Traffic Characteristic Map-based Intrusion Detection Model for Industrial Internet

Rui-Hong Dong, Dong-Fang Wu, Qiu-Yu Zhang and Tao Zhang
(Corresponding author: Qiu-Yu Zhang)

School of Computer and Communication, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
(Email: zhangqylz@163.com)
(Received June 4, 2017; revised Aug. 16, 2017 and accepted Sep. 25, 2017)

Abstract

After the Stuxnet security event in Iran, the security issues on industrial Internet are very serious. Besides, there are many flaws existing in the modern traffic modelling approaches to the industrial field network. Aiming at these problems, the traffic characteristic map-based intrusion detection model for industrial Internet was proposed. Firstly, information entropy method was adopted to select vital traffic characteristics attributes set which is used to form traffic characteristic vectors. Secondly, multiple correlation analysis approach was applied to transform traffic characteristics vector into triangle area mapping matrix and traffic characteristic map can be established. Finally, using discrete cosine transform (DCT) and singular value decomposition (SVD) methods, perceptual hash digest database of normal and abnormal traffic characteristics maps was obtained. Thereafter, the corresponding intrusion detection rule set can be generated, which is essential for the modelling of network traffic periodic characteristics in industrial field network. In particular, the robustness and discrimination of the traffic characteristics map perceptual hash algorithm (TCM-PH) were proved. Experimental results show that the proposed approach has a good performance of intrusion detection in the industrial field network.

Keywords: Hash Digest; Industrial Control Network; Intrusion Detection; Network Traffic Characteristics Map; Rule Set

1 Introduction

The traditional industrial control system (ICS) is widely used in many national critical infrastructures (NCI), for instance, petrochemical industry, power and water conservancy industry, industrial production, nuclear energy and transportation. According to the analysis of Security Situation Report of ICS-CERT [6] in 2015, more than 80% NCI rely on ICS to achieve the automation of production process. Therefore, ICS plays a vital role in our daily life. The ICS security issues directly affect national security and economic development. In 2010, the Stuxnet virus infected the Bushehr nuclear power station in Iran. Until 2015, a series of network security issues appeared, which brought great influence on human's life. The security situation of industrial Internet is very serious [1, 3, 12].

Industrial Internet includes three layers: enterprise management network, supervisory network and field network. In the research of security problems in field network, the periodicity characteristic of network traffic information is the key point. The intrusion detection methods to field network can be divided into three kinds: intrusion detection approaches based on model, fuzzing detection and Snort rule. The Snort-based method is mostly used to analyse the protocol used in the field network. However, this kind of method highly relies on the prior knowledge, which is mostly used in known attacks [18, 23, 26]. The fuzzing-based method is mainly used to test the protocol vulnerability [21].

Aiming at the above questions, from the image point, the intrusion detection issues and relationships between every two attributes are researched. The traffic characteristic map-based intrusion detection model for industrial Internet was proposed in this paper. The presented method can meet the real-time and high efficiency of intrusion detection approach. Traditional text information can be transformed into image via the traffic characteristics map technique. In order to research traffic characteristics from different point, the single attribute research is replaced by the research about the relations between attributes. By using image perceptual hash features extraction method, hash digest can be obtained and intrusion detection rule set can be produced. The perceptual hash features extraction method obtains robustness and discrimination. The robustness ensures that the intrusion detection approach can effectively find the known traffic information. The discrimination keeps the distinguishing characteristics of unknown attacks. Furthermore, the time complexity of image perceptual hash algorithm is

very low. Finally, the training and test processes can take the testbed data set [9] and NSL-KDD [20].

This research deals with four issues. 1) By using traffic characteristics map technique, the traffic text information can be transformed into traffic characteristics map. 2) By using image perceptual hash features extraction method, the hash digest can be captured and intrusion detection rule set can be produced. 3) Intrusion detection rule matching operation includes three steps: strings-based precise match, similarity measure based on Hamming distance and clustering based on Euclidean distance. These three steps ensure the intrusion detection performance. In the intrusion detection stage, three-level detection pattern is set. The adaptability of the proposed method is increased. The unknown attacks can be detected, which decreases the false alarm rate resulted from fuzzy matching. Our method has a good detection performance. 4) The study proves the robustness and discrimination of TCM-PH algorithm.

The rest of the paper is organized as follows: In Section 2, the related works of intrusion detection method based on traffic characteristics were described. The theory of traffic characteristics map technique and the image perceptual hash features extraction method were introduced in Section 3. In Section 4, an industrial Internet intrusion detection model based on traffic characteristics map was proposed. And the robustness and discrimination of this algorithm are also proved. In Section 5, the experimental results were analysed then the performances of our method and other methods were compared. Finally, we conclude our paper in Section 6.

2 Related Works

In industrial field network, intrusion detection method based on model has adaptability, which is essential for the detection of unknown attacks. Therefore, many researchers achieve more works in intrusion detection method based on traffic periodicity characteristics. In [5], the research work of Modbus traffic periodicity features was finished. According to the deep analysis of packets, the deterministic finite automation (DFA) approach was used to establish Modbus normal behaviour model, which displays a good abnormal detection performance and adaptability. Yet, the study did not analyse the algorithm complexity of the DFA. In [22], the researchers analysed the normal traffic characteristics to get the Snort rule set. Then, traffic white list was set and the abnormal traffic information can be detected. But, the performance verification of the proposed approach should have taken a universal data set. In [23], according to the prior knowledge, fuzzing detection method was applied to analyse the structure of packets. Thereafter, the vulnerability can be found.

In [26], fuzzing method was used to produce large number of malformed packets including function code, which can be adopted to test the vulnerability of SCADA system. The data space was compressed and fuzzing test time was optimized. Mostly, the fuzzing test method was used to find the vulnerability of industrial field network protocol. In [21], Modbus traffic information and terminal unit information were extracted to produce Snort rules. The intrusion detection system based on Modbus protocol and Snort rule was established. But, the production of Snort rule highly relies on prior knowledge. In [28], network data was mapped into different dimension of hash histogram to establish detection vector. Support vector data description machine (SVDD) was used to detect network abnormal information. And the comparing works between several different classifiers were finished. In [16], by using PSO-SVM method, in Modbus protocol packets, the research of function code appearance frequency was achieved.

In [27], aiming at network traffic top-down time series characteristics, a network traffic analysis system based on multi-view was established. In [19], the multiple correlation analysis (MCA) method was used to transform text information into corresponding traffic images. The differences between two traffic images were computed by Manhattan distance, which realized the abnormal intrusion detection. By using MCA, the traffic data characteristics can be kept. For the abnormal detection in field network, in [24], cumulative sum (CUSUM) method was used to deeply analyse network packet. According to [15], multiscale principal component analysis (MSPCA) method was used to research traffic periodicity and traffic matrix space-time correlation, which modelled the network normal traffic behaviours.

In [11], the active degree of input and output traffic in researched network was counted and the active entropy was computed via the active entropy method. This method produced intrusion detection rule set, which reduced the false positive rate. By [7], the improved affinity propagation (AP) method decreased the number of clustering classes and the time cost and ensured true positive rate, which increased intrusion detection performance. In [17], the simulations of network intrusion detection attacks were added into the testbed data proposed by [9]. The existing intrusion detection methods were evaluated. In [10], the rule set was captured from the Modbus protocol contents and traffic packet periodicity characteristics. And, the intrusion detection system was established. In [4], according to the research of registers value change characteristics in SCADA industrial control system, parameter models were established. These models can detect network abnormal traffic information.

Image perceptual hash features extraction approaches include DCT, SVD, wavelet transform and principal component analysis (PCA). In this paper, image perceptual hash features extraction methods based on SVD and DCT were adopted. In [8], colourful histogram and DCT coefficient matrix were regarded as perceptual features. The image contents tamper localization was achieved via DCT and PCA. This method demonstrated robustness and discrimination. In [2], the robustness characteristics were

captured via audio cochleogram. And the established non-negative matrix was factorized to produce perceptual hash digest. By recurrence quantification method, the hash digest was matched. In [14], audio clips were mapped into hash digests. And the indexing and authentication of audios were achieved by this method. This method obtained robustness and discrimination.

3 Related Techniques and Theory

3.1 Modbus Traffic Characteristic Map Techniques

The approaches of information collection and features extraction in industrial Internet were researched. Based on above research works, the attributes features set of experimental data can be captured. The traffic information features space of Modbus protocol field network can be established. By using traffic characteristic map (TCM) technique, traffic characteristic map of field network traffic information can be produced. The traffic characteristic map is the input data for the image perceptual hash features extraction method.

Traffic information of field network has a strong periodicity, which leads to a fixed pattern. Traffic characteristics are much different between normal and abnormal traffics. The statistical characteristics of traffic information can be used to describe traffic behaviours. In [9], for the standardization of experimental data, a SCADA testbed experimental data was proposed. However, the testbed data and NSL-KDD [20] cannot be transformed into traffic characteristics map directly. Before transformation, the pre-processing works are needed to be finished. As the Figure 1 shown, the technique road of Modbus traffic characteristics map method is illustrated.

3.1.1 Compute Attributes Information Entropy and Normalization

In the pre-processing stage of experimental data, the incomplete traffic records are deleted. Then, the information entropy [25] of traffic attributes is computed. The vital attributes are selected. The definition of information entropy is as follow.

$$H(x) = -\sum_{i=1}^{s}(\frac{d_i}{T})log(\frac{d_i}{T}) \tag{1}$$

where x is an attribute, and $H(x)$ is the information entropy of attribute x. The total number of attributes is n. The number of different traffic records is s. These traffic records can be expressed as $\{a_1, a_2, \cdots, a_s\}$. The corresponding occurrence number is $\{d_1, d_2, \cdots, d_s\}$. The computed information entropy of attributes can be sorted by descending order. The experimental data [9] includes the following data sets. Data 1 and Data 2 are collected from gas pipeline system. Data 3 and Data 4 are collected from water storage system. Data 1 and Data 3 are training data, and Data 2 and Data 4 are tested data. The traffic attributes number set of Data 1 and Data 2 is {1, 2, 3, 4, 5, 6, 12, 13, 24, 25, 26, 27}. The traffic attributes number set of Data 3 and Data 4 is {1, 2, 3, 4, 5, 6, 10, 12, 13, 18, 20, 21, 22, 23, 24}. The traffic attributes number set of NSL-KDD is {1,2,3,4,5,6,10,12,13,18,20,21,22,23,24}, the attributes tables are shown in Tables 3, 4 and 5.

The normalization of attributes set is defined as follow.

$$f(x) = \begin{cases} 0 & x \in [0, m) \\ \frac{255x}{n-m} & x \in [m, n] \\ 255 & x \in (n, \infty) \end{cases}. \tag{2}$$

where n and m represent maximum and minimum, respectively. $f(x)$ is the normalization value, which is within the range of grey value, $f(x) \in [0, 255]$.

3.1.2 Multiple Correlation Analysis

In [19], adopting MCA method and triangle area method, normal and abnormal traffic characteristics were obtained. The correlations between attributes were also obtained. The flow steps are listed as follows.

Experimental data can be expressed as $X = \{x_1, x_2, \cdots, x_n\}$. According to the obtained traffic attributes sets, $x_i = [x_1, x_2, \cdots, x_n]$, $(1 \le i \le n)$, expresses the i-th m dimension traffic record. Triangle area method is used to capture the correlation between attributes j and k in vector x_j.

Vector x_j is mapped into $(j-k)$ dimension Euclidean subspace. $(1 \le i \le n, 1 \le j \le m, 1 \le k \le m, j \ne k)$, $y_{i,j,k} = [\varepsilon_j \varepsilon_k]^T = [f_j^i f_k^i]^T$, $\varepsilon_j = [e_{j,1}, e_{j,2}, .., e_{j,n}]$, $\varepsilon_k = [e_{k,1} e_{k,2} .. e_{k,n}]^T$, $e_{j,j} = e_{k,k} = 1$, and other elements equal to zero. $y_{i,j,k}$ is a 2-dimension vector, which can be expressed as one point $(f_j^i f_k^i)$ in $(j-k)$ dimension Euclidean subspace. On the Cartesian coordinate system, a triangle area $\Delta f_j^i O f_k^i$ is formed by the origin and the projected points of the coordinate $(f_j^i f_k^i)$ are found on the k and j axis. The triangle area can be expressed as following.

$$Tr_{j,k}^i = (\parallel (f_j^i, 0) - (0,0) \parallel \times \parallel (0, f_k^i) - (0,0) \parallel)/2. \tag{3}$$

where $1 \le i \le n, 1 \le j \le m, 1 \le k \le m$, and $j \ne k$.

For the complete analysis of traffic records, x_i represents correlation between every two attributes. And, the corresponding triangle area is computed. The complete triangle area map (TAM) of traffic record including all triangle area is computed on the basis of every two attributes correlation. In i-th traffic record, $Tr_{j,k}^i$ expresses j-th row and k-th column triangle area. When $j = k$, $Tr_{j,k}^i = 0$. Therefore, the research focus on the correlations between every two attributes. When $j \ne k$, $Tr_{j,k}^i = Tr_{k,j}^i$. The obtained ***TAM*** is a symmetric matrix, whose main diagonal vector equal to zero. 4-dimension ***TAM*** can be expressed as follow.

$$TAM_x^i = \begin{bmatrix} 0 & Tr_{1,2}^i & Tr_{1,3}^i & Tr_{1,4}^i \\ Tr_{2,1}^i & 0 & Tr_{2,3}^i & Tr_{2,4}^i \\ Tr_{3,1}^i & Tr_{3,2}^i & 0 & Tr_{3,4}^i \\ Tr_{4,1}^i & Tr_{4,2}^i & Tr_{4,3}^i & 0 \end{bmatrix} \tag{4}$$

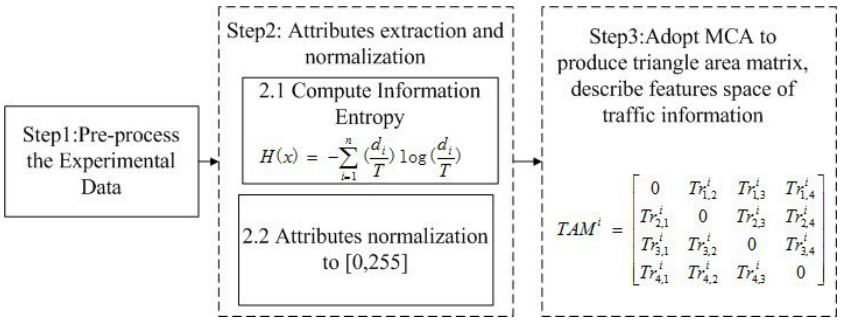

Figure 1: Technique rode of Modbus traffic characteristics map method

There are several merits of MCA method. 1) There is no need of prior knowledge. 2) The MCA which is based on triangle area is not vulnerable to linear changes of all features. 3) Provide individual network traffic records. 4) Analyse the correlation between every two attributes.

Algorithm 1 TCM Algorithm

1: Input: Training data
2: Output: Traffic Characteristics Map TAM^i
3: According to Equation (1), compute the information entropy of attributes and select vital attributes set
4: According to Equation (2), normalize attributes set to $[0, 255]$
5: Get width and height of the dimension
6: **for** i from 1 to height **do**
7: **for** j from 1 to width **do**
8: According to Equation (3), compute $Tr^i_{j,k}$, and send value to the corresponding place in $\boldsymbol{TAM}^i$
9: **end for**
10: **end for**
11: Output the traffic characteristics map $\boldsymbol{TAM}^i$

3.2 Image Perceptual Hash Features Extraction

3.2.1 Discrete Cosine Transform

DCT method has several merits: explicit physical meaning, middle complexity, swift calculation and separable property. DCT is regarded as the optimization method used in audio and image transformation. The transformation of image is achieved via DCT. According to [8], DCT can be defined as follow.

$$F(u,v) = \frac{C(u)C(v)}{4} \sum_{x=0}^{N} \sum_{y=0}^{N} f(x,y) \cdot \cos(\frac{\pi(2x+1)u}{N^2}) \cos(\frac{\pi(2y+1)v}{N^2}) \quad (5)$$

where f expresses $N \times N$ pixels matrix, and F is $N \times N$ coefficient matrix. C expresses the cosine coefficient matrix.

The steps of algorithm as follow:

1) In Data 1, Data 2 and NSL-KDD train data set, by using TCM method, the 11×11, 14×14 and 14×14 traffic characteristics maps are obtained. And, in Data 3, Data 4 and NSL-KDD test data set, the 11×11, 14×14 and 14×14 traffic characteristics maps are got.

2) According to Equation (5), by using DCT method, 11×11, 14×14 and 14×14 DCT coefficient matrices are obtained.

3) For the discrimination of perceptual hash digest, the complete DCT coefficient matrix including low and high frequency domains is used to produce hash digest. And, the mean value of coefficient matrix is computed, named ***mean***.

4) According to Equation (7), SVD is used to decompose and reconstruct DCT coefficient matrix. The useful information can be obtained and the data noise is removed. $N = 11$ and 14, the left singular value u_3 and the right singular v_3, which are corresponded to $_3$, are used to produce hash digest ***DCT_m***.

$$DCT\_m = [u_1, u_2, .., u_N] \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_N \end{bmatrix} [v_1, v_2, .., v_N]^T \quad (6)$$

$$SVD\_matrix = [u_3^T, v_3^T] \quad (7)$$

5) From left to right, the traversal work of SVD_matrix is achieved. The hash rule is defined as follow.

$$h(x) = \begin{cases} 1, & x \geq m \\ 0, & x < m \end{cases}. \quad (8)$$

where x is the SVD result, and $h(x)$ is the corresponding hash code. After the matrix traversal, the hash digests database can be obtained. And, the corresponding rule set is produced.

3.2.2 Match Hash Digest

The hash digests of test data are captured. These hash digests are the input data for hash match algorithm. By this way, the abnormal traffic information can be detected.

The image contents match methods include Euclidean distance, Hamming distance and norm. Hamming distance method is adapted to measure similarity of different images. Before hash matching, by using traffic characteristics map method, traffic text information can be transformed into traffic characteristics map. There are three matching stages in the improved matching algorithm. The three-level matching method increases adaptability of the TCM-PH algorithm.

1) Precise matching based on string

   The hash digest of test data is captured, named H_{s1}. Adopting the precise matching method, the normal traffic hash digest H_{s2} and abnormal traffic hash digest H_{s3} are matched with H_{s1}. Then, the matching results are output. After the precise matching, some traffic hash digests don't have any detection result. These hash digests take part in the second matching stage.

2) Similarity matching based Hamming distance

   By using Hamming distance Equation (9), the similarity between H_{s1} and normal traffic H_{s2} can be computed. And, the distance between H_{s1} and H_{s3} can also be calculated. According to the computed results, in condition to meet the match threshold value, the H_{s1} can obtain the matching result. However, some unknown intrusion traffic digests cannot meet this threshold. These unknown attacks participate in the third matching stage. The similarity can be expressed by D_H or bit error rate BER.

$$D_H(H_{s1}, H_{s2}) = \frac{\sum_{w=1}^{L} \mid H_{s1}(w) - H_{s2}(w) \mid}{L} \tag{9}$$

   where $BER = D_H(H_{s1}, H_{s2})$, H_{s1} and H_{s2} have equal length. In Data 1 and Data 2, $L = 22$. In Data 3 and Data 4, $L = 28$, In NSL-KDD, $L = 28$. w is one hash code in hash digest. The threshold value of similarity matching is set.

3) Clustering matching based on Euclidean distance

   The Euclidean distance can be expressed as follow.

$$d(x, y) = \sqrt{\sum_{j=1}^{n}(x_j - y_j)^2} \tag{10}$$

   According to Equation (10), the distance from hash digest clustering centre to test hash digests can be computed. The test digest can be detected by the smallest Euclidean distance. The clustering method has adaptability, which is essential for the detection of unknown intrusion.

4 The Proposed Model

4.1 Intrusion Detection Model Based on TCM-PH

In the existing intrusion detection methods to industrial Internet, the nature of intrusion detection method based on traffic is to find the abnormal change rules of traffic. By the establishment of network traffic characteristics map in SCADA and field network, the intrusion detection model based on traffic characteristics map is established. The network intrusion detection issues are solved via image features extraction methods. Traffic characteristics map perceptual hash (TCM-PH) algorithm is a supervisory learning method. The intrusion detection thought is illustrated in Figure 2.

Algorithm 2 TCM-PH

```
Input: Training data and test data
Output: Intrusion detection results
Get training data set.
while the number of training data do
    The TCM algorithm is adopted to produce traffic characteristics map.
    By DCT method, the normal and abnormal hash digest are captured.
    Produce intrusion detection rule set.
end while
Get test traffic data set.
while test data do
    By TCM algorithm, the traffic characteristics map is produced.
    Adopting DCT method, the hash digest is captured.
    if meet precise matching then
        while rule do
            Hash digest match rule set, output detection result
        end while
    else if Meet similarity measure then
        According to Equation (9), the similarity between hash digest and intrusion detection rule set is computed.
        if matching threshold then
            Output intrusion detection result
        else if Meet similarity measure then
            According to Equation (10), compute distance between hash digest and clustering centre, output intrusion detection result
        end if
    end if
end while
```

4.2 The Property Proof of TCM-PH

When perceptual hash is applied in network intrusion detection, the robustness and discrimination [8] of TCM-PH

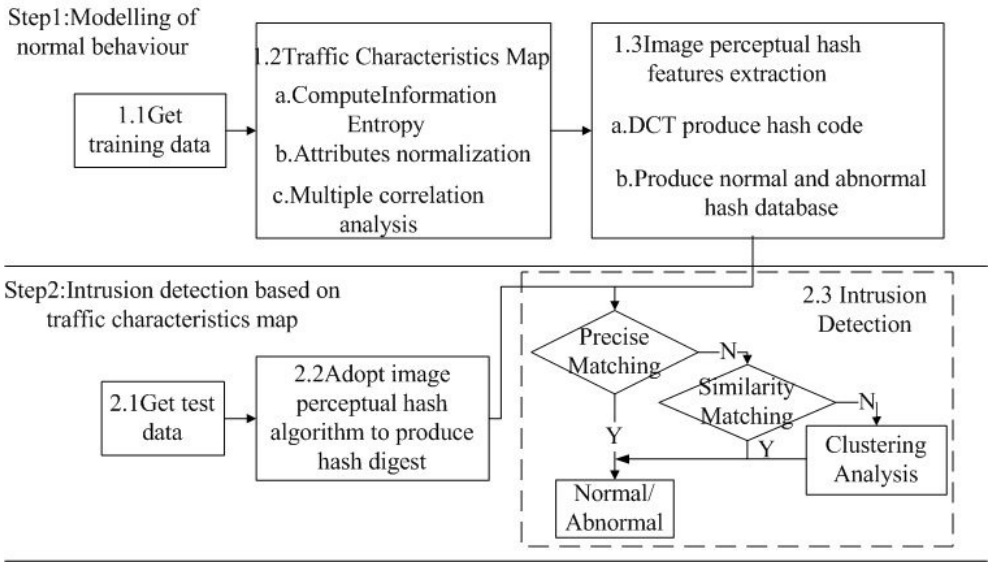

Figure 2: Intrusion detection model based on traffic characteristics map

algorithm are proved. The perceptual hash function has robustness and discrimination [13]. The details are illustrated as follows.

Property 1. *(**Robustness**) After the content hold operations, the different media digital representation which possessed same perceptual content can produce one same hash digest.*

Property 2. *(**Discrimination**) The different media digital representation which possessed different content produce different hash digests.*

Assume that $x, y, z \in M$ is experimental data, and h_x, h_y, $h_z \in H_p$ are normal and abnormal traffic hash digests. $h_x = PH(x), h_y = PH(y), h_z = PH(z)$, PH is hash function. $dis(\cdot,\cdot)$ is perceptual distance (or false accept rate), and τ is matching threshold value. $dis(\cdot,\cdot)$ is geometric distance, and T_p is perceptual threshold. In data $\boldsymbol{M}$, x is the traffic characteristics map transformed from traffic text information. In 3.2 Section, traffic characteristics map method is illustrated carefully. x can be expressed as Equation (4). By DCT perceptual hash function, the hash digest is produced, and the hash digest can be expressed as $h_x = \{h_{x1}, h_{x2}, h_{x3}, hx4\}$.

The theory of geometric distance is Hamming distance in Equation (9). The matching threshold τ meet the range $(0, 1]$. The perceptual distance describes the differences between multi-media data, which can be defined as follows.

$$disp(x, y) = \begin{cases} 1, & x \neq y \\ 0, & x = y \end{cases}. \tag{11}$$

where perceptual distance $T_p \in (0, 1)$. When x and y are same $x = y$, $disp(x, y) < T_p$. When x and y are different, $x \neq y$, $disp(x, y) > T_p$. Let assume that $x = y$ and $x \neq z$.

Prove 1. *(**Robustness**) When the perceptual hash-based intrusion detection method has robustness, $\forall x, y \in M$, event $A = \{(x, y) : disp(x, y) < T_p$ and $dis(h_x, h_y) < \tau)\}$, $P(A) = 1$.*

It demonstrates the fact that x and y are same, $x = y$. Therefore, $disp(x, y) = 0$, $disp(x, y) < T_p$. When the perceptual hash is used in intrusion detection, there is no any content keeping manipulations. According to the robustness of perceptual hash function, the same media digital representation map into the same hash digest, $h_x = h_y$. According to Equation (10), $dis(h_x, h_y) = 0$, $dis(h_x, h_y) < \tau$. So, the probability of event A is 1, $P(A) = 1$. It means that x and y produce the same hash digest. The robustness of TCM-PH is proved.

Prove 2. *(**Discrimination**) When the perceptual hash-based intrusion detection method has discrimination, $\forall x, z \in M$, $B = \{(x, z) : disp(x, z) > T_p$ and $dis(h_x, h_z) < \tau\}$, $P(B) = 0$.*

Let assume that $P(B) = 1$, $dis(h_x, h_z) < \tau$, according to Equation (10), $h_x = h_z$. Considering the robustness of TCM-PH algorithm, we can judge that x and z are same traffic data, $x = z$. And, according to $P(B) = 1$, we can learn that $disp(x, z) > T_p$, by perceptual distance Equation (11). Therefore, x and z are different traffic data. According to the theory of reduction to absurdity, there is a contradiction in the mathematical reasoning. In fact, the original mathematical hypothesis is wrong. And, $P(B) = 0$. The discrimination of TCM-PH algorithm is proved, which ensure that different traffic data has different hash digest.

5 Experimental Results and Analysis

5.1 Selection of Experimental Data

The experimental data [9] and NSL-KDD [20] are adopted in our research to test the performance of TCM-PH algorithm. There are three merits in the testbed data. 1) This data provide more research opportunities with general researchers. 2) The data ensure that other researchers can test more vital studies and experimental results. 3) The proposed data provide the general test platform, which is helpful for researchers to compare and analyse every related methods. The merits of NSL-KDD data set include: 1) The redundancy data and the repeated data were removed for the objective evaluation. 2) The percentage and kinds of the records are same with the KDD Cup 99 data set. 3) The number of the NSL-KDD is feasible which decreases the payloads of the intrusion detection method.

Comparing with KDD99 data set, the proposed data [9] also sign every record with information type in 0 to 7 numbers. There are 8 kinds of traffic records. 0 represents normal data. Other numbers represent attack information. The normal traffic information is captured from the testbed SCADA system. And, abnormal traffic information can be divided into four kinds, reconnaissance, response injection, command injection and denial-of-service. There are total eight kinds of testbed data in Table 1.

NSL-KDD data is the improved version of the original KDD99 data set. Each value of label expresses different kinds of data. 0 is normal and others are abnormal. NSL-KDD includes four kinds of abnormal: Dos, Probe, U2R and R2L, shown in Table 2.

Table 2: The kinds of NSL-KDD data set

Label	Value	Description
Normal	0	Normal data
Dos	1	Deny of service attack
Probe	2	Probe attack
U2R	3	User to root attack
R2L	4	Remote to login attack

The features selection result of gas data set is $\{1, 2, 3, 4, 5, 6, 12, 13, 24, 25, 26, 27\}$, shown as Table 3.

The features selection result of water data set is $\{1, 2, 3, 4, 5, 6, 12, 13, 24, 25, 26, 27\}$, shown as Table 4.

The features selection result of NSL-KDD data set is $\{3, 5, 6, 23, 24, 29, 30, 31, 32, 33, 34, 35, 36, 37\}$, shown as Table 5.

The Modbus protocol is widely used in field network. Considering the structure of protocol, data features and information entropy, the above attributes were selected, as Table 3, Table 4 and Table 5 shown. Table 1 and Table 2 illustrate data composition, for example, the kinds of attacks. Table 6 shows the base condition of data set.

5.2 The Analysis of The Traffic Characteristics Map

Adopting traffic characteristics map method [19], traffic characteristics are extracted to produce traffic characteristics map.

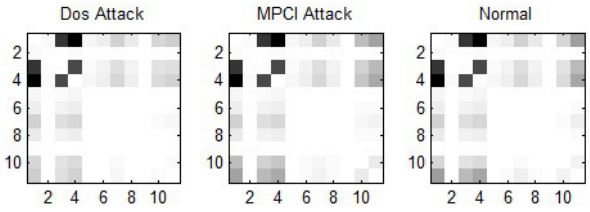

Figure 3: The traffic characteristic map of Dos, MPCI and normal traffic record in Data 1

According to the proposed method TCM-PH in Section 4, the experimental programs are realized in MATLAB. The testbed data and NSL-KDD data are chosen as the test data. The simulation results are shown in Figure 3. The subfigures express the different features in grey values. Dos attack and normal records are much different. The difference between MPCI and normal record is not much apparent. The reason is that the little difference in grey value can be recognized by TCM-PH method but not human vision.

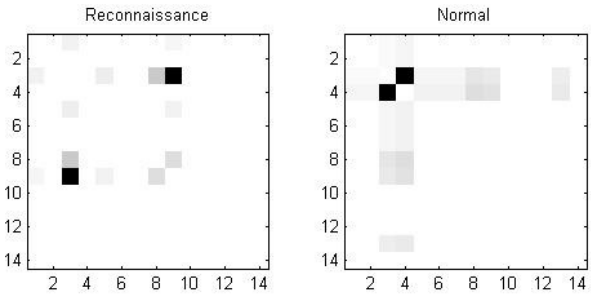

Figure 4: The traffic characteristic map of reconnaissance and normal traffic record in Data 3

In Figure 4, the difference between these two kinds traffic map is apparent. TCM-PH can also capture the features in the maps. The length of gas data is $L = 22$, and the length of water storage data is $L = 28$. The format of hash digest is binary strings. Table 7 describes the detection performance. TP is true positive rate, and FP is false positive rate.

In Figure 5, 5 kinds of records in the training data are shown. According to the results of the features selection method, the size of the map is 14×14. The difference between every map is obvious. These maps are the input data for the next operation.

Table 1: The kinds of Gas and Water data set

Label	Value	Description
Normal	0	Instance not part of an attack
NMRI	1	Naive malicious response injection attack
CMRI	2	Complex malicious response injection attack
MSCI	3	Malicious state command injection attack
MPCI	4	Malicious parameter command injection attack
MFCI	5	Malicious function command injection attack
Dos	6	Denial-of-service attack
Reconnaissance	7	Reconnaissance attack

Table 3: Attributes of gas data

Number	Attribute name	Description
1	*command_address*	Device ID in command packet
2	*response_address*	Device ID in response packet
3	*command_memory*	Memory start position in command packet
4	*response_memory*	Memory start position in response packet
5	*command_memory_count*	Number of memory bytes for R/W command
6	*response_memory_count*	Number of memory bytes for R/W response
12	*command_length*	Command packet length
13	*response_length*	Response packet length
24	CRC rate	CRC error rate
25	measurement	Pipeline pressure or water level
26	time	Time interval between two packets
27	result	Kinds of data

Table 4: Attributes of water data

Number	Attribute name	Description
1	*command_address*	Device ID in command packet
2	*response_address*	Device ID in response packet
3	*command_memory*	Memory start position in command packet
4	*response_memory*	Memory start position in response packet
5	*command_memory_count*	Number of memory bytes for R/W command
6	*response_memory_count*	Number of memory bytes for R/W response
10	*resp_fun*	Response function code
12	*command_length*	Command packet length
13	*response_length*	Response packet length
18	*control_model*	Automatic, manual or shutdown
20	pump-state	Compressor/pump state
21	CRC rate	CRC error rate
22	measurement	Pipeline pressure or water level
23	time	Time interval between two packets
24	result	Kinds of data

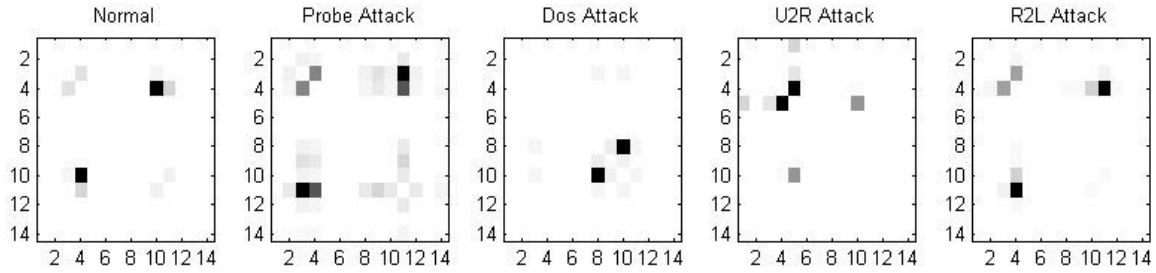

Figure 5: The traffic characteristic map of NSL-KDD train data set

Table 5: Attributes of NSL-KDD data

Number	Attribute name	Description
3	service	Service Type
5	*src_bytes*	The number of bits from source to destination
6	*dst_bytes*	The number of bits from destination to source
23	count	Number of connecting same hosts in past 2s
24	Srv count	Number of connecting same services in past 2s
29	same srv rate	Rate of same connecting service
30	diff srv rate	Rate of different connecting service
31	srv diff host rate	Rate of different connecting host
32	dst host count	Number of connecting same host
33	dst host srv count	Number of same host and same service
34	dst host same srv rate	Rate of same host and same service
35	dst host diff srv rate	Rate of different service in different host
36	dst host same src port rate	Rate of connecting host in same src port
37	dst host diff src port rate	Rate of connecting host in different src port
42	type	Kinds of data

Table 6: Experimental data composition

Name	Dimension	Normal Record Number	Abnormal Record Number	Attack Kinds
Data 1	2027×27	1732	295	*MPCI&Dos*
Data 2	2844×27	2594	250	*MPCI&Dos*
Data 3	23673×24	9554	14119	Reconnaissance
Data 4	1664×24	657	1007	Reconnaissance
NSL-KDD train	25192×42	13449	11743	*Dos&Probe&U2R&R2L*
NSL-KDD test	22544×42	9711	12833	*Dos&Probe&U2R&R2L*

Table 7: Rule set captured from Data 1 and Data 3.

Name	Normal Rule Set	Abnormal Rule Set	TP(mean)	FP(mean)
Data 1	75	103	0.9866	0.014
Data 3	76	67	0.9925	0.015
NSL-KDD train	471	535	0.9893	0.0012

5.3 Discrimination Experiments

The robustness and discrimination of TCM-PH are essential and vital for the abnormal intrusion detection. The robustness ensures that the same traffic record can produce same hash digest. The discrimination ensures that different and unknown attacks can map into different hash digests. The evaluation of discrimination is the false accepting rate (FAR) [8].

$$FRA = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\tau} \exp[\frac{-(x-\mu)^2}{2\sigma^2}] \qquad (12)$$

where μ is the mean of normal distribution and σ is the standard deviation. τ is the matching threshold.

In total, 143 different hash digests were taken to test the discrimination of TCM-PH algorithm. The total matching times is 10,153. Figure 6 is the normal distribution curve of the false accepting rate. The blue curve is coincided with the mean straight line. But, there are still some fluctuations.

The mean is 0.4991, and the theoretical standard deviation is 0.0418. And, the real standard deviation is

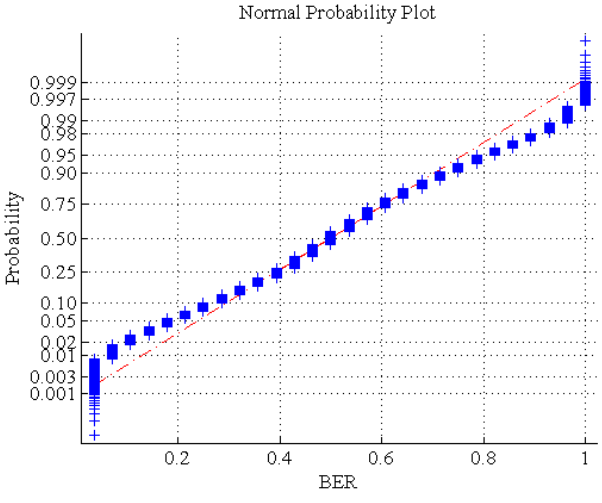

Figure 6: Normplot image of our scheme

0.1791. Both ends of the curve appear aggregation phenomenon. The aggregation in lower left quarter expresses that the discrimination of hash digest is very high. Another aggregation in upper right corner expresses that there indeed exist many analogical traffic characteristics maps, which is corresponding to the periodicity of traffic information.

Table 8: Comparing with FAR

Threshold τ	0.0357	0.02	0.01	0.005
FAR	0.0048	0.0037	0.0032	0.0029

When $\tau = 0.0357$, $FAR = 0.0048$. That is to say that there happen 4.8 false accepting intrusion attacks in 1000 traffic records, which meets the network detection request. Table 8 shows the correlations between FAR and τ.

The format of the hash digest is binary string. According to Equation (9), the hash distance is the normalized Hamming distance. It is also named as BER. We can think that every bit of hash digest is independent and identically distributed. Each bit can take the value at 0 or 1. The probability of these two values is equal. The probability is 0.5. The normalization Hamming distance obeys to normal distribution, which has 0.5 mean value and $\sigma = 0.5/\sqrt{N}$ standard deviation. When the attributes transform into binary string, the redundant information between attributes are kept. Therefore, the real standard deviation has little difference with the theoretical standard deviation. Figure 7 is the bit error rate (BER) colour histogram of discrimination of TCM-PH. The centre of BER distribution is close to 0.5, which is 0.4991. And standard deviation is 0.1791. The proposed algorithm has a good discrimination.

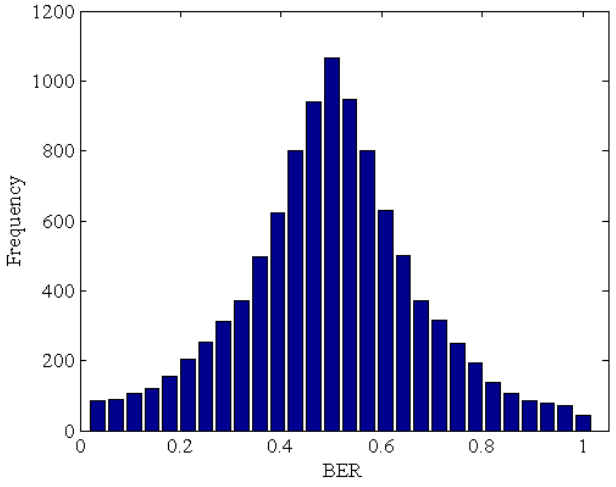

Figure 7: Colour histogram of BER

5.4 Algorithm Performance Analysis

The gas pipeline data, water storage data and NSL-KDD data set are adopted in experiments. The performance of the proposed method is shown in Table 9. The average TP of gas data is 0.986, and the corresponding average FP is 0.014. The average TP of water storage data is 0.9925, and the corresponding average FP is 0.015. The average TP of NSL-KDD is 0.9893, and the average FP is 0.0012. The TP of water storage data and NSL-KDD data are higher than gas pipeline data, which demonstrates that the precise detection needs more training data.

The number of training records is N_1 and the number of test records is N_2. The number of attributes is M. The number of normal hash digests is $nhash$ and the number of abnormal hash digests is $ahash$. The time complexity of TCM-PH algorithm is $O(N_1 + N_2)(M^2 + 5M)$ which is little bigger than MCA [19], and TP is 0.993. The FP of proposed method is minimum value. In [19], the complexity of MCA is $O(M^4)$. In [15], the complexity is $O((N_1+N_2)M^2)$. The complexity of the proposed method is better than Ref. [7, 16, 28].

6 Conclusions

In this paper, our study deal with three issues, transformation and features extraction of traffic characteristics map, intrusion detection rule matching problem and the proof of the robustness and discrimination of TCM-PH. By using traffic characteristics map technology, the text data are transformed into figure information. The features of the figure can be captured via perceptual hash features extraction method, which provides the new solutions from the figure features extraction point to deal with intrusion detection in industrial internet area. The three-level detection pattern adds the adaptability of our method. With this help, many unknown attacks can be recognized. The experimental results proved the robustness and discrimination of TCM-PH method, which provides theoretical support to our research. The experiments prove the feasibility of TCM-PH algorithm. The most vital result is that traffic characteristics map method provides network intrusion detection with new solutions.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61363078), the Natural Science Foundation of Gansu Province of China (No. 1310RJYA004), the Open Project Program of the National Laboratory of Pattern Recognition (NLPR) (No. 201700005). The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

Table 9: Detection performance analysis

Method	TP	FP	Time Complexity
AP [7]	0.9436	0.08	$O(N_1N_2M^2)$
MSPCA [15]	0.9	0.2	$O((N_1+N_2)M^2)$
PSO-SVM [16]	0.9583	-	$O(200\times N_1N_2)$
MCA [19]	0.993	0.018	$O(M^4)$
SVDD [28]	0.970	0.070	$O(N_1^2N_2)$
TCM-PH of our scheme (gas data)	0.986	0.014	$O((N_1+N_2)(M^2+5M))$
TCM-PH of our scheme (water data)	0.9925	0.015	$O((N_1+N_2)(M^2+5M))$
TCM-PH of our scheme (NSL-KDD)	0.9893	0.0012	$O((N_1+N_2)(M^2+5M))$

References

[1] M. El Boujnouni and M. Jedra, "New intrusion detection system based on support vector domain description with information gain metric," *International Journal of Network Security*, vol. 20, no. 1, pp. 25-34, 2018.

[2] N. Chen, H. D. Xiao, J. Zhu, J. J. Lin, Y. Wang, and W. H. Yuan, "Robust audio hashing scheme based on cochleogram and cross recurrence analysis," *Electronics Letters*, vol. 49, no. 1, pp. 7–8, 2013.

[3] R. H. Dong, D. F. Wu, Q. Y. Zhang and H. X. Duan, "Mutual information-based intrusion detection model for industrial internet," *International Journal of Network Security*, vol. 20, no. 1, pp. 131-140, 2018.

[4] N. Erez and A. Wool, "Control variable classification, modelling and anomaly detection in modbus/tcp scada systems," *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 59–70, 2015.

[5] N. Goldenberg and A. Wool, "Accurate modelling of modbus/tcp for intrusion detection in scada systems," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63–75, 2013.

[6] ICS-CERT, "Monitor (ics-mm201612)," *https://ics-cert.us-cert.gov/monitors/ICS-MM201612*, November 2016.

[7] J. Jiang, Z. F. Wang, T. M. Chen, C. Zhu, and B. Chen, "Adaptive ap clustering algorithm and its application on intrusion detection," *Journal of Communication*, vol. 36, no. 11, pp. 119–126, 2015.

[8] Z. Jie, "A novel block-dct and pca based image perceptual hashing algorithm," *International Journal of Computer Science Issues*, vol. 10, no. 3, pp. 399–403, 2013.

[9] T. Morris and W. Gao, "Industrial control system traffic data sets for intrusion detection research," in *International Conference on Critical Infrastructure Protection*, pp. 65–78, Berlin, Heidelberg, March 2014.

[10] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, "Deterministic intrusion detection rules for modbus protocols," in *46th Hawaii International Conference on System Sciences (HICSS)*, pp. 1773–1781, Wailea, Maui, HI, USA, January 2013.

[11] X. K. Mu, J. S. Wang, Y. F. Xue, and W. Huang, "Abnormal network traffic detection approach based on alive entropy," *Journal of Communication*, vol. 34, no. Z2, pp. 51–57, 2013.

[12] A. Nezarat, "Distributed intrusion detection system based on mixed cooperative and non-cooperative game theoretical model," *International Journal of Network Security*, vol. 20, no. 1, pp. 56-64, 2018.

[13] X. M. Niu and Y. H. Jiao, "An overview of perceptual hashing(in chinese)," *ACTA ELECTRONICA SINCA*, vol. 36, no. 7, pp. 1405–1411, 2008.

[14] M. Nouri, N. Farhangian, Z. Zeinolabedini, and M. Safarinia, "Conceptual authentication speech hashing base upon hypotrochoid graph," in *Sixth International Symposium on Telecommunications (IST)*, pp. 1136–1141, Tehran, Iran, November 2012.

[15] Y. K. Qian, M. Chen, L. X. Ye, F. Liu, S. Zhu, and H. Zhang, "Network-wide anomaly detection method based on multi-scale principal component analysis," *Journal of Software*, vol. 23, no. 2, pp. 361–377, 2012.

[16] W. L. Shang, S. S. Zhang, and M. Wan, "Modbus/tcp communication anomaly detection based on pso-svm," *Applied Mechanics and Materials*, vol. 490, pp. 1745–1753, 2014.

[17] S. N. Shirazi, S. A. Gouglidi, K. N. Syeda, S. Simpson, A. Mauthe, I. M. Stephanakis, and D. Hutchison, "Evaluation of anomaly detection techniques for scada communication resilience," in *Resilience Week (RWS)*, pp. 140–145, Chicago, IL, USA, August 2016.

[18] D. Stiawan, M. Y. B. Idris, A. H. Abdullah, and A. Mohammed, "Penetration testing and mitigation of vulnerabilities windows server," *International Journal of Network Security*, vol. 18, no. 3, pp. 501–513, 2016.

[19] Z. Tan, A. Jamdagni, and X. He, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 447–456, 2014.

[20] M. Tavallaee, E. Bagheri, W. Lu, , and A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 1–6, Ottawa, ON, Canada, July 2009.

[21] W. Tylman, "Native support for modbus rtu protocol in snort intrusion detection system," *New Results in Dependability and Computer Systems*, vol. 224, pp. 479–487, 2013.

[22] W. Tylman, "Scada intrusion detection based on modelling of allowed communication patterns," *New Results in Dependability and Computer Systems*, vol. 224, pp. 489–500, 2013.

[23] A. G. Voyiatzis, K. Katsigiannis, and S. Koubias, "A modbus/tcp fuzzer for testing internetworked industrial systems," in *20th Conference on Emerging Technologies & Factory Automation (ETFA)*, pp. 1–6, Luxembourg, September 2015.

[24] M. Wan, W. L. Shang, and P. Zeng, "Anomaly detection approach based on function code traffic by using cusum algorithm," in *4th National Conference on Electrical, Electronics and Computer Engineering (NCEECE)*, pp. 12–13, Xian, China, December 2015.

[25] W. Wang, Y. He, J. Liu, and S. Gombault, "Constructing important features from massive network traffic for lightweight intrusion detection," *IET Information Security*, vol. 9, no. 6, pp. 374–379, 2015.

[26] Q. Xiong, H. Liu, Y. Xu, H. Rao, S. Yi, B. Zhang, W. Jia, and H.Deng, "A vulnerability detecting method for modbus-tcp based on smart fuzzing mechanism," in *International Conference on Electro/Information Technology (EIT)*, pp. 404–409, Dekalb, IL, USA, May 2015.

[27] Y. Zhao, Q. Wang, Y. Z. Huang, W. Qing, and Z. Sheng, "Collaborative visual analytics for network traffic time-series data with multiple views," *Journal of Software*, vol. 27, no. 5, pp. 1118–1198, 2016.

[28] L. M. Zheng, P. Zou, Y. Jia, and W. H. Hang, "How to extract and train the classifier in traffic anomaly detection system," *Chinese journal of computer*, vol. 25, no. 4, pp. 719–729, 2012.

Biography

Dong Ruihong Vice researcher, worked at school of computer and communication in Lanzhou university of technology. His research interests include network and information security, information hiding and steganalysis analysis, computer network.

Wu Dongfang In 2015, Wu Dongfang obtained his bachelor of engineering degree from Northwest University for Nationalities. Currently, he is studying for his master's degree at Lanzhou University of Technology. His research focuses on the industrial control network security.

Zhang Qiuyu Researcher/PhD supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research centre, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.

Zhang Tao He is studying for his master's degree at Lanzhou University of Technology. His research focuses on the network and information security.