INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2020.14.105 Volume 14, 2020

A Prediction Method of Network Security Situation based on QPSO-SVM

Jian-an Zhang, Hui Luo

Kunming Branch, No.3 College, PLA Information Engineering University, Kunming650231, Yunnan, China

Received: August 16, 2020. Revised: November 18, 2020, Accepted: November 19, 2020. Published: November 20, 2020.

Abstract—In network security situation awareness system, situation prediction is the key point. The traditional intrusion detection method lacks scalability in the face of the changing network structure and lacks adaptability in the face of unknown attack types. In order to ensure and improve the accuracy of situation prediction, a QPSO-SVM prediction model is proposed by combining the optimization performance of quantum particle swarm optimization and the prediction accuracy of support vector machines. By adding the original sequence to the original sequence, this model weakens the irregular disturbance in the original sequence and enhances the regularity of the sequence. Compared with the traditional SVM and PSOSVM, the superiority of the prediction precision is better, the prediction accuracy can be ensured, and the validity of the model is tested by the simulation experiment.

Keywords— network security, situational prediction, SVM, PSO, QPSO

I. INTRODUCTION

WITH the rapid development of computer technology and network technology, people's work, study and life more and more dependent on the network, the resulting flow of network security problems are highlighted. The anomaly intrusion detection is a kind of strategy, improve the network security has become a hot spot at present. Network intrusion detection technology has been rapid development [1]-[3]. But because of the complexity of the network intrusion technique and diversity, and still can't find the network intrusion behavior and determine the function relationship between network data characteristics, many research methods are attempt to estimate the function relation between them and approximation, and machine learning research is the problem. Although it is unclear what network intrusion behavior and the function relation between the network data features, but it still can use the principle of machine learning, through the analysis of network data to predict whether network intrusion behavior occurs.

Invasion is to point to in the case of unauthorized any attempt to compromise the integrity of the network resources, confidentiality, or availability of intentional act. Intrusion detection is refers to has been implemented or are implementing or trying to implement intrusion detection and recognition, the key point of the collection system and the network information, and use of certain means to deal with these information, in order to determine whether deviating from attack and whether the existing security policy [4]. The intrusion detection system is designed for active protection system of network security, it is based on a certain security policy monitoring network system operation, found that all kinds of invasion behavior, attempt, or as a result, and automatically respond to detect intrusion characteristics, to effectively guard against unauthorized access or invasion behavior. The system generally adopts the misuse intrusion detection and anomaly intrusion detection of two kinds of processing methods. The former will first of all possible adverse, unacceptable behavior, a model is set up, all accord with the access behavior of the model will be determined as the invasion; The latter constructs a system model of normal access behavior, and any access that does not conform to this model will be determined as an intrusion.

Network intrusion detection mainly accomplishes the identification of intruders; Identification of intrusions; Detect and monitor successful security breakthroughs; Provide important security information. On industrial control network intrusion detection method compared with the computer network, there is no difference in nature between them is by collecting and analyzing network behavior, security logs, audit data and other information available on the network and a number of key information in a computer system, check the network or system whether there is a violation of security policy and the signs of being attacked [5]-[6].

IDS is a security management system used to identify abnormal activities and incomplete signatures in computers or networks. The number of methods and frameworks has been built many systems to detect intrusions. The single classification support vector machine (OCSVM) is widely used in the abnormal detection [7], but the OCSVM can not deal with the defect of the influence of the internal anomaly point and the outlier point on the decision function when it is applied to the anomaly detection. Tom Bartman study [8] introduced how to

network intrusion detection method combined with SCADA networks, industrial intrusion detection task, and also discusses the industry network attackers attack mode and network vulnerability. Wang Ming et al. [9] studied the function code characteristics of Modbus/TCP protocol. The pattern matching method is used to match the rules to determine abnormal or normal. It can detect some attacks by using the rules of intrusion detection, but only by analyzing the function code, it produces the omission behavior. Kim G[10] took advantage of the intrusion detection method of hierarchical misuse detection and anomaly detection, divided the normal training data into multiple subsets, and then created multiple OCSVM models using subset data. Although the process avoids the problem of internal anomaly detection, the effect of isolation point on OCSVM is not eliminated. Literature [11] used the improved holter-winters algorithm to predict network traffic, and achieved certain results. However, due to its only detection of network traffic characteristics, it is often difficult to detect the increasingly complex network abnormal traffic. Literature [12] describes the distribution of network traffic at different levels in different dimensions, and the detection accuracy is greatly improved compared with the single dimension. Literature [13] using ARIMA algorithm to the normal behavior of the web service model, when the confidence interval of characteristic value more than normal behavior, is judged to be abnormal, the method for anomaly detection has good effect in actual data. In Gupta and Shrivastava [14], the authors propose a new approach of combining SVM and Bee Colony to achieve high quality performance of IDS. Their algorithm is implemented and evaluated using a standard benchmark KDD99 dataset. Experimental results show that SVM with Bee colony achieves an average accuracy is 88.46%. In [15], this method uses a training set KDD-CUP99. The algorithm uses three main learning algorithms, SVM, naive Bias and J48 decision tree respectively. These algorithms are also implemented and evaluated respectively. The results show that the J48 algorithm and dimensionality reduction method are 97% advantages of AdaBoost classification learning efficiency. In Horng et al. (16); the authors proposed an SVM-based intrusion detection system, which combines a hierarchical clustering algorithm, a simple feature selection procedure, and the SVM technique. The hierarchical clustering algorithm provided the SVM with fewer, abstracted, and higher-qualified training instances that are derived from the KDD Cup 1999 training set.

Many studies have carried out intrusion detection and use from multiple machine learning algorithms, such as classification and clustering, or combining them with different ideas, as well as a feature selection method. Considering the past research, we should reduce the problem of false positives, because it should not be considered, and there seems to be a blank in this field. Therefore, in this article, we have put forward new ways to solve the gap, and provide the following methods.

Aiming at the shortcomings of the above methods and defects, in this paper, QPSO-SVM technology was applied to network abnormal intrusion detection, proposes a network intrusion detection model based on QPSO-SVM can reduce the variable dimension, remove noise pollution, eliminate the multiple correlation among variables, have an advantage in terms of rapid processing large sample data, the two organic combine, complementary advantages, in order to solve the abnormal intrusion detection of large sample modeling problem quickly. Experiments show that the proposed intrusion detection model has high detection rate and high accuracy for unknown attacks.

II. Procedure for Paper Submission

A. The Principles on Regression of SVM

SVM is a kernel based supervised machine learning technology to solve various classification and regression problems. It relies on the principle of structural risk minimization so that they are superior to existing neural network models in a wide range of pattern recognition in each field of research, classification, image processing, remote sensing, using a linear function hypothesis by Cristianini and Shotel "support vector machine learning system" The theory of training and learning algorithm realizes a learning bias derived from statistical learning theory, [30]. In support vector machine, every sample data is regarded as an n-dimensional space, and an optimal hyperplane (decision boundary) is constructed to classify different classes of samples. The idea of SVM on regression is to input the training samples into the SVM with a pre-set regression function for training, and obtain the regression function by determining the important parameters of the function through continuous fitting. How to derive the regression function of SVM is described below.

Let $\{x_i, y_i\}(i = 1, 2, \mathrm{L}\ , n)$ denote the training samples of network security status, where x_i and y_i denote the input vector and output, n denotes the number of training samples. The idea of SVM regression is to find a nonlinear mapping from input to output in the high-dimensional feature space. It is in this space that the regression function is used to regress the training samples. The function $f(x)$ is defined as

$$f(x) = W \times \varphi(x) + b \qquad \varphi : R^n \to G, W \in G \quad (1)$$

Where W denotes the weight vector, and b denotes the bias vector.

SVM is intended to address the following optimization problem.

$$\min J = \frac{1}{2}\|W\|^2 + C\sum_{i=1}^{n}\left(\xi_i + \xi_i^*\right) \qquad (2)$$

subject to

$$\begin{cases} y_i - W \times \varphi(x) - b \le \varepsilon + \xi_i \\ W \times \varphi(x) + b - y_i \le \varepsilon + \xi_i^* \\ \xi_i \ge 0, \xi_i^* \ge 0 \end{cases} \quad (3)$$

Where C denotes the penalty parameter, ξ_i, ξ_i^* denote the relaxation variables, ε denotes the insensitive loss function used to control the error of regression. And it is defined as

$$L_\varepsilon\left(f(x_i), y_i\right) = \begin{cases} \left|f(x_i) - y_i\right| - \varepsilon & \left|f(x_i) - y_i\right| \ge \varepsilon \\ 0 \quad \text{otherwise} \end{cases} \quad (4)$$

The optimization problem can be addressed using the method of Lagrange multiplier, which introduces the multipliers α_i and α_i^* to obtain the Lagrange function.

$$\begin{aligned} L = \frac{1}{2}\|W\| + C\sum_{i=1}^{n}\left(\xi_i + \xi_i^*\right) - \sum_{i=1}^{n}\left(\xi_i\beta_i - \xi_i^*\beta_i^*\right) \\ -\sum_{i=1}^{n}\alpha_i\left(\xi_i + \varepsilon - y_i + f(x_i)\right) - \sum_{i=1}^{n}\alpha_i^*\left(\xi_i^* + \varepsilon - y_i + f(x_i)\right) \end{aligned} \quad (5)$$

Based on these derivations, the final expression of SVM regression can be written as

$$f(x) = \sum_{i=1}^{n}\left(\alpha_i - \alpha_i^*\right)\left(\varphi(x_i), \varphi(x)\right) + b \quad (6)$$

The curse of dimensionality can be avoided by substituting the kernel function $k(x, x_i)$ for $\left(\varphi(x_i), \varphi(x)\right)$. The Gaussian kernel function is empirically more effective than other choices and is thus used as the kernel function in this paper.

B. Optimization of SVM Parameters

The mathematical complexity of the optimization of SVM parametersis examined as follows.

STEP1. Given the data set *T*, *T* is divided into set A and set B according to a fixed proportion.

STEP2. Select the kernel function, set the initial value of the kernel parameter in the kernel function, and use the optimization tool to solve the optimal solution, that is, the optimal value of the kernel parameter.

STEP3. The initial value of penalty parameter C is set by substituting the optimal value of kernel parameter obtained in STEP2, and then the optimal solution of parameter C is determined by using optimization tools.

STEP4. The optimal values of kernel parameters and penalty parameters obtained in STEP2 and STEP3 are substituted into the support vector machine model, and then the classification performance of SVM is measured by the average training sample classification accuracy rate and the average test sample classification accuracy rate by using the 50 fold cross validation technology.

The 50 fold cross validation technique is a simple and reliable cross validation method. The 50 fold cross validation method is that the original data set is randomly divided into five disjoint subsets, each of which is approximately the same size. Each time, four subsets are selected as the training set, and SVM model is established with the given parameters, and then the sample points in the remaining subset are tested.

The SVM-based model for the prediction of network security status is very sensitive to the choice of model parameters and the prediction accuracy is dependent on the choice of parameters. These parameters include the penalty factor C, the width of kernel function σ, and the insensitive loss function ε. Setting C to an excessively high or small value may cause overlearning or underfitting. The parameter σ is responsible for controlling the complexity of the optimal solution to the non-linear problem; setting it to an excessively high or small value will reduces the generalization ability of SVM. The parameter ε denotes the expectation of training error, and it determines the number and computational complexity of SVMs. Here, the three parameters are optimized using the particle swarm optimization (PSO) algorithm.

The quantum particle swarm optimization (QPSO) algorithm is a variant of PSO. As the particle searches a limited region, the traditional PSO methods are almost unable to cover the entire solution space and thus cannot guarantee convergence to the globally optimal solution. QPSO combines the idea of PSO and quantum computing. The location of quantum particle is coded using the quantum bits and updated through the quantum rotate gate, thereby considerably improving the randomness of particle location. The particles thus have a higher possibility of appearing at any location in the solution space throughout. By searching the solution space in its entirety, QPSO has greater ability to find the global optimum and provides an approach for the defect of the traditional PSO algorithm.

The location of the quantum particle is represented with the quantum bit and is defined as

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_l \\ \beta_1 & \beta_2 & \ldots & \beta_l \end{pmatrix} \quad (7)$$

where $\left|\alpha_j\right|^2 + \left|\beta_j\right|^2 = 1, (j = 1, 2, ..., l)$. To make the algorithm simpler and more effective, we set $0 \le \alpha_j \le 1$ and $0 \le \beta_j \le 1$ and thus have $\beta_j = \sqrt{1 - \alpha_j^2}$. The definition of the location of the i-th quantum particle can be simplified as

$$x_i = \left(\alpha_{i1} \quad \alpha_{i2} \quad \ldots \quad \alpha_{il}\right) = \left(x_{i1} \quad x_{i2} \quad \ldots \quad x_{il}\right) \quad (8)$$

The location of the i-th quantum particle is updated using the

quantum rotate gate and let $R\left(\theta_{ij}^{k}\right)=\begin{pmatrix}\cos\theta_{ij}^{k} & -\sin\theta_{ij}^{k}\\ \sin\theta_{ij}^{k} & \cos\theta_{ij}^{k}\end{pmatrix}$. Using the quantum rotate gate $R\left(\theta_{ij}^{k}\right)$, the j-th quantum bit of the i-th quantum particle can be written as

$$\mathrm{x}_{ij}^{k+1}=\left|R\left(\theta_{ij}^{k}\right)\mathrm{x}_{ij}^{k}\right|=\left|\begin{pmatrix}\cos\theta_{ij}^{k} & -\sin\theta_{ij}^{k}\\ \sin\theta_{ij}^{k} & \cos\theta_{ij}^{k}\end{pmatrix}\mathrm{x}_{ij}^{k}\right| \tag{9}$$

Similarly, it can be simplified as

$$\mathrm{x}_{ij}^{k+1}=\left|\mathrm{x}_{ij}^{k}\times\cos\theta_{ij}^{k+1}-\sqrt{1-\left(\mathrm{x}_{ij}^{k}\right)^{2}}\times\sin\theta_{ij}^{k+1}\right| \tag{10}$$

When the quantum rotation angle $\theta_{ij}^{k}=0$, the quantum bit can be updated using the quantum nor gate V, and the updating process can be written as

$$\mathrm{x}_{ij}^{k+1}=\mathbf{V}\mathrm{x}_{ij}^{k}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\mathrm{x}_{ij}^{k} \tag{11}$$

It can be simplified as

$$\mathrm{x}_{ij}^{k+1}=\sqrt{1-\left(\mathrm{x}_{ij}^{k}\right)^{2}} \tag{12}$$

The major idea of QPSO is to transform the updating of particle location and speed into the updating of quantum particle location and rotation angle.

Therefore, the function capable of representing the controlling performance should be used as the fitness function. The metric of multiplying the step response time and the integral of absolute error (IATE) is very feasible and selective. Because of this property, IATE is adopted in this paper as the fitness function , and

$$\begin{cases} J_{ITAE}=\sum_{k=0}^{\frac{\mathrm{L}}{\mathrm{h}}}k\mathrm{h}\left|e\left(k\mathrm{h}\right)\right| \\ \left|e\left(\mathrm{kh}\right)\right|=\left|y\left(k\mathrm{h}\right)-r\left(k\mathrm{h}\right)\right| \end{cases} \tag{13}$$

where h denotes the step size, L denotes the computing length. The computing accuracy increases with an increase in L and a decrease in h. Here, h=0.01s and L=100s. Let denote the output value of the closed-loop system at the corresponding time, and denote the given value in the system, which is set to 1 during simulation. A small value of indicates a short control period of step response and a small steady state error.

In QPSO, updating the rotation angle and location of the i-th quantum particle at the d-th dimension is equivalent to updating the speed and location of the corresponding particle. This process can be written as

$$\theta_{id}^{k+1}=c_1\cdot\varepsilon_1\cdot\left(P_{id}^{k}-x_{id}^{k}\right)+c_2\cdot\varepsilon_2\cdot\left(P_{gd}^{k}-x_{id}^{k}\right) \tag{14}$$

$$x_{id}^{k+1}=\begin{cases}\sqrt{1-\left(x_{id}^{k}\right)^{2}}, & \theta_{id}^{k+1}=0\\ \left|x_{id}^{k}\times\cos\theta_{id}^{k+1}-\sqrt{1-\left(x_{id}^{k}\right)^{2}}\times\sin\theta_{id}^{k+1}\right|, & \theta_{id}^{k+1}\neq 0\end{cases} \tag{15}$$

Where $1\le i\le m$, $1\le d\le 5$, k and k+1 denote the number of iterations, θ_{id}^{k} denotes the rotation angle of the i-th quantum particle at the d-th dimension during the k-th iteration, ε_1 and ε_2 denote random numbers which follows the Gaussian distribution with a mean of zero and a variance of 1, c_1 and c_2 control the degree of influence that the locally optimal solution of individual quantum particles and the globally optimal solution of the entire quantum particle swarm have on the process of updating the quantum particle's location, x_{id}^{k} denotes the location of the i-th particle at the d-th dimension during the k-th iteration, P_{id}^{k} denotes the location of the local extreme point of the i-th particle at the d-th dimension during the k-th iteration, P_{gd}^{k} denotes the location of the global extreme point of the entire particle swarm at the d-th dimension during the k-th iteration.

In summary, the network security situation prediction model in this paper is shown in Figure 1.

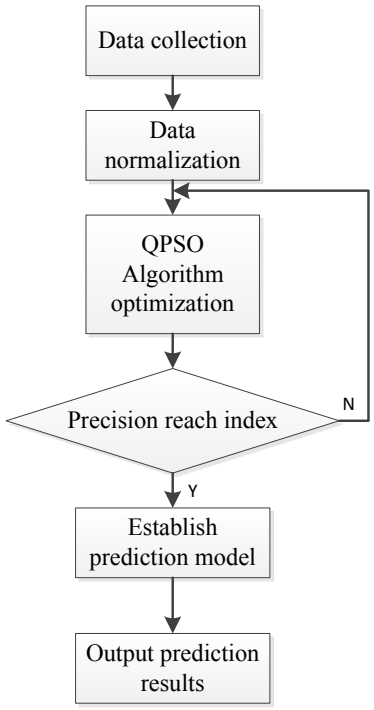

Fig. 1. Network security situation prediction model process

III. Simulation Experiment

A. Data Source

The simulation data comes from the KDD CUP 99 database. The four types of attacks include the Denial of Service (DOS), Remote Gain Root (U2R), User to Root (U2L), and Probe. A total of 1000 normal data samples, 100 DOS samples, 100 R2L samples, 120 U2R samples, and 120 Probe samples are randomly extracted from the database.

The irregularity and non-linearity associated with the status of network status makes it a big challenge to establish an ideal prediction model. As we know, the additive process can explicitly reveal the integral property or pattern of the disordered original data without affecting the pattern of the original data sequence. Therefore, an additive operation is first performed on the time sequence $\left\{x^{x(0)}(1), x^{x(0)}(2), \cdots, x^{x(0)}(n)\right\}$ of all original status values in the prediction model, yielding a new sequence $\left\{x^{x(1)}(1), x^{x(1)}(2), \cdots, x^{x(1)}(n)\right\}$, where

$$x^{(1)}(1) = \sum_{i=1}^{k} x^{(0)}(i) \quad k = 1, 2, \cdots n \tag{16}$$

Because the SVM is sensitive to the data in 0-1 and can be trained very fast, the added data need to be normalized.

$$x^{(1)}(i)' = \frac{x^{(1)}(i) - x^{(1)}(\min)}{x^{(1)}(\max) - x^{(1)}(\min)} \tag{17}$$

where $x^{(1)}(i)$ denotes the added value, $x^{(1)}(i)'$ denotes the normalized added value, $x^{(1)}(\max)$ and $x^{(1)}(\min)$ denote the maximal and minimal of the added values.

In the end of the experiment, the accuracy of the prediction model is measured using the mean of relative error. Let s_i denote the actual status of the i-th sample, and s_i' denote the predicted value. The relative prediction error φ_i of this sample can be defined as

$$\varphi_i = \frac{\left|s_i' - s_i\right|}{s_i} * 100\% \tag{18}$$

The mean of relative error φ for all samples is defined as

$$\varphi = \frac{1}{n} \sum_{i=1}^{n} \varphi_i \tag{19}$$

B. Simulation Analysis

In order to verify the effectiveness and generality of the proposed network security situation prediction model, SVM, PSO-SVM method and QPSO-SVM method are selected to compare the network situation data. Take the first 475 sequences as training set and the latter 25 as the test set. At this point, the predicted result is cumulative result, and the result is the final prediction after accumulating and restoring. Compare the prediction results of the three methods, as shown in Figure 2.

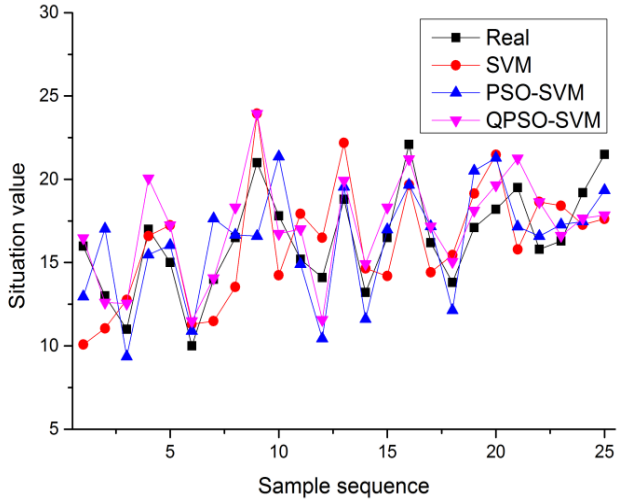

Fig. 2 Comparison of prediction results

The error comparison is shown in Figure 3. It can be seen from Figure 3 that the error of this method is lower than that of PSO-SVM at most sample points.

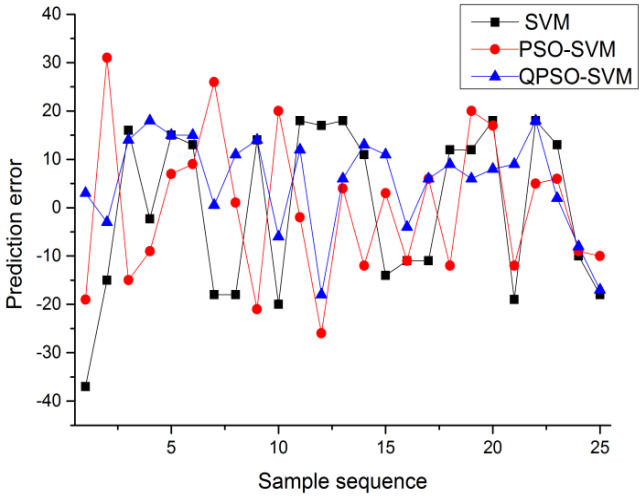

Fig. 3 Prediction error contrast

In order to compare the results of the two methods more clearly, the evaluation criteria of the three methods, that is, maximum error, minimum error and mean error. The comparison results are shown in Table 1. It can be seen from the table that all indexes of the method proposed in this paper are higher than SVM and PSO-SVM methods.

Table 1 Error comparison of three model prediction indexes

Prediction Model	Max error	Min error	Mean error
SVM	42.8%	2.31%	15.53%
PSO-SVM	32.1%	1.05%	12.52%
QPSO-SVM	18.9%	0.52%	9.86%

Based on the theory of artificial intelligence, an integrated network security situation prediction model based on ensemble learning boosting algorithm can be considered, which can realize the comprehensive evaluation of the current and future security situation of the target network.

The future research direction can use machine learning method to predict the time series of security situation, and propose a network security situation prediction model based on foa-svr algorithm. This method combines the excellent nonlinear fitting ability of SVR algorithm and the good global optimization ability of FOA, and uses FOA to embed the dimension n into the time series of network security situation value, The penalty coefficient C of SVR and the parameter g of RBF kernel function are optimized to avoid the blindness of parameter selection and improve the accuracy of network security situation prediction.

IV. Conclusion

NID systems have been implemented by many different approaches, different approaches aim at different goals, such as increasing accuracy,reducing false alarms, and reducing modleing time. In this paper, a support vector machine network anomaly detection method optimized by quantum particle swarm optimization (QPSO) is proposed. The simulation results show that the prediction accuracy of SVM is improved effectively, and the effectiveness of the method is proved by experiments. Simulation experiments with two sets of different data show that the prediction model is effective and generalization. The system reduces the error rate of intrusion detection to a certain extent, improves the efficiency of intrusion detection and improves the detection degree of unknown threat to the network. It has important practical significance and application value. The next step is to reduce the amount of computation and complete the higher iterations from data dimensionality reduction, so as to improve the accuracy of detection. Because of the rapid development of cloud computing technology at present stage, we can improve computing power through cloud computing, and further improve the performance of network intrusion detection.

References

[1] Hajisalem V, Babaie S. "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection", *Computer Networks*, vol. 136, pp. 37-50, 2018.

[2] Hamed T, Dara R, Kremer S C. "Network intrusion detection system based on recursive feature addition and bigram technique", *Computers & Security*, vol.73, pp. 137-155, 2018.

[3] Akashdeep, Manzoor I, Kumar N. "A feature reduced intrusion detection system using ANN classifier", *Expert Systems with Applications*, vol. 88, pp. 249-257, 2017.

[4] Verwoerd T, Hunt R. "Intrusion detection techniques and approaches", *Computer Communications*, vol. 25, no.15, pp. 1356-1365, 2002.

[5] KNOWLES W, PRINCE D, JONES K, et al. "A survey of cyber security management in industrial control systems", *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52-80, 2015.

[6] SHANG WENLI, AN PANFENG, WAN MING, et al. "Research and development overview of intrusion detection technology in industrial control system". *Application Research of Computers*, vol. 34, no. 2, pp. 328-333, 2017.

[7] HOFFMANN H. "Kernel PCA for novelty detection", *Pattern Recognition*, vol. 40, no. 3, pp. 863-874, 2007.

[8] TOM BARTMAN, JASON KRAFT. "An Introduction to Applying Network Intrusion Detection for Industrial Control Systems", AISTech2016-The Iron & Steel Technology Conference and Exposition. Pittsburgh, USA: May 16–19, 2016.

[9] Hiba Basim Alwan, Ku Ruhana Ku-Mahamud, Solving SVM model selection problem using ACOR and IACOR, WSEAS transactions on computers, pp. 356-365, Issue 9, Volume 12, September 2013.

[10] WAN MING, SHANG WENLI, ZENG PENG, et all. "Modbus/TCP Communication Control Method Based on Deep Function Code Inspection", *Information and Control*, vol. 45, no. 2, pp. 248-256, 2016.

[11] KIM G, LEE S, KIM S. "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection". *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690-1700, 2014.

[12] Lv Junhui, Zhou Gang, Jin Yi. "Adaptive aberrant network traffic detection algorithm based on time series forecast", *Journal of Beijing University of Aeronautics and Astronautics*, vol. 35, no. 5, pp. 636- 639, 2009.

[13] Ge Xiaoming, Chen Xingshu, Wang Haizhou, et al. "An anomalous behavior detection model in cloud computing", *Tsinghua Science and Technology*, vol. 21, no. 3, pp. 322-332, 2016.

[14] Shirani P, Azgomi M A, Alrabaee S. "A method for intrusion detection in web services based on time series," IEEE 28th Canadian Conference on Electrical and Computer Engineering, Halifax: IEEE, 2015, pp. 836-841.

[15] Gupta, M., Shrivastava, S.K., "Intrusion detection system based on SVM and bee colony", *Int. J. Comput. Appl.* vol. 111, 27–32, 2015.

[16] Mazraeh, S., Ghanavati, M., Neysi, S.H.N.,"Intrusion detection system with decision tree and combine method algorithm", *Int. Acad. J. Sci. Eng.* vol. 3, pp. 21–31, 2016.

[17] Horng, S.J., Perkasa, C.D., "A novel intrusion detection system based on hierarchical clustering and support vector machines", *Expert Syst. Appl*, vol.38, pp. 306–313, 2011.

Jian-an Zhang was born on June 10, 1972**.** He received the Master degree in Computer Science and Technology from PLA Information Engineering University. Currently, he is a researcher (professor) at Kunming Branch, No.3 College, PLA Information Engineering University, China. His major research interests include information security and cryptography. He has published many papers in related journals.

Hui Luo was born on Sep. 14, 1981**.** He received the Master degree in Software Engineering from Yunnan University. Currently, he is a researcher (assistant professor) at Kunming Branch, No.3 College, PLA Information Engineering University, China. His major research interests include information security and data analysis. He has published many papers in related journals.