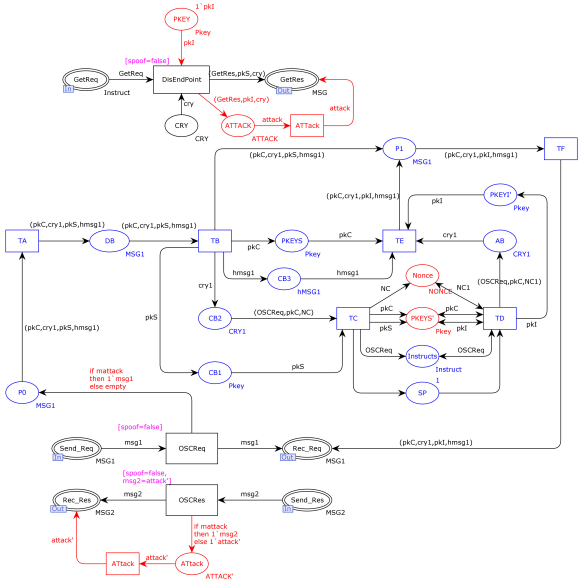


Figure 18: Security assessment model for the attacker of the OpenSecureChannel sub-protocol

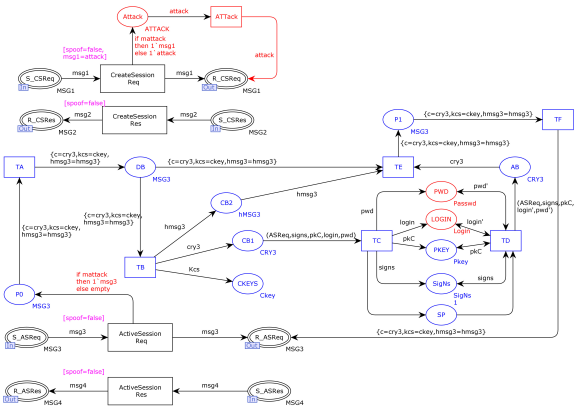


Figure 19: Security assessment model for the attacker of the CreateSession sub-protocol

message is stored in the place AB and concurrency control place SP in the process of synthesis should be introduce to restrict and limit; The transition TF is used to synthesize the last attack message which is sent to the port library. The purple part imitates a spoofing attack, covering all transitions in the process of network transmission in the two sub-protocols.

4.2 Security Evaluation of OPC UA Sub-protocol Model

Table 3 and Table 4 are the state space reports of the two sub-protocol attacker security assessment models. It can be seen that the number of state space nodes, directed arcs and strongly connected nodes and strongly connected arcs is same, which shows that all state nodes in the attacker model are reachable. Compared with the

Table 3: State space comparison of OpenSecureChannel sub-protocol model

Categorys	Original	Attacker
State space node	30	184
Directed arc	59	402
Strongly connected node	30	184
Strongly connected arc	59	402
Dead node	1	4
Death transition	3	7

Table 4: State space comparison of CreateSession sub-protocol model

Categorys	Original	Attacker
State space node	64	87
Directed arc	168	213
Strongly connected node	64	87
Strongly connected arc	168	213
Dead node	1	1
Death transition	3	3

original model, the number of state space nodes and arcs does hardly increase after the attacker model is added, indicating that there will be no state space explosion after the attacker model is introduced, declining the size of the state space node and reducing the message that is not recognized by the receiver.

After comparison of dead transition between original model and attacker modelin Tables 3 and 4, it can be found that for the dead marking of the OpenSecureChannel sub-protocol become 4 and the dead transitions become 7.Through further inquiry and analysis, there are 3 dead markings and 4 dead transitions because of the introduction of replay and spoofing attacks. The intruder tampered with the destination of the data stream, bypassed the protection of replay attacks and generated an authentication attack, protocol produced unpredictable end state. For the CreateSession sub-protocol after adding the attacker model, the number of dead markings and dead transitions has not been changed and the attacker cannot obtain any credentials of the sub-protocol. It shows that the CreateSession sub-protocol meets the security attribute goals.

The security of the two sub-protocols of OPC UA needs to be evaluated by introducing an attacker model. Since the attacker's public key pk(I) is used in message 2 to tamper with the client's public key pk(C) and sent to the client, the destination of the message flow is changed, thus leading to the client to initiate a conversation with the attacker, After receiving it, the attacker uses his own private key to decrypt it and initiates a session with the server, thereby generating a spoofing attack on the client's identity verification by the random number N_C; In addition, random numbers are exchanged in the form of plain text

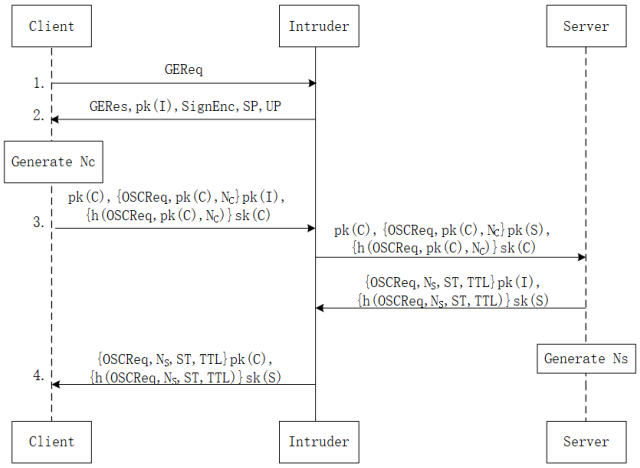


Figure 20: Attacks on N_C and N_S authentication

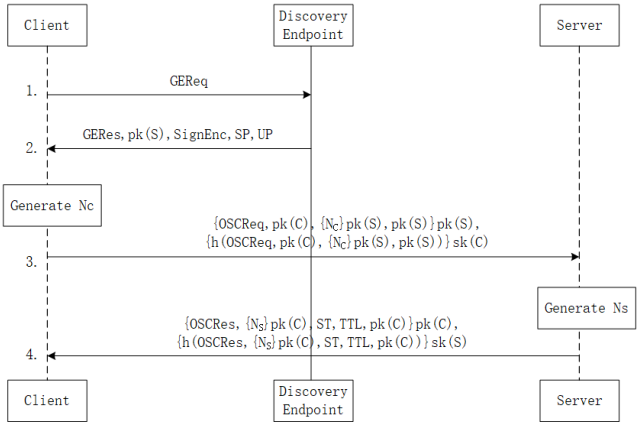


Figure 21: The message flow model of the new and improved OpenSecureChannel

in the process of message flow interaction, which causes the confidentiality of random numbers.

Therefore, the OpenSecureChannel sub-protocol has spoofing attacks on the client and server authentication by the random number N_C and N_S respectively, and the confidentiality of the random number. As shown in Figure 20, Spoofing attacks that use N_C and N_S to authenticate the client and server respectively, Because the OPC UA protocol standard does not require the identity of the message recipient to be displayed, this attack is possible. Therefore, it allows the intruder to send the client's signed message to the server. This attack is similar to the man-in-the-middle attack of the NS (Needham-Schroeder) protocol.

5 New Scheme of OPC UA Protocol

5.1 New Plan Reinforcement Method

As for the security evaluation results, the authors in this paper add the recipient's public key to the message in the sub-protocol session in order to solve the spoofing attack of identity authentication, thus leading to preventing the intruder from resending the signed message to the tampering host. As for the confidentiality of random numbers, the key wrapping mechanism is used to replace all random numbers NC in message 3 with $N_C$pk(S), and replace all random numbers N_S in message 4 with $N_S$pk(C). Since the industrial control protocol has higher requirements for real-time performance, this scheme of security enhancement that improves the protocol on the message stream is adopted so that the real-time performance of the protocol will not be affected. Figure 21 shows message flow model that has been improved.

5.2 OpenSecureChannel New Improvement Scheme Model

CPN modeling for the security enhancement scheme of the sub-protocol is performed. On the basis of the original model, the color sets Sec1 and Sec2 with the key packaging are newly added. The message flow in the sub-protocol has been changed, the top-level and middle-level models of the sub-protocol remain unchanged. This refers to the internal model that gives the substitution transitions, which have been changed.

Figure 22 shows the internal model of the new scheme of substitution transitions Instruction.The newly added places Sec1 and Sec2 are used to store the security data wrapped by the key, the random number N_C is generated by the place Generates_NC and the transition T4 will package the random number N_C that has been received and public key pk(S), and then integrated by Transition T5; Transition Combination combines the signed information and encrypted information. Finally, this information is sent to the server through the place Send_Req; Transition Break 2 means that verification of the random number N_C that has been received failed to perform the operation; The place Rec_Res is used to receive the data information sent by the server and the transition Reception, T6 and T7 indicate that the security data that has been received will be decomposed.

Figure 23 shows the internal model of the new scheme substitution transitions Generate_NS. The newly added places Sec1'and Sec2'store the security data wrapped by the key, the place Rec_Req is used to receive the data information sent by the client to the server, transition Reception',T8, T9 are used to decompose security data, transition Rec_S' verifies that the random number N_C that has been received generates a random number N_S after the verification is passed and executes the interruption of Break 3 operation if the verification fails; Transition T10 will package the random number N_S that has been received and public key pk(C) and integrate

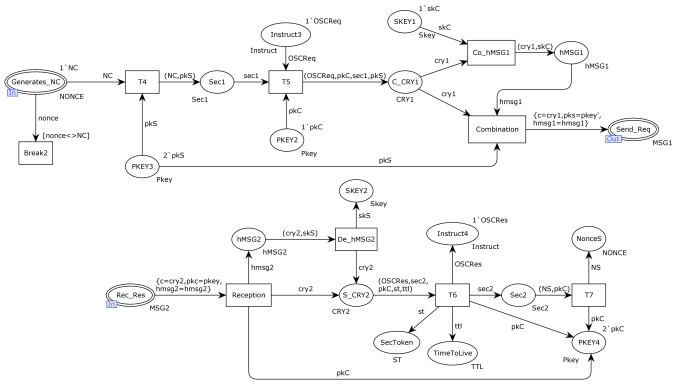


Figure 22: The internal model of the new improvement plan substitution transition Instruction

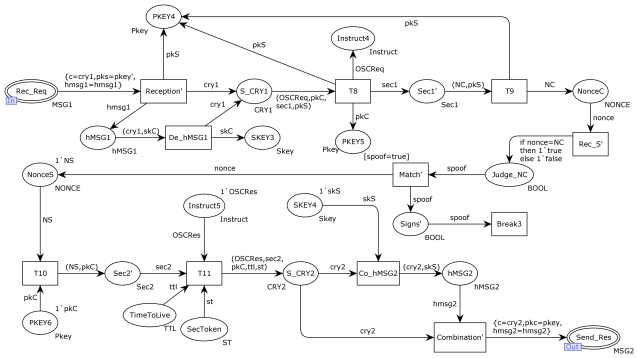


Figure 23: The new improvement plan substitution transition Generate_NS internal model

the response command OSCRes, identifier and its life cycle through the transition T11; Transition Combination'combines the signed information and encrypted information. Finally, the information is sent to the client through place Send_Res.

5.3 Safety Assessment Model of the New Scheme

Same as 4.1, we introduce the Dolev-Yao attacker model to the new scheme, and add man-in-the-middle attacks such as tampering, deception, and replay to the network layer of the new scheme of the OpenSecureChannel sub-protocol. As shown in Figure 24, the blue, red, and purple parts respectively simulate replay, tampering, and spoofing attacks.

5.4 Security Assessment of the New Scheme of the Sub-protocol

Table 5 shows the comparison of results of the state space in the OpenSecureChannel sub-protocol security evaluation model after the improvement. Because the wrapper mechanism of the key and the definition of related color

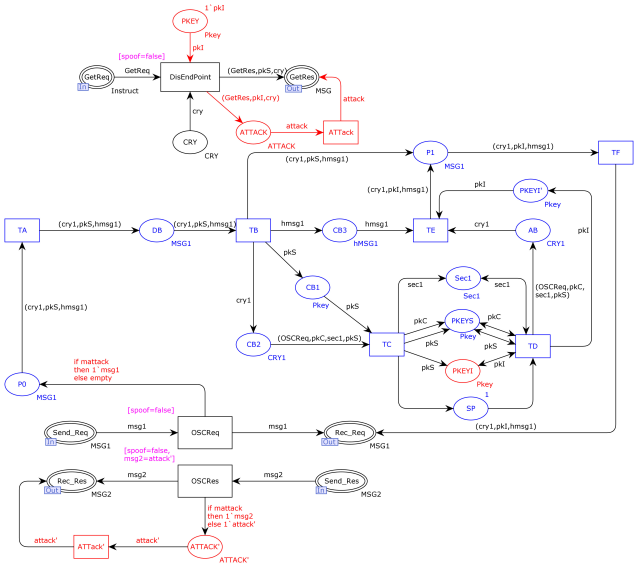


Figure 24: OpenSecureChannel new solution security evaluation model

sets are added to the message flow, the number of transitions and places is correspondingly increased and the number of state space nodes and directed arcs has also increased after improvement.

Table 5: State space comparison of OpenSecureChannel sub-protocol before and after improvement

Categorys	Before Improvment	New Scheme
State space node	184	264
Directed arc	402	536
Strongly connected node	184	264
Strongly connected arc	402	536
Dead marking	4	1
Death transition	7	6

It can be found after analysis that the number of dead marking is reduced by one,which is consistent with the number of dead marking in the original model of the sub-protocol.

This dead marking shows the final state of the protocol that has been performed after SML sentence analysis, indicating that there is not any attack on the new scheme. The number of dead transitions is reduced by 6 and the analysis shows that 3 dead transitions occurred during the operation of the protocol, which resulted in an error termination operation. Besides, the reason why the other three dead transitions are at the network level is that the attacker cannot set off an effective attack.

The attacker cannot obtain the receiver's public key and the confidentiality of the random number that is sent must be guaranteed, forcing the attacker not to initiate a spoofing attack, which reveals that the new scheme can

protect against attacks from sub-protocol identity authentication and enhance the security of the protocol.

6 Conclusion

Colored Petri nets and Delov-Yao attack methods is adopted as the theoretical basis in this study and the OPC UA protocol between factory equipment is regarded as the research object, Because the two sub-protocols of OPC UA handshake, including OpenSecureChannel and CreateSession represent the core of the OPC UA protocol security, CPN Tools are employed to make formal modeling and do security assessment for these two sub-protocols. It has been found after the modeling and analysis of these two sub-protocols that a security enhancement scheme adding the recipient's public key to the message and the key packaging mechanism is proposed and CPN Tools is used to verify the security scheme.This study only set off attack to a man-in-the-middle in the protocol, analyzed the security of the protocol itself, but did not take other forms of attacks into consideration. The next research should consider whether the protocol has other security issues at other levels in the future study and can make analysis security in other forms of attacks.

Acknowledgments

This research is supported by The National Natural Science Foundation of China (Grant No. 61762060), Educational Commission of Gansu Province, China (Grant No.2017C-05), Foundation for the Key Research and Development Program of Gansu Province, China (Grant No.20YF3GA016). Tao Feng is the corresponding author.

References

[1] M. Abbaszadeh, S. Saeedvand, "Weak consistency model in distributed systems using hierarchical colored petri net," *Journal of Computers*, vol. 13, no. 2, pp, 236-243, 2018.

[2] D. Arena, F. Criscione, N. Trapani, "Risk assessment in a chemical plant with a CPN-HAZOP tool," *IFAC-Papers OnLine*, vol. 51, no. 11, pp. 939-944, 2018.

[3] I. V. Artamonov, A. P. Sukhodolov, "CPN tools-based software solution for reliability an analysis of processes in microservice environments," *International Journal of Simulation: Systems, Science and Technology*, vol. 19, no. 6, pp. 1-8, 2018.

[4] Y. L. Bai, X. M. Ye, "An improved CPN-based attacker model of cryptographic protocol," *Journal of Inner Mongolia Agricultural University*, (Natural Science Edition), vol. 35, no. 5, pp. 103-136, 2014.

[5] A. Baskar, R. Ramanujam, S. P. Suresh, "Dolev-Yao theory with associative blindpair operators," in *Proceedings of International Conference on Implementation and Application of Automata*, pp. 58-69, 2019.

[6] P. Birnstill, C. Haas, D. Hassler, J. Beyerer, "Introducing remote attestation and hardware-based cryptography to OPC UA," in *22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'17)*, Limassol, Cyprus, pp. 1-8, 2017.

[7] C. Cremers, M. Dehel-Wild, K. Milner, "Secure authentication in the grid: A formal analysis of DNP3 SAv5," *Journal of Computer Security*, vol. 27, no. 2, pp. 203-232, 2019.

[8] D. Dolev, A. Yao, "On the security of public key protocols," *IEEE Transcations on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983.

[9] Y. Gong, Z. Wang, D. Han, "OPC UA information modeling method and xml definition," in *IEEE Conference on Telecommunications, Optics and Computer Science (TOCS'20)*, Shenyang, China, pp. 328-331, 2020.

[10] R. Huang, F. Liu, D. Pan, "Research on OPC UA security," in *5th IEEE Conference on Industrial Electronics and Applications*, Taichung, Taiwan, pp. 1439-1444, 2010.

[11] V. M. Igure, S. A. Laughter, R. D. Williams, "Security issues in SCADA networks," *Computer Security*, vol. 25, no. 7, pp. 498–506, 2006.

[12] G. Karthikeyan, S. Heiss, "PKI and user access rights management for OPC UA based applications," in *IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA'18)*, Turin, Italy, pp. 251-257, 2018.

[13] F. Kohnhäuser, D. Meier, F. Patzer, S. Finster, "On the security of IIoT deployments: An investigation of secure provisioning solutions for OPC UA," *IEEE Access*, vol. 9, pp. 99299-99311, 2021.

[14] Z. R. Konigsberg, "Modeling and verification analysis of a flexible manufacturing system: A model logic approach," *Neural, Parallel & Scientific Computation*, vol. 26, no. 1, pp. 64-74, 2018.

[15] L. Li, F. Basile, Z. Li, "An approach to improve permissiveness of supervisors for GMECs in time petri net systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 1, pp. 237-251, 2019.

[16] Z. Luo, X. Zhang, "Research on OPC UA security encryption method," in *IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA'20)*, Chongqing, China, pp. 287-292, 2020.

[17] S. Marksteiner, "Reasoning on adopting OPC UA for an IoT-enhanced smart energy system from a security perspective," in *IEEE 20th Conference on Business Informatics (CBI'18)*, Vienna, Austria, pp. 140-143, 2018.

[18] S. G. Mathias, S. Schmied, D. Grossmann, R. K. Müller, B. Mroß, "A compliance testing structure

for implementation of industry standards through OPC UA," in *25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'20)*, Vienna, Austria, pp. 1091-1094, 2020.

[19] N. Mühlbauer, E. Kirdan, M. O. Pahl, G. Carle, "Open-source OPC UA security and scalability," in *25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'20)*, Vienna, Austria, pp. 262-269, 2020.

[20] S. C. Patel, G. D. Bhatt, J. H. Graham, "Improving the cyber security of SCADA communication networks," *Communication of ACM*, vol. 52, no. 7, pp. 139-142, 2009.

[21] M. Puys, M. L. Potet, P. Lafourcade, "Formal analysis of security properties on the OPC-UA SCADA protocol," in *International Conference on Computer Safety, Reliability, and Security*, pp. 67-75, 2016.

[22] A. Rashid, U. Siddique, S. Tahar, "Formal verification of cyber-physical systems using theorem proving," in *Proceedings of International Workshop on Formal Techniques for Safety-Critical Systems*, pp. 3-18, 2019.

[23] M. Rocchetto, N. O. Tippenhauer, "CPDY: Extending the Dolev-Yao attacker with physical-layer interactions," in *Proceedings of International Conference on Formal Engineering Methods*, pp. 175-192, 2016.

[24] M. Simon, D. Moldt, D. Schmitz, *et al.*, "Tools for curry-coloured petri nets," in *Proceedings of International Conference on Applications and Theory of Petri Nets and Concurrency*, pp. 101-110, 2019.

[25] A. Volkova, M. Niedermeier, R. Basmadjian, H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 619-639, 2019.

Biography

Feng Tao, was born in 1970, researcher/PhD supervisor, CCF senior member, IEEE and ACM member.He graduated from Xidian University,and then worked at school of computer and communication in Lanzhou University of Technology. His research interests include Cryptography and information security.

Ma Zhuang-yu, was born in 1997,CCF member.He is a master's student at lanzhou university of technology.His research interests include technical information security and industrial control systems.

Fang Jun-li, was born in 1985,CCF member.She is a doctor's student at lanzhou university of technology.Her research interests include network and information security.

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.