EURASIP Journal on Information Security

RESEARCH Open Access

Situation prediction of large-scale Internet of Things network security

Wenjun Yang[1,2], Jiaying Zhang[1,2*], Chundong Wang[1,2] and Xiuliang Mo[1,2]

Abstract

The Internet of Things (IoT) is a new technology rapidly developed in various fields in recent years. With the continuous application of the IoT technology in production and life, the network security problem of IoT is increasingly prominent. In order to meet the challenges brought by the development of IoT technology, this paper focuses on network security situational awareness. The network security situation awareness is basic of IoT network security. Situation prediction of network security is a kind of time series forecasting problem in essence. So it is necessary to construct a modification function that is suitable for time series data to revise the kernel function of traditional support vector machine (SVM). An improved network security situation awareness model for IoT is proposed in this paper. The sequence kernel support vector machine is obtained and the particle swarm optimization (PSO) method is used to optimize related parameters. It proves that the method is feasible by collecting the boundary data of a university campus IoT network. Finally, a comparison with the PSO-SVM is made to prove the effectiveness of this method in improving the accuracy of network security situation prediction of IoT. The experimental results show that PSO-time series kernel support vector machine is better than the PSO-Gauss kernel support vector machine in network security situation prediction. The application of the Hadoop platform also enhances the efficiency of data processing.

Keywords: Network security, Situation prediction, Sequence correlation, Support vector machine

1 Introduction

With the popularity of the Internet of Things and the rapid development of cloud computing, security issues become increasingly prominent. Security vulnerabilities and security incidents are increasing notably. Network security incidents have occurred occasionally such as network worms, hackers dragging databases, 0-day exposure, and privacy data leakage. Network security is becoming the focus of many nations, enterprises, and individuals. China set up the Central Internet Security and Informatization Leading Group in February 2014, which indicated that the government had put network security on the national strategic position [1].

The Internet of Things (IoT) is a new technology rapidly developed in recent years. With the development of communication technology, IoT devices have made good development in smart cities, wireless sensing, cloud computing, and many other fields. However, with the popularity of Internet of Things devices, security and privacy issues have become increasingly prominent [2–6]. Due to increasingly serious problems of IoT network security, network security situation awareness of IoT comes into being and gradually becomes the focus of the network security field. By assessing the operating status of the network in real-time and promptly predicting the problems before the security incidents occur, the network security situation awareness can help the administrators make the right decisions [7].

Utilizing the characteristic of situational factors that are randomness, time-sequence, and complexity, an improved network security situation awareness model for IoT is proposed in this paper. Considering the close relationship between the network security situation and time, we agree that situation prediction of network security is a kind of time series forecasting problem in essence [8]. A modification function is constructed that is suitable for time series data to revise the kernel function

* Correspondence: 516350070@qq.com
[1]Key Laboratory of Computer Vision and System, Ministry of Education, Tianjin University of Technology, Tianjin 300384, China
[2]Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, Tianjin 300384, China

of traditional support vector machine. The sequence kernel support vector machine is obtained and the particle swarm optimization method is used to optimize related parameters. It proves that the method is feasible by collecting the boundary data of a university campus network. Finally, a comparison with the PSO-SVM is made to prove the effectiveness of this method in improving the accuracy of network security situation prediction.

The main contributions of our work are listed as follows:

1) We propose an improved network security situation awareness model for IoT based on PSO-time series kernel support vector machine.
2) We employ a sequence kernel support vector machine and the particle swarm optimization to optimize related parameters, improving the accuracy of network security situation prediction.
3) The experimental results show that PSO-time series kernel support vector machine is greatly effective.

1.1 Roadmap

The rest of this paper is organized as follows. First, we survey related work in Section 2. Then, we introduce the design of network security situation prediction of IoT in Section 3. We describe the system implementation and report evaluation results in Section 4. Finally, we conclude our work in Section 5.

2 Related work

The concept of situational awareness originated from the military field which requires an understanding of the strengths and weaknesses of the enemy in order to make the right decisions on the battlefield. In 1988, Endsley [9] gave the definition of situational awareness for the first time, which was the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status after some variables had changed. In 1999, Bass [10] first proposed the concept of Cyberspace Situation Awareness, which aimed at using the SA for the network management and network security to improve the cognitive ability of administrators to shorten the decision time.

There were many groundbreaking researches in the field of network security situation awareness [11]. After analyzing the concept of network situational awareness, Bass [12] proposed a framework for network security situation based on multi-sensor data fusion technology. By reasoning to identify the intruders' identity and locate intrusion goals, it was a good way to assess the security status of the network.

A prediction method combined with the quantitative and qualitative of network security situation based on the cloud was proposed by Lei Xuan [13]. The future situation was predicted by combining the current trend with the prediction rules mining from history evolvement data.

After the assessment of current network security situation, You and Ren [14, 15] proposed different prediction models based on a neural network. By using the advantage of a neural network in dealing with nonlinear problems, they implement the accurate forecast of the network security situation.

A complex network-based network security situation prediction mechanism was proposed by Li [16]. Using the model of Markov, we can not only trace the dynamic behavior of the numerical fluctuations in the security situation but also predict security state effectively.

Chen [17] proposed a prediction method of network security situation based on the algorithm of IHS_LSSVR. An improved Harmony Search (IHS) algorithm is used to optimize the parameters of least squares support vector machine and then to forecast the network security status.

The related principles of the proposed method are described below.

3 Network security situation prediction of IoT

3.1 Data analysis initial normalization based on Hadoop

In the Internet of Things, the massive heterogeneous data about security contain various information. In this paper, MapReduce technology is adopted to realize data analysis and fusion processing based on attribute phase heterogeneity. The network data of IoT usually includes logs and traffic. Therefore, in the map phase, the log and the flow file are read and the packets are extracted. Converts the device address, time, and other attributes of the packet to the key-value pair of MapReduce processing for <key,value> format, the process is Map<key1,value1 > →list<key2,value2>. Key1 represents the number of the data line. Value1 represents the content of each row of packets. The packet contains complete data content. Key2 is a collection of important attributes needed. Value2 is the remaining property in the packet. Because both key2 and value2 have multiple attributes. We use # to separate properties when implemented. In case of subsequent data parsing errors, the processed property item becomes like a list<string1,string2 > string. In the Reduce stage, the Hadoop platform was used to preprocess the string, and the record of the upcoming string was merged to realize Reduce<key2,value2 > →list<key3, value3>. Extract all administrative configuration and system run class logs from the log file. The log (the event_type, priority, the user, sourceIP, operation, the time, the result) of the same is aggregated into a log record. At the same time, increase the count origID and attribute, the count records including log which is composed of

several raw log, logID origID record raw logs, and semicolons to separate the Map Reduce input and output of the details in Table 1, as shown in Table 2

Firewall logs can reflect network traffic, and the log aggregation of traffic abnormal classes is mainly extracted from the firewall logs and related to connection classes. Similar configuration to polymerization with the management, traffic exception class log aggregation also need to increase the count origID and attribute, the role of the same, and Map Reduce the input and output of the details such as Table 3, shown in Table 4.

Network attack is usually in a variety of network security equipment in the log traces of attack [18], according to the above design, log aggregation rules and attribute characteristics to aggregation of attack mode, increase the count, origID, and mode three attributes. Graphs of input and output details are shown in Table 5 and 6.

Through clustering algorithm, this node initializes the firewall and IDS logs through Hadoop and builds a comprehensive and accurate data source for the subsequent chapters of this article, based on the prediction of log files.

3.2 Situation prediction model based on sequence kernel support vector machine

On the basis of different levels, different information sources, and different needs, this paper proposed a network security situation prediction model based on sequence kernel support vector machine as shown in Fig. 1.

In the model, the whole situation of the network is divided into four first-class indicator situations: threat situation, fragile situation, stable situation and disaster situation [19]. Each first-class indicator situation is described by several secondary indicators. We use the T-S fuzzy neural network (FNN [20]) method, which makes secondary indicators as input and first-class indicator situation as output to get the threat situation, fragile situation, stable situation, and disaster situation, respectively. Finally, the analytic hierarchy process (AHP) is used to decide the relative weight of each first-class indicator situation, thus the whole situation of the network is obtained [21].

Finally, the PSO-sequence kernel support vector machine is used to deal with the value of the whole situation; thus, we get the prediction results of the future state of the network. Situation prediction of network security can help network administrators have a good understanding of network status. For network attacks, administrators can release network security warning timely.

Table 1 Manages the Map phase input output for the configuration class log

Map	INput	OUTput
Key	Row value	Event_type&priority &user&sourceIP &operation&time &result
Value	log	1&logID&device_type

Table 2 Manage the Reduce phase input output for the configuration class log

Reduce	INput	OUTput
Key	Event_type&priority &user&sourceIP&operation &time&result	Event_type&priority &user&sourceIP&operation &time&result
Value	1&lodID&device_type	n&lodID&device_type

3.3 Support vector machine

Support vector machine (SVM) is a general and effective machine learning method based on statistical learning theory [22]. It has many obvious advantages in the study of complex nonlinear prediction. The regression function of network security situation prediction based on support vector machine is as follows:

Set up network security situational training sample is $\{x_i, y_i\}$, $i = 1, 2, \ldots n$, Where x_i and y_i represent input vectors and output values. n is the training sample number. The prediction idea of SVM is to find a nonlinear mapping from input to output and to map data into high dimensional feature space. In this feature space, the training samples are predicted by prediction equation $f(x)$.

$f(x)$is defined as follows:

$$f(x) = w \times \phi(x) + b, \phi : R^n \rightarrow G, w \in G \tag{1}$$

Where w is the weight vector and b is the bias vector. SVM solves the optimization problem as follows:

$$\min J = \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}(\xi + \xi^*) \tag{2}$$

Constraint conditions are as follows:

$$\begin{cases} y_i - w \cdot x_i - b \le \varepsilon + \xi_i \\ \mathrm{w} \cdot \mathrm{x_i} + \mathrm{b} - y_i \le \varepsilon + \xi_i^* \\ \xi_i \ge 0, \xi_i^* \ge 0 \end{cases} \tag{3}$$

where C is the penalty parameter, ξ_i and ξ_i^* are slack variables, ε is insensitive loss function.

Table 3 The MAP phase input and output of the traffic exception class log

Map	INput	OUTput
Key	Row value	sourceIP&sourcePort &destPort&time&protocol
Value	log	Sum(inpackage)&sum (outpackage)&sum(sent) &sum(recevice)&1&logID&device

Table 4 The Reduce phase input and output of the traffic exception class log

Reduce	INput	OUTput
Key	sourceIP&sourcePort&dest Port&time&protocol	sourceIP&sourcePort&dest Port&time&protocol
Value	Sum(inpackage)&sum (outpackage)&sum(sent) &sum(recevice)&1&logID&device	Sum(inpackage)&sum (outpackage)&sum(sent) &sum(recevice)&n&logID &device

ε is defined as follows:

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

By introducing Lagrange multipliers, the nonlinear prediction problem is transformed into the optimization problem as follows:

$$\begin{aligned} L = & \frac{1}{2}\omega^T\omega \\ & + c\sum_{k i=1}^{k}\left(\zeta_i + \zeta_i^*\right) - \sum_{i=1}^{k} a_i(\zeta_i + \varepsilon - y_i + f(x_i)) \\ & - \sum_{i=1}^{k} a_i\left(\zeta_i^* + \varepsilon - y_i + f(x_i)\right) - \sum_{i=1}^{k}\left(\eta_i\zeta_i + \eta_i^*\varepsilon_i^*\right) \end{aligned} \tag{5}$$

Where a_i and α_i^* are Lagrange multipliers.

According to the KKT condition, the support vector machine prediction problem can be solved by solving the dual problem in formula (2), that is

$$f(x) = \sum\nolimits_{i=1}^{n}\left(\alpha_i - \alpha_i^*\right) k(x, x_i) + b \tag{6}$$

Constraint conditions are as follows:

$$\begin{cases} \partial_b L = 0 \Rightarrow \sum\nolimits_{\mathrm{i}=1}^{l}\left(\alpha_i - \alpha_i^*\right) = 0 \\ 0 \le \alpha_i, \alpha_i^* < c, \mathrm{i} = 1, 2, \cdots, l \\ \partial_\omega L = 0 \Rightarrow \omega = \sum\nolimits_{i=1}^{l}\left(\alpha_i - \alpha_i^*\right)\Phi(x_i) \end{cases} \tag{7}$$

where $k(x, x_i)$ is the kernel function of the support vector machine, describing the inner product of the high dimensional feature space.

As the Gauss kernel function is better than other kernel functions, this paper uses the Gauss kernel function as the kernel function of support vector machine. Gauss kernel function is defined as follows:

Table 5 The Map phase input and output of the attack class event log

Map	INput	OUTput
Key	Row value	sourceIP&destIP&destPort&time
Value	log	1&logID&device&AttRule 1/AttRule2/AttRule3/AttRule4

Table 6 The Reduce phase input and output of the attack class event log

Reduce	INput	OUTput
Key	sourceIP&destIP&destPort&time	sourceIP&destIP&destPort&time
Value	1&logID&device&AttRule1/ AttRule2/AttRule3/AttRule4	n&logID&device&AttRule1/ AttRule2/AttRule3/AttRule4

$$k(x, x_i) = \exp\left(\frac{\|x - x_i\|^2}{\sigma^2}\right) \tag{8}$$

Bringing Eq. (8) into Eq. (6), the final expression of the SVM prediction model is as follows:

$$f(x) = \sum\nolimits_{i=1}^{n}\left(\alpha_i - \alpha_i^*\right) \exp\left(\frac{\|x - x_i\|^2}{\sigma^2}\right) + b \tag{9}$$

where σ is the width of the Gauss kernel function.

3.4 Support vector machine based on time sequence kernel

Network security situation prediction is closely related to time. But the Gauss kernel function cannot reflect the time correlation. By fusing the Gauss kernel function with temporal correlation, we can improve the traditional support vector machine.

In order to fuse the Gauss kernel function with temporal correlation, the definition of the window, modified kernel function, and time sequence kernel function is given.

3.4.0.1 Definition 1 The input space is divided into m sub-windows according to the time points, that is, $T = \{T_1, T_2, \ldots, T_{m-1}, T_m,\}$. The definition of the window function is as follows:

$$g_{T_s}(x) = \begin{cases} \omega_{is}, & x \in T_s \\ \omega_{is}^*, & \text{otherwise} \end{cases} \tag{10}$$

where, m is the number of sub-windows, which is related to time characteristics of the learning task. ω_{is} and ω_{is}^* are weight parameters, which represent the time correlation between two points to be predicted in the data set. If the two points to be predicted are close to each other in time characteristics (for example less than the threshold θ, they belong to the same sub-window and the kernel function has a larger weight. The values of ω_{is} and ω_{is}^* are related to the level of the window and the radius of the window. In general, in the same sub-window, ω_{is} should be greater than ω_{is}^*.

3.4.0.2 Definition 2 By modifying Gauss kernel function with a window function, we get the modified kernel function.

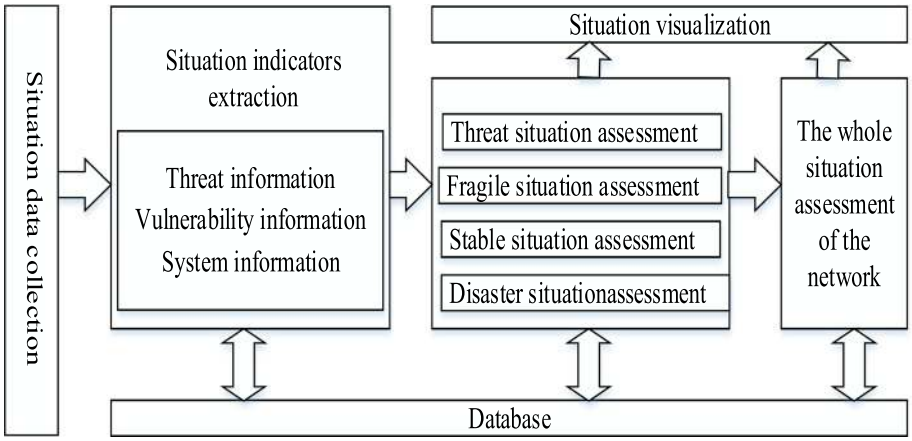

Fig. 1 Network security situation prediction model based on sequence kernel support vector machine

$$F_{T_s}(x) = f(x)\, g_{T_s}(x) \tag{11}$$

where $f(x)$is the Gauss kernel function.

The modified kernel function judges if the two points to be predicted are in the same window by a window function. Then, we get the modified value and function.

3.4.0.3 Definition 3 The time sequence kernel function can be defined after the window function and modified kernel function. The time sequence kernel function is as follows:

$$F^T(x) = \sum_{i=1}^{L} F_{T_s}(x) \tag{12}$$

where L is the level of the window.

The choice of the number of window layer and the radius of the sub-window should improve the support vector machine prediction ability greatly.

3.5 Parameters optimization of support vector machine

The network security situation prediction model based on SVM is sensitive to the parameters. The accuracy of SVM prediction is determined by the choice of parameters. The parameters affecting the accuracy of SVM prediction include the penalty factor C, the width of the kernel function σ and the insensitive loss function ε. The value of C is too large or too small will produce the phenomenon of over learning or less learning. σ is used to control the complexity of the optimal solution of the nonlinear problem in SVM. The value of $\sigma$is too large or too small will reduce the generalization ability of SVM. ε is the expectation of error in training. It determines the number of support vectors and the computational complexity of SVM. Therefore, the particle swarm optimization algorithm is used to optimize the three parameters in this paper. Particle swarm optimization algorithm is an optimization algorithm based on swarm intelligence. It uses a particle which has no quality and no volume as an individual and provides simple action rules for each particle. Thus the whole particle swarm exhibits complex characteristics. Finally, the optimal solution is found through the collaboration between individuals. In this paper, the particle swarm optimization algorithm is used to optimize the three parameters of SVM. We construct a three-dimensional solution space. c, σ, and ε are respectively represented as one-dimensional of three-dimensional space. The specific working process of the particle swarm algorithm is as follows. Setting fitness function is F. F is defined as the average error of the forecast data. Randomly construct the initial population which consists of i particles. Give all particles initial position $W_i^1$and initial speed V_i^1. According to the formula (13) and (14), the optimal solution could be found.

$$\begin{aligned} V_i^{(k+1)} = {} & \omega_i V_i^k + c_1\gamma_1\left(p_{best} - W_i^k\right) \\ & + c_2\gamma_2\left(g_{best} - W_i^k\right) \end{aligned} \tag{13}$$

$$W_i^{(k+1)} = W_i^k + V_i^{(k+1)} \tag{14}$$

p_{best} is the optimal position of the particle, g_{best} is the optimal position of population, k is iteration, $c_1$andc_2 are learning factors, ω is inertia weight, $\gamma_1$and γ_2 are the random numbers between 0 and 1.

3.6 Network security situation prediction process based on PSO-time sequence kernel function support vector machine

The network security situation prediction process based on PSO-time sequence kernel function support vector machine is shown in Fig. 2.

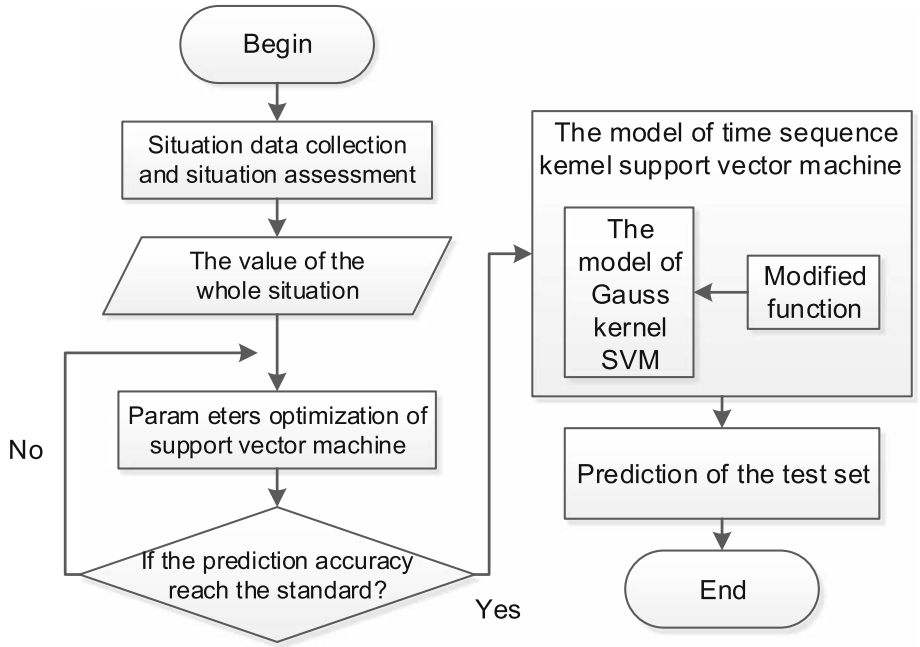

Fig. 2 The network security situation prediction process based on PSO-time sequence kernel function support vector machine

4 Experiment and analysis

4.1 Experimental data set

In order to verify the reasonability of the method in this paper, the related data of a campus network are collected as the experiment data. The topological structure of the campus IoT network is shown in Fig. 3. Experiment raw data are the attack information by Snort, data flow information by Netflow, vulnerability information by Nessus and asset performance information by Sigar. The rich data source provides a reliable guarantee for the simulation experiment.

In this study, we acquired 360 data from March 1, 2015, to May 31 (90 days and 4 times daily samples) from the university as the training data. According to the steps and algorithms of 3.1, we obtained the value of the whole situation of the network. Then, the model of PSO-sequence kernel support vector machine was trained by the obtained values of the network. The 120 data which was from June 1, 2015, to June 30 (30 days and 4 times daily samples) were acquired as the test data.

4.2 Experiment and analysis of the network security situation prediction

For the prediction model of time series kernel support vector machine, the embedding dimension was set as

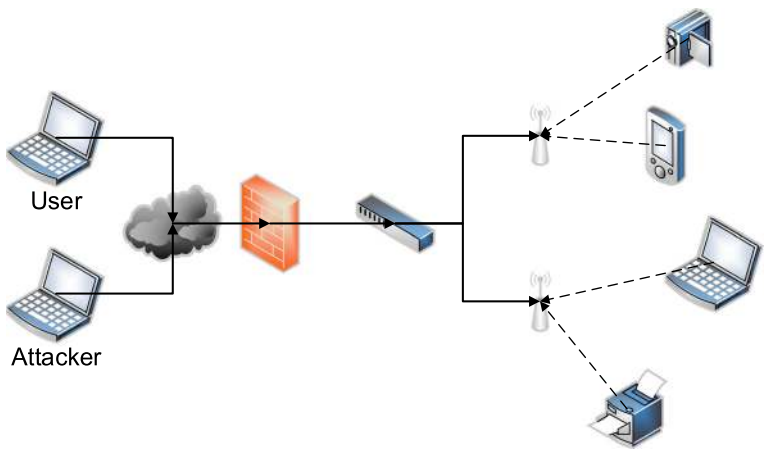

Fig. 3 The topological structure of the campus IoT network

seven by trial and error. That is using the previous week's data to predict the network security situation in the coming day. The prediction model is the time sequence kernel support vector machine optimized by the particle swarm. The parameters of the particle swarm are shown in Table 7.

4.3 The results of network security situation prediction

In order to verify the feasibility and effectiveness of PSO-time series kernel support vector machine, we compared the predictive value of PSO-time series kernel support vector machine with the actual security situation value and the predictive value of PSO-Gaussian kernel support vector machine.

4.3.1 Analysis of experimental results of network security situation prediction in a certain day

The PSO-time series kernel function support vector machine and PSO-Gauss kernel function support vector machine were used to predict the network security situation in a certain day of June. The results were shown in Fig. 4.

The relevant parameters were as follows. c is 100, σ is 15, ε is 0.001, window radius is 30, window weight parameters were ω_{1s} is 1, ω_{1s}^{*} = 0.9.

In order to reflect the prediction results of the two forecasting methods in the same parameter intuitively, the partial relative errors of a certain day in June were shown in Table 8.

4.3.2 Analysis of experimental results of network security situation prediction in a certain week

The PSO-time series kernel function support vector machine and PSO-Gauss kernel function support vector machine were used to predict the network security situation in a certain week of June. The results were shown in Fig. 5.

The relevant parameters were as follows. C is 500, σ is 50, ε is 0.001, window radius were 1 and 3.

Table 7 The setting table of particle swarm parameters

Particle swarm parameters	Default
Population size	25
The initial inertia weight ω_1	0.8
Termination inertia weight ω_2	0.3
Learning factor $c_1 = c_2$	2
The scope of c	(0.1, 5000)
The scope of σ	(0.001, 1)
The scope of ε	(0.001, 10)
Velocity interval of particle	(0, 0.5)

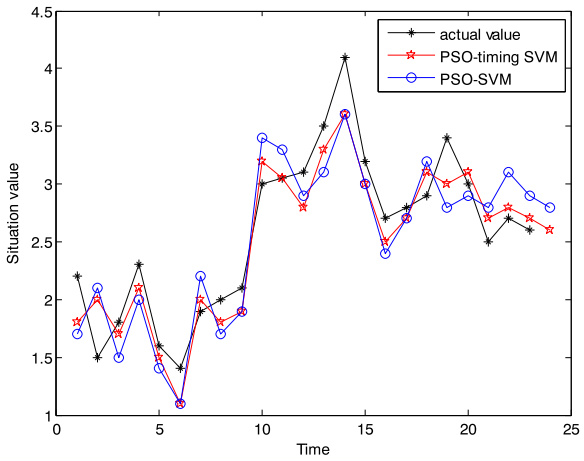

Fig. 4 Situation comparison of a certain day in June

The first layer of the window weight parameters was that ω_{1s} is 0.6 and ω_{1s}^{*} is 0.4.

The second layer window weight parameters were as follows:

$\omega_{2s}$is 0.4 and $\omega_{1s}^{*}$is 0.3.

The relative error of a certain week in June between the actual value of the network situation and the predictive value of two kinds of forecasting methods are shown in Table 9.

The experimental results show that PSO-time series kernel support vector machine is better than the PSO-Gauss kernel support vector machine in network security situation prediction. And during the week, the network security situation value of weekend was higher than normal, so network administrators should strengthen the network protection in time.

From the above results, it is feasible to predict the network security situation based on the PSO-time series kernel function support vector machine. Compared with the PSO-Gauss kernel support vector machine, the PSO-time

Table 8 Partial relative error of a certain day in June

Relative error	PSO-time series kernel SVM	PSO-Gaussian kernel SVM
1	18.18	22.73
3	5.56	16.67
4	8.69	13.04
5	6.25	12.50
8	10.00	15.00
9	9.52	9.52
18	6.91	10.34
19	11.76	17.65
21	8.00	12.00
23	3.85	11.54

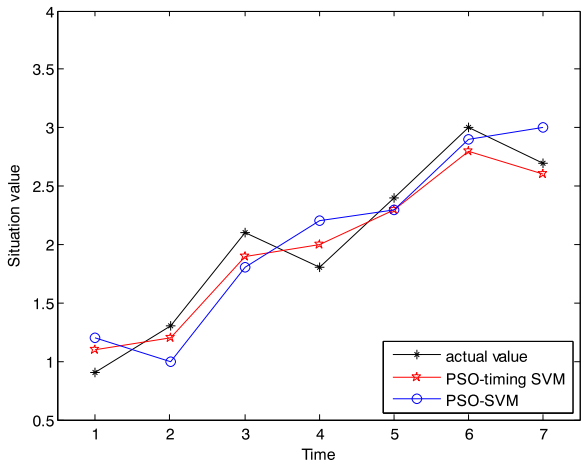

Fig. 5 Situation comparison of a certain week in June

series kernel support vector machine has great advantages in network security situation prediction.

4.4 System time performance analysis.

Network security situational awareness system for predicting equipment log of this article is based on the Hadoop big data processing platform, in order to verify the Hadoop platform to handle large amounts of log time performance, in this article, the experiment will be treated as a traditional single log spent time comparing with Hadoop cluster processing time spent, dealt with different levels of the log data; the time it takes is shown in Table 10.

Table 10 shows that when the log data level is less than 50,000, the single-machine processing capability is better than the processing power of the Hadoop cluster. But as the growth of the log magnitude cluster around the time grows smaller, the rise in single machine processing time spent is almost in a straight line, and the increase in the number of nodes in the cluster processing efficiency is also higher. The efficient operation makes the log quantity of network security device more and more obvious, and the quiet of the single-machine processing mode is more and more prominent. Therefore, the design of this paper is based on the big data platform

Table 9 Relative error of a certain week in June

Relative error	PSO-time series kernel SVM	PSO-Gaussian kernel SVM
1	22.22	33.33
2	7.69	23.08
3	9.52	14.29
4	11.11	22.22
5	4.17	4.17
6	3.67	3.33
7	3.70	11.11

Table 10 Compare the time to log in different modes (unit: millisecond)

Log volume/bar	Single machine processing	Hadoop cluster processing (2 nodes)	Hadoop cluster processing (4 nodes)	Hadoop cluster processing (6 nodes)
10,000	5379	11,132	12,432	10,145
50,000	12,898	15,312	13,652	11,437
100,000	20,114	21,241	19,845	12,657
500,000	43,354	27,663	26,324	16,357
1,000,000	53,372	31,897	29,986	16,689
5,000,000	116,832	45,782	31,347	17,012

to deal with the security log system has strong practical significance.

5 Summarize

There is an in-depth study of the existed network security situation prediction achievement in this paper. For the characteristic of situational factors which are randomness, time-sequence, and complexity, we propose a network security situation prediction method based on PSO-sequence kernel support vector machine. A modification function which is suitable for time series data is constructed to revise the kernel function of traditional support vector machine. Then the sequence kernel support vector machine is obtained and the particle swarm optimization is used to optimize related parameters. By building an experimental environment and using the obtained values of the situation, it is verified that the method in this paper is feasible and effective. Simulation results show that the method in this paper has high accuracy for the prediction of the network security situation, thus it can give network administrators useful help in making timely and effective decisions. In the future development of Internet of Things technology, the network situational awareness prediction method proposed in this paper can be applied to many scenarios, such as the communication field, cloud computing field and smart city construction field. I hope the research results presented in this paper can contribute to the development of Internet of Things network security. In the next step, the focus will be on the situation visualization research of network security.

Acknowledgements

Our work was supported by the General Project of Tianjin Municipal Science and Technology Commission under Grant No.15JCYBJC15600, the Major Project of Tianjin Municipal Science and Technology Commission under Grant No.15ZXDSGX00030, and NSFC: The United Foundation of General Technology and Fundamental Research (No.U1536122). The authors would like to give thanks to all the pioneers in this field and also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the quality of this paper.

Authors' contributions

WY contributed to the design and implementation of the study and writing part of the paper. JZ and CW conducted analysis and simulation experiments and XM supplemented the manuscript. Final draft read and approved by all authors.

Authors' information

Wenjun Yang, School of Computer Science and Engineering, Tianjin University of Technology. He received a Master's Degree from Northeastern University in 2004. His research interests include Internet and information security. Email: yangwj@tjut.edu.cn

Funding

There is no financial support for this study.

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Received: 24 January 2019 Accepted: 26 July 2019
Published online: 28 August 2019

References

1. http://www.cac.gov.cn/2014-02/27/c_133148354.htm
2. Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta. Secure integration of IoT and cloud computing [J]. Future Gen Comp Sy, 2016.
3. Stergiou C, Psannis K E, Gupta B B, et al. Security, privacy & efficiency of sustainable cloud computing for big data & IoT [J]. Sust Comput, 2018.
4. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices [M]. Inderscience Publishers, 2017.
5. Aakanksha Tewari,B.B. Gupta. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework [J]. Future Generation Computer Systems, 2018.
6. Vasileios A. Memos,Kostas E. Psannis,Yutaka Ishibashi,Byung-Gyu Kim,B.B. Gupta. An Efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework [J]. Future Generation Computer Systems,2018,83.
7. X. Zhang, Z. Yang, Y. Liu, et al., Toward efficient mechanisms for mobile crowdsensing [J]. IEEE Trans Veh Technol **66**(2), 1760–1771 (2017)
8. W. Juan, Study on index system in network situation awareness [J]. Comp App lications. **27**(8), 1907–1909 (2007)
9. M.R. Endsley, Design and evaluation for situation awareness enhancement [C]. Proc Human Factors Soc Annu Meet, 97–101 (1988)
10. Tim Bass, Dave Gruber. A glimpse into the future of ID [EB/OL].USENIX .16, 1999
11. L. Gong, W. Yang, D. Man, et al., iPil: improving passive indoor localisation via link-based CSI features [J]. Int J Ad Hoc Ubiq Com **23**(1-2), 36–45 (2016)
12. T. Bass, Intrusion detection systems and multi-sensor data fusion: creating cyberspace situational awareness [J]. Commun ACM **43**(4), 99~105 (2000)
13. Lei Xuan. Prediction of network security situation based on cloud [J]. ICCCT2010, 2010
14. Ma-Yan Y. Prediction Method for Network Security Situation Based on Elman Neural Network [J]. Comput Sci. 2012;39(6):61-60.
15. R. Wei, RBFNN- based prediction of networks security situation [J]. Computer Engineering and Application (2007)
16. Li Fang wei. Network security situation prediction mechanism based on complex network [J]. Computer Application Research, 2014
17. C. Hong, Method of network security situation prediction based on IHS_ LSSVR [J]. Comp Eng Appl **50**(23), 91–94 (2014)
18. C. Xiang, P. Yang, C. Tian, et al., Calibrate without calibrating: an iterative approach in participatory sensing network [J]. IEEE Trans Parall Distr Syst **26**(2), 351–336 (2015)
19. L. Gong, W. Yang, D. Man, et al., WiFi-based real-time calibration-free passive human motion detection [J]. Sensors **15**(12), 32213–32229 (2015)
20. C.T. Lin, C.M. Yeh, S.F. Liang, et al., Support-vector-based fuzzy neural network for pattern classification [J]. IEEE Trans Fuzzy Syst **14**(1), 31–41 (2006)
21. Chun dong Wang, Li Yue. Situation assessment of network security based on T-S fuzzy neural network [J]. J Comput Inf Syst, 2015, 11:16: 5999~6006
22. Z. Yang, C. Wu, Z. Zhou, et al., Mobility increases localizability: a survey on wireless indoor localization using inertial sensors [J]. Acm Comput Surv **47**(3), 1–34 (2015)

Publisher's Note