International Core Journal of Engineering Volume 6 Issue 4, 2020
ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

Research on Model of Assessing Security Situation for Industrial IoT

XiangDong Hu, ZhaoTao Chen

Chongqing University of Posts and Telecommunications, Chongqing 400000, China.

Abstract

Aiming at the fact that the current security situation of the Industrial Internet of Things is difficult to be accurately and autonomously perceived and evaluated, an intelligent sensing and assessment model of the Industrial Internet of Things security situation based on particle swarm optimization to optimize the support vector machine is proposed. First, it defines the indicators of industrial IoT security situation assessment, that is, the importance of industrial IoT assets, network vulnerability, and network threats, and proposes calculation formulas for industrial IoT security situation assessment, and combines the methods of gray correlation to obtain security. Situation assessment. Based on this, the particle swarm algorithm is used to optimize the support vector machine to train the security situation assessment model of the Industrial Internet of Things. Moreover, simulation experiments were carried out, and the proposed model was used to evaluate the safety data of the Industrial Internet of Things, and compared with other methods. The results show that the model has the advantages of high prediction accuracy, and has greater advantages than other methods.

Keywords

Industrial Internet of Things; Security posture; Support vector machine; Particle swarm optimization.

1. Introduction

With the widespread application of the Industrial Internet of Things technology in the industrial field, the control devices at the equipment level in the industrial control system will realize information interaction through the network, and can seamlessly integrate the management layer with the market layer [1]. However, the increasingly open networked connections have made industrial control systems, networked devices, and industrial cloud platforms vulnerable to intrusion, bringing threats such as downtime, production interruption, and asset loss to the industrial environment[2].

The traditional industrial IoT security monitoring system is a passive security defense method, which cannot accurately and comprehensively describe the current security status and future status of the network system. The industrial IoT security posture is a real-time monitoring of the security status of the Internet of Things And, an active defense method that accurately evaluates the future security status, it can effectively overcome the shortcomings of traditional IoT security monitoring systems, and has become a hot issue in the current research on industrial IoT network security [3].

2. Research status of security situation analysis

In recent years, security situation assessment has become a research hotspot in the field of network security. Scholars at home and abroad have proposed many theories and methods, and established effective evaluation models and methods, such as Bayesian networks, fuzzy reasoning, game theory, and graph models [4]. Wait.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

Xie Lixia and others integrated the research results of security assessment and large-scale networks, proposed a security posture hierarchical indicator evaluation model and 25 candidate indicators, and established an evaluation indicator system, organized candidate indicators and further abstracted them [5]. In the network security situation assessment based on Hidden Markov Model (HMM), Shaanker M and others proposed a method to obtain the improved observation sequence and transition matrix in a random manner, which can effectively characterize the security of the network [6]. Wen et al. proposed a security situation prediction method based on radial basis function (RBF) neural network, which can achieve a more accurate prediction effect in the environment of small scale neural network nodes, which is not suitable for large-scale networks Prediction of security situation under environmental conditions [7]. Liu Xiaowu and others established a security assessment model based on Back Propagation (BP) neural network, and based on this, used the RBF network to predict the current security situation, and used genetic algorithms to optimize network parameters, which can predict more accurately. Security posture [8]. Chen Hao et al. Based on the idea of defense in depth, integrated a variety of existing network attack detection technologies, and proposed a technology-independent modular situation assessment framework structure [9]. Zhao Guosheng and others integrated the existing network security system, developed a network security framework for identifying and defending against attacks, and used a visual way to reflect the security status of the network [10].

So far, most of the literature has been researched on the network security situation of the Internet, and there is a lack of comprehensive and systematic research on the network security situation in the field of Industrial Internet of Things. In addition, the domestic security situation research still has problems such as insufficient accuracy and low real-time performance [11]. This paper proposes a security situation assessment model for the Industrial Internet of Things based on PSO-SVM. Firstly, an index system for the security situation of the Industrial Internet of Things was developed. The grey correlation analysis was used to determine the weight of the vulnerability index of the Industrial Internet of Things. The security situation of the Industrial Internet of Things system was determined. The security situation data set is trained to establish an industrial Internet of Things security situation assessment model. Finally, the accuracy and practicability of the model are tested through specific simulation experiments.

3. Industrial IoT Security Situation Assessment Method

3.1 Industrial IoT Security Situation Index System

Based on the controller status, protocol characteristics, network characteristics, and traffic characteristics of the Industrial Internet of Things, the indicators of asset importance, vulnerability, and threat are classified to form a reasonable industrial Internet of Things security situation index system.

Based on the above analysis, the security situation index system of the Industrial Internet of Things in Table 1 is established.

Table 2: Classification of industrial IoT security levels

Primary indicator	secondary indicator
Asset importance	Key equipment average survival time Asset importance Flow change rate Number of surviving critical devices
Vulnerability Index	Data length

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

	Vulnerability Index Function Code, Cyclic Check Code Packet interval
Threat index	Threat Index Type of Attack

For the above-mentioned indicators for the evaluation of the security situation of the Industrial Internet of Things, this article gives a quantitative method corresponding to each indicator.

First, identify the normal data and abnormal data for the data length, function code and cyclic check code, and quantify the indicators according to the following methods:

Data length index c_i: The Normal data length is marked as $c_i = 0.5$, The abnormal data length is marked as $c_i = 1$.

Function code index e_i: Normal function codes are marked as $e_i = 0.5$, The abnormal function code is marked as $e_i = 1$.

Cyclic Check Code Index t_i: Normal cyclic check codes are marked as $t_i = 0.5$, The abnormal cyclic check code is marked as $t_i = 1$.

Vulnerability analysis of the Industrial Internet of Things system includes analysis of data length, function code, cyclic check code, and data packet interval in the system. Therefore, the system's vulnerability index at time t is defined as:

$$m_i(t) = \omega_c c_i(t) + \omega_e e_i(t) + \omega_t t_i(t) + \omega_T T_i(t) \quad (1)$$

Among them ω_c、ω_e、ω_t、ω_T are the data length, function code, cyclic check code, and packet interval, respectively. The weight of the system vulnerability is obtained by applying the gray correlation analysis method, which will be introduced in the next chapter.

In addition, this article defines the importance and threat of assets in the system:

1) Asset importance index p_i: Take into account factors such as the number of surviving critical equipment and the average survival time of critical equipment in the Industrial Internet of Things system, and evaluate the asset importance of the system to obtain the asset importance index p_i.

2) Threat index r_i: To evaluate the attacks on the system in a hierarchical manner and obtain the threat index r_i.

Considering the importance, vulnerability, and threat of assets in the Industrial Internet of Things system, the system security situation assessment index at all times is:

$$F_i(t) = f(p_i, m_i(t), r_i(t)) = p_i \cdot m_i(t) \cdot 10^{r_i(t)} \quad (2)$$

Among them, $F_i(t)$ represents the security situation assessment value of the system in the time period t.

Through the construction of the situation assessment index system, combined with the security operation status of the Industrial Internet of Things, according to the calculated safety situation assessment value, and standardizing it, the safety index is obtained, and four types of situation assessment indicators are given, which are classified as severe danger, Moderate danger, mild danger and safety [12].

Table 2: Classification of industrial IoT security levels

Safety rate	Security Level	Security Situation Value
0-0.2	safe	1

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

0.2-0.5	Mild danger	2
0.5-0.8	Moderate danger	3
0.8-1	Severe danger	4

3.2 Grey correlation analysis to determine the weight of the vulnerability index

This article refers to the method in [3] and uses the grey correlation analysis method to determine the weight of the security vulnerability index of the Industrial Internet of Things.

In the industrial IoT security situation assessment, a set of vulnerability index data is selected as a sample. For each group of industrial IoT vulnerability index data, there are n characteristic information. Let $x_i(t)$ be the fragile characteristic information of the Industrial Internet of Things, and its observation data on the time serial number t is $x_i(t)=\{x_i(1),x_i(2),\ldots,x_i(k)\}$, which represents the feature value at the moment k of the sample x. By establishing a grey correlation analysis model, the weights of various industrial IoT vulnerability indicators can be quickly determined, and according to the industrial IoT security situation calculation formula established in 2.1, the industrial IoT security situation assessment value under the time serial number is calculated. The specific steps for establishing a gray correlation analysis model are:

1) Select the data sequence of the security situation vulnerability index of the Industrial Internet of Things selected in 2.1 as the reference data sequence: $x_0(t)=\{x_0(1),x_0(2),\ldots x_0(k)\}$ and the attack level of the Industrial Internet of Things system as the comparison factor sequence $x_i(t)=\{x_i(1),x_i(2),\ldots,x_i(k)\}$, where $i=1,2,3,\ldots,n$.

2) Preprocess the data selected in step 1). The method used in this paper is the mean method transformation; that is, first to find the average value x_i of the sequence $x_i(t)$, and use all the data x_i in the sequence to obtain a new mean sequence $y_i(t)$. The transformation formula is:

$$f(x_i(t))=\frac{x_i(t)}{\overline{X}} \tag{3}$$

3) Calculate the correlation coefficient.

$$\zeta_i(k)=\frac{\min\limits_s\min\limits_t|x_0(t)-x_s(t)|+\rho\max\limits_s\max\limits_t|x_0(t)-x_s(t)|}{|x_0(t)-x_i(k)|+\rho\max\limits_s\max\limits_t|x_0(t)-x_s(t)|} \tag{4}$$

$\zeta_i(k)$ Is the correlation coefficient of the attack level sequence to the vulnerability index sequence at time, where $\rho\in[0,1]$ is the resolution coefficient, $\max\limits_s\max\limits_t|x_0(t)-x_s(t)|$ and $\min\limits_s\min\limits_t|x_0(t)-x_s(t)|$ are the two-stage maximum absolute difference and the two-stage minimum absolute difference. Generally, the larger the resolution factor, the larger the resolution ρ, and the smaller ρ, the smaller the resolution.

4) Determine the gray correlation. Take the average of the correlation coefficients at k times.

$$r_i=\frac{1}{n}\sum_{k=1}^{n}\zeta_i(k) \tag{5}$$

Where r_i is the correlation of $x_i(t)$ and $x_0(t)$.

5) List the correlation matrix and determine the weight of each industrial IoT security vulnerability index according to the correlation of each data index.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

3.3 PSO-SVM training

Through the gray correlation analysis to determine the various vulnerability indicators, according to formula (2) to obtain the security situation assessment value of the Industrial Internet of Things, this paper designs a method based on particle swarm algorithm to optimize the support vector machine. The security situation assessment data of the Internet of Things constitutes training data. After normalization, training is performed to obtain the security situation assessment model of the Industrial Internet of Things. Figure 1 is a flowchart of the overall scheme of this article.

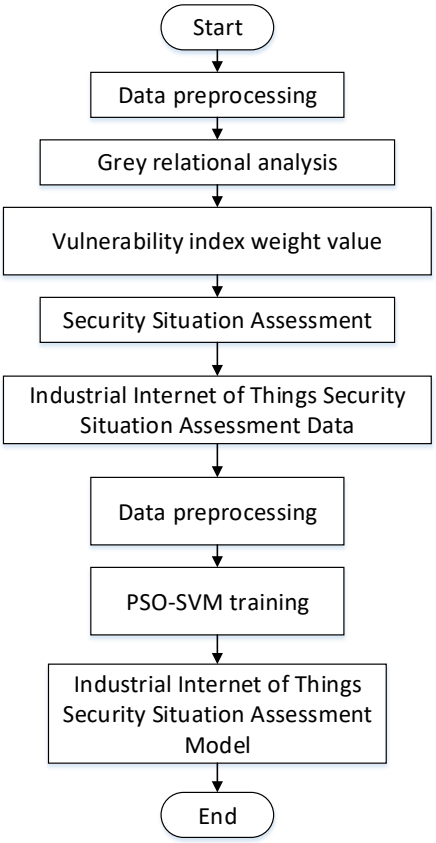

Figure 1 .Overall scheme flowchart

The advantages of support vector machines are mainly in solving small samples, non-linear and high-dimensional pattern recognition. It has a complete short training time, theoretical basis, strong adaptability and strong generalization performance [13]. According to the complexity of the safety eigenvalues of the Industrial Internet of Things, this paper uses support vector machines with kernel functions as Gaussian radial kernel functions for classification.

Through experimental comparison with genetic algorithm and fish swarm algorithm, we decided to use particle swarm algorithm to optimize the kernel function parameters c and penalty factor parameters g of support vector machines. For specific experimental data, refer to Chapter 3. FIG. 2 is a flowchart of training a security situation assessment model of the Industrial Internet of Things by a particle swarm algorithm optimized support vector machine.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

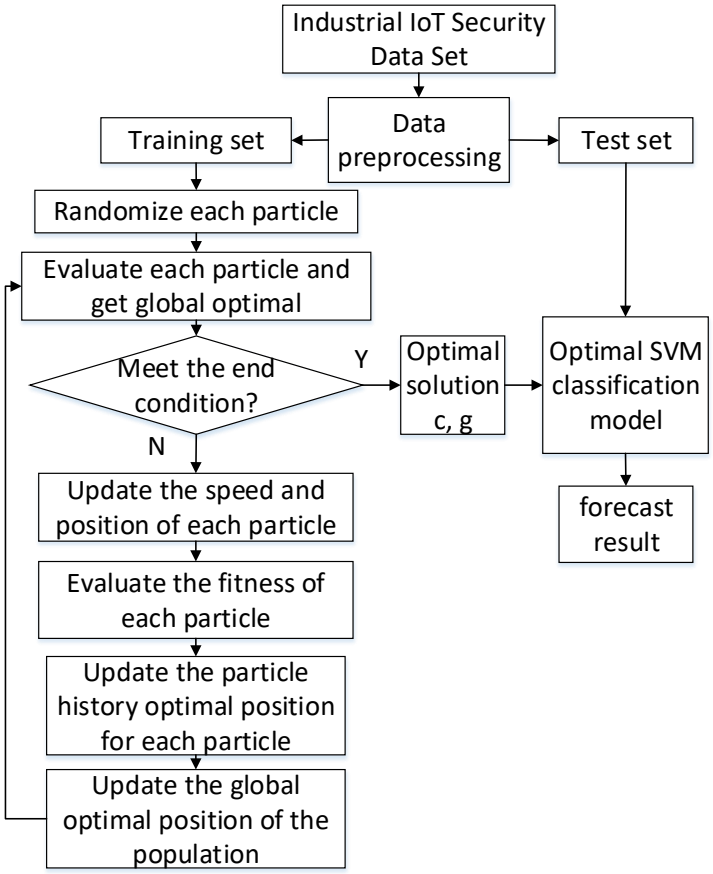

Figure 2. PSO-SVM training flowchart

The basic process of the PSO-SVM method designed in this paper to train the industrial Internet of Things security situation assessment model is:

1) Input the standardized industrial Internet of Things security situation data into the SVM model as a training sample. The output value is the security situation assessment value of the Industrial Internet of Things.

2) Initialize the particle swarm, set each particle as a combination (X_1, X_2) of the kernel function parameters and penalty factor coefficients of the SVM, and set the number size=50 of particle swarms. Due to the kernel function parameters c>0 and penalty factor coefficients $g > 0$, this method takes $c = |X_1|, g = |X_2|$, that is, 50 sets of kernel function parameters c and The penalty factor parameter g is used as the initial particle swarm population.

3) The SVM is set to the 50 sets of kernel function parameters c and penalty factor parameters g to train the data, evaluate its performance and obtain the optimal value among them, and store the optimal value.

4 Update each set of kernel function parameters c and penalty factor parameters g, compare them with the previously stored optimal values, and save the obtained optimal parameters.

5) To determine whether the maximum number of iterations has been reached, the maximum number of iterations ξ=15 set by the method in this article. If the maximum number of iterations is reached, the best kernel function parameters c and penalty factor parameters g are obtained, and the optimal parameters are output to train the data samples to obtain the corresponding industrial Internet of Things security situation assessment value, otherwise proceed to step 4).

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

3.4 Multi-Class SVM Based on Partial Binary Tree

The principle based on partial binary tree classification is as follows: First, the multi-classification problem is decomposed into a series of binary classification problems by constructing a binary tree, and then SVM is used to implement the binary classification [14]. For the application scenario of the Industrial Internet of Things security situation assessment in this article, it should be divided into 4 categories (security situation assessment values are 1, 2, 3, and 4). When training and testing a binary tree SVM, it starts with the SVM of the node and classifies it in order according to a certain classification order. First, identify the data with a security situation assessment value of 1, and put the rest of the data into the next SVM for classification, and get the data with a security situation assessment value of 2, 3, and 4, in order. Figure 3 is a schematic diagram of a partial binary tree SVM for the security situation assessment of the Industrial Internet of Things.

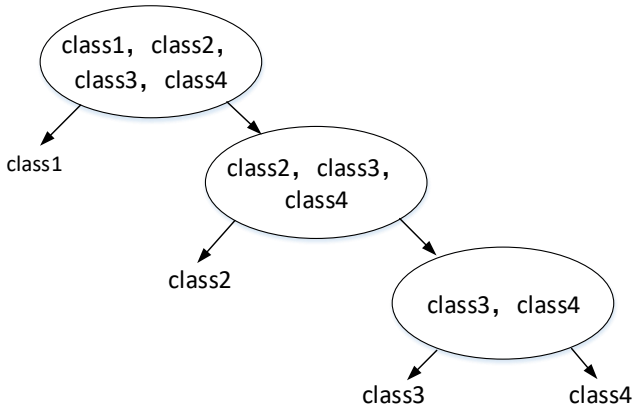

Figure 3. Partial Binary Tree SVM

4. Experimental analysis

In order to verify the superiority of this method, this paper uses the industrial control standard data set proposed by the University of Mississippi Key Facilities Protection Center to simulate the industrial Internet of Things security situation assessment method proposed in this paper. This experiment was run on a Windows operating system, written in python.

The data set was normalized and PCA dimensionality reduced, and it was obtained by the method of gray correlation analysis: $\omega_c = 0.93$, $\omega_e = 0.94$, $\omega_t = 0.94$, $\omega_T = 0.97$.

This sample is trained using the method in this article. 1000 sample data is randomly taken from the sample data set, and the sample data is randomly divided. The training data accounts for 70% and the test data accounts for 30%. This experiment uses particle swarm optimization to optimize the parameters of the support vector machine algorithm, and also uses fish swarm algorithm and genetic algorithm for comparison experiments. Figure 4 shows the experimental results.

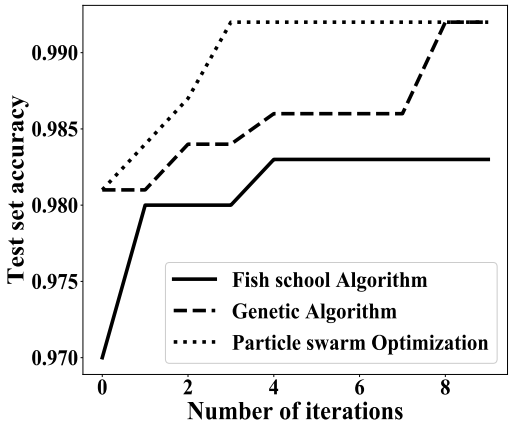

Figure 4 .Comparison of training of three optimization algorithms

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

It is found through experiments that the convergence speed of the particle swarm algorithm is significantly better than the other two algorithms, and the accuracy rate of the test set reached is the highest, reaching 99.2%. The particle swarm algorithm has global optimization, and has better stability and accuracy. Big advantage.

Through the method of this article, the test set in the sample is tested to obtain the security situation of the sample point in the test set. The figure shows the security situation of some sample points, which can intuitively display the security situation of the sample point, and enables the Industrial Internet of Things. Security administrators can make security defenses in a timely manner.

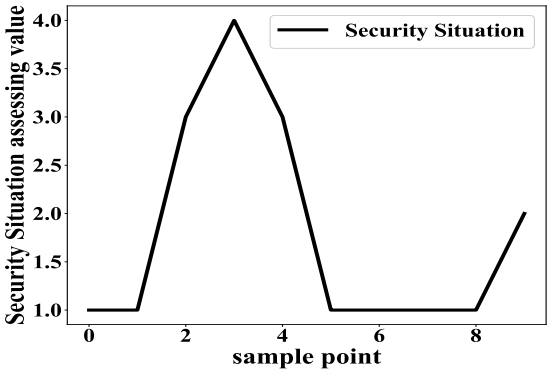

Figure 5. Security situation of some samples in the test set

As shown in Figure 5, the security situation assessment of sample point 1 and sample point 2 are both 1, indicating that the system is safe at this time. The safety situation assessment values of the system in sample points 3 and 4 reached 3 and 4, which indicates that the system is in a moderately dangerous state and a severely dangerous state at this time. The security status of the system tended to be stable from sample point 6 to sample point 9 and was slightly threatened by sample 10.

In order to further verify the accuracy of the proposed model, the proposed model is compared with the support vector machine and the Kalman entropy based method in [15] and the naive Bayesian method in [16].

Table 3: Comparison of accuracy of different methods

Method name	Evaluation accuracy
Method of this article	99.2%
SVM	97.4%
Method of Reference [15]	96.4%
Method of Reference [16]	97.1%

As shown in Table 3, the evaluation accuracy of the method in this paper is higher than the other three methods. Obviously, the method in this paper has greater advantages.

5. Conclusion

Industrial Internet of Things Situation Assessment Comprehensive security elements of various parts of the Industrial Internet of Things system to assess the overall security situation of the system. This paper proposes a PSO-SVM-based intelligent perception and assessment model for the security situation of the Industrial Internet of Things. Based on various parts of the Industrial Internet of Things system, it extracts the evaluation indicators of the security situation of the Industrial Internet of Things, and describes the specific evaluation method. The method is simulated and compared with support vector machines and Kalman entropy based on [15] and Naive Bayes based on [16]. The results show that the mentioned model has an evaluation accuracy rate. High advantage and strong feasibility.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202004_6(4).0011

References

[1] Wang Bin. Research on Information Security Protection Technology of Industrial Internet of Things [D]. University of Electronic Science and Technology of China, 2018

[2] Dai Xiaoli. Research on Internet of Things security technology [D]. Beijing University of Posts and Telecommunications, 2012.

[3] Wang Caiyin. Network Security Situation Assessment Based on the Combination of Grey Relation Analysis and Support Vector Machines [J]. Application Research of Computers, 2013, 30 (06): 1859-1862.

[4] LI F, ZHENG B, ZHU J, et al. A method of network security situation prediction based on AC-RBF neural network [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2014, 26 (5): 576-581. (Li Fangwei, Zheng Bo, Zhu Jiang et al. A network security situation prediction method based on AC-RBF neural network [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2014, 26 (5): 576-581.)

[5] XIE L, WANG Y. New method of network security situation awareness [J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37 (5): 31-35.

[6] Xie Lixia, Wang Yachao. New Network Security Situation Awareness Method [J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37 (5): 31-35.)

[7] Batsell S G, Rao N S, Shaanker M. Distributed Intrusion Detection And Attack Containment for Organizational Cyber Security [C / OL],http://www.ioc.oml.gov/projects/documents/containment.pdf, 2005.

[8] Wen C L, Wen C B. The Multiscale Sequential Filter with Multisensor Data Fusion Systems and Contral in Aerospace and Astronautics [C]. Proc of the 1st International Conference on Systems and Contral in Aerospace and Astronautice. 2006.

[9] Liu Xiaowu, Wang Huiqiang et al. Network security situational awareness model based on heterogeneous multi-sensor fusion [J]. Computer Science. 2008, 35 (8): 69-73.

[10] Li Xiaoyan. Research on network security situation prediction method based on wavelet neural network [D]. Hunan University, 2016.

[11] Wang Huiqiang. New progress in situational awareness of network security [J]. Journal of Daqing Teachers College, 2010, 30 (03): 1-8.

[12] FAN Rongzhen, ZHOU Mingkuai. Network Security Awareness and Tracking Method by GT [J]. Journal of Computational Information Systems, 2013, 9 (3): 1043-1050.

[13] Luo Zhao. Research on network security situation assessment and prediction technology based on neural network [D]. Northwest University, 2018.

[14] Fu Yan. Research and implementation of security privacy protection in IoT sharing platform [D]. Beijing Jiaotong University, 2011.

[15] Li Weiwei, Wang Li, Zhang Lin, Liu Jin. Multi-fault classification algorithm based on improved binary tree support vector machine [J]. Journal of Detection and Control, 2015, 37 (03): 34-39.

[16] Zhu Wenya. Kalman Entropy Model for Network Security Situation Estimation ［J］. Journal of Huaqiao University: Natural Edition, 2017, 38 (1): 101-104.

[17] Wen Zhicheng, Cao Chunli, Zhou Hao. Network Security Situation Assessment Method Based on Naive Bayes Classifier ［J］. Computer Applications, 2015, 35 (8): 2164-2186.