Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

Application of Network Security Event Correlation Analysis and Situation Evaluation Technology

Yu Qing
Xinyang Vocational and Technical College, Xinyang, Henan, China

Abstract:

Network security situational awareness can integrate all aspects of network security elements. Through correlation analysis, information fusion, situation prediction and other technologies to realize the intelligent analysis and comprehensive decision-making of complex information systems, network security situation awareness can improve the management efficiency and effect of complex networks. In order to solve the problem of parameter optimization of existing situation assessment methods, the parameters of SVM model are optimized based on Particle Swarm Optimization PSO algorithm. This paper presents a network security situation assessment method based on PSO and SVM. Using this algorithm can get a better balance between time-consuming and improving accuracy. At the same time, the index weight is determined according to grey correlation analysis, and the training samples are input to support vector machine for training. In this paper, the improved particle swarm optimization algorithm is used to optimize the parameters of support vector machine to improve the effect of situation assessment. Simulation test results show that the evaluation method improves the effectiveness and accuracy of situation assessment.

Keywords: *Network Security, Situation Awareness, Association Analysis, Improved Particle Swarm Optimization.*

I. INTRODUCTION

Looking at the international and domestic situation, cyberspace is full of ups and downs and smoke of gunpowder. It is evolving into the main means of big country game and a new battlefield of attack and defense confrontation [1-2]. On the one hand, emerging technologies are constantly applied to the network field. Cloud computing and the Internet of things are penetrating into various network applications at an unprecedented speed, bringing a new revolution to the network society [3]. On the other hand, the application of new technology also

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

makes the structure of network infrastructure and network information system more complex, which brings great difficulties to network security supervision. In order to effectively deal with network threats, various research institutions and functional departments have strengthened protection, built a single point defense system represented by firewall, IDS, VPN and anti-virus software, and carried out response defense against all kinds of network threats [4-7].

Network threat situational awareness can fuse a large number of multi-source heterogeneous threat information obtained, and graphically display the fusion results, so as to provide decision-making reference for administrators to deal with network threats [8]. Because the data source of network threat situation awareness technology covers all kinds of network security equipment, the perception results are more objective and accurate. At the same time, it has good real-time performance, so that the network administrator can quickly judge the current network threat situation, formulate Countermeasures in time, and reduce and prevent the damage caused by network threat. Therefore, the research on network threat situation awareness is of great significance and practical value.

II. NETWORK SECURITY SITUATION AWARENESS MODEL

1.Major threats to network security

Due to the openness of network and information system, information is vulnerable to security threats such as theft, tampering and destruction in the whole life cycle of generation, storage, processing and transmission. Security threat refers to the event or element that destroys the three elements of network security. At present, the main security threats faced by computer networks are [9-10]:

(1) Fake. Counterfeiting refers to the act of forging the certificate of the legal person, counterfeiting the identity of the legal person, and accessing or destroying unauthorized information. Counterfeiting is generally carried out in the form of stealing keys and replaying data packets, which poses a great threat to the information system. Such attacks mainly affect the confidentiality and integrity of the three elements of security. (2) Denial of service. Denial of service refers to the attack on the system, resulting in the interruption of the normal external service of the information system. The interruption of service may be temporary or permanent. Such attacks mainly affect the availability of the three elements of security. (3) Eavesdropping. Eavesdropping refers to monitoring signals by means of grounding, etc. Attackers use the possible security vulnerabilities in the generation, processing, transmission and storage of computer information to monitor and intercept the information. Such attacks mainly affect the confidentiality of the three elements of security. (4) Back door. The back door is a way to enter the system. Backdoors are generally preset by developers and are mainly used for remote monitoring and control of the target system and potential malicious damage to the target system. In a few cases, the back door is formed due to the negligence of developers in the process of

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

system design.

2.Network security situation awareness index system

For the network information system, its security mainly depends on whether the key hosts and core services in the system can run safely and healthily. Network attackers mainly rely on the vulnerabilities of network hosts or services to penetrate into the target system for information theft, data destruction and other attacks. According to the code for information security risk assessment, the value of assets, the possibility of threat, the severity of threat and the vulnerability of assets are the key factors affecting the network security status. Therefore, these elements are also considered as important elements of network security situational awareness, forming the primary indicators of network security situational awareness.

Establish the network security situational awareness index system as shown in Table 1.

TABLE I. Network security situation awareness index system

PRIMARY INDEX	SECONDARY INDEX
ASSET IMPORTANCE	Average survival time of key equipment
	Flow change rate
	Total data flow
	Number of surviving critical equipment
	Mean time between failures of key equipment
VULNERABILITY INDEX	Number and level of network vulnerabilities
	Number and severity of system vulnerabilities
	Number of safety devices
	Number and level of critical equipment vulnerabilities
	Memory capacity, frequency and bandwidth utilization
	CPU dominant frequency and number of cores
	Installation of security software
	Total number of open ports of each key equipment
THREAT INDEX	Type of attack
	Number of attacks
	Severity of attack
	Network bandwidth occupancy

III. NETWORK SECURITY SITUATION ASSESSMENT BASED ON PSO AND SVM

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

1.SVM theory

Support vector machines (SVM) is a machine learning method based on statistical learning theory and VC dimension theory. Using the principle of structural risk minimization, it can not only overcome the problems of "dimension disaster" and "over learning", but also has advantages in solving nonlinear, small sample and high-dimensional pattern recognition. In addition, it has a solid theoretical foundation and simple data model. It has been widely used in the fields of pattern recognition, regression analysis, function estimation, time series prediction and so on.

VC dimension is the core of statistical learning theory. It is defined as: for an indicator function set, if there are h samples that can be separated by the functions in the function set according to all possible 2H forms, it is said that the function set can disperse h samples, and the VC dimension of the function set is the maximum number of samples it can disperse H. The size of VC dimension indicates the learning ability of the method. The larger the dimension, the stronger the learning ability.

Statistical learning theory is a method to study the correlation between actual risk (immediate expected risk) and empirical risk (i.e. training error) in function concentration, which is also called generalized bound. For the study of this problem, it is now generally agreed that for all functions in the indicator function set, the probability between empirical risk and actual risk is at least $1-\eta$ The following relationships are satisfied:

$$R(w) \le R_{emp}(w) + \sqrt{\frac{h\left(In\frac{2l}{h}+1\right)-In\frac{\eta}{4}}{l}} \quad (1)$$

Where h is the VC dimension of the function set; L is the number of samples.

From the above conclusions, theoretically speaking, the actual risk of learning machine can be divided into two parts: one is empirical risk (training error); The second is the confidence range. Among them, the relationship among the actual risk, the VC of the learning machine and the number of training samples can be expressed by the following formula:

$$R(w) \le R_{emp}(w) + \Phi(h/n) \quad (2)$$

According to the above formula, under the condition of limited training samples, the confidence range has a positive correlation with the VC dimension of the learning machine. The VC dimension increases with the increase of the confidence range, which will also lead to the increase of the difference between empirical risk and real risk. At the same time, this is the reason for the phenomenon of over learning in the learning machine. In the process of machine learning, if we want to have good generalization for future samples and make the empirical risk and actual risk small, we should try to control the VC dimension to reduce the confidence range.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

2.Network security situation assessment based on SVM

The quantitative index is mainly expressed by the maximum membership degree. The common membership degree solving methods are as follows:

(1) fuzzy statistical method. The fuzzy statistical method first judges whether the determined element AI in the universe belongs to a changeable fuzzy set a, then continuously modifies the boundary of a and re judges AI, and calculates the membership of AI to a by counting the number of occurrences of element AI in fuzzy set a.

(2) Expert experience method. The expert experience method is to determine the corresponding processing formula and corresponding weight coefficient for each fuzzy information according to the expert's experience knowledge. When an initial value is determined, it is improved and modified through repeated learning and practice.

(3) Binary comparison ranking method. This method is the most commonly used method at present. By comparing several different things, it determines the sequence of transaction characteristics, and obtains the membership function of things under the corresponding characteristics. Different ranking methods can be adopted according to different comparison measures.

According to the network security situational awareness index system, the network security evaluation standards are finally obtained, as shown in Table 2.

TABLE II. Quantitative standard for first level indicators of network situation security assessment

Evaluating indicator	Vl	L	M	H	Vh
ASSET IDENTIFICATION	0	2	4	6	8
VULNERABILITY INDEX	0	1	2	3	4
THREAT INDEX	3	2.5	2.0	0.5	1.0

According to the above-mentioned quantitative standards and methods for the first level indicators of network situation security assessment, the second level indicators are quantified. For example, the quantitative indicators of threat index are shown in Table 3 below.

TABLE III. Quantitative criteria for secondary indicators of network situation security assessment

Evaluating indicator	Vl	L	M	H	Vh
TYPE OF ATTACK	0	2	4	6	8
NUMBER OF ATTACKS	0	1	2	3	4

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

SEVERITY OF ATTACK	4	3	2	1	0
NETWORK BANDWIDTH OCCUPANCY	0	1	2	3	4

IV. NETWORK SITUATION PREDICTION METHOD BASED ON IMPROVED ELMAN NEURAL NETWORK

Artificial neural network is a nonlinear and adaptive intelligent information processing system composed of a large number of nodes. Artificial neural network is based on imitating the working principle of human neural network and simulating the way of brain storing and processing information to deal with complex problems. Each node is called neuron, which represents a specific output function, also known as excitation function. There is a weighted connection between the two neural networks, which represents the memory of the neural network. Excitation function and connection weight are the key of neural network. Different excitation function and connection weight form different neural networks.

There are two forms of neural network learning: guided learning and non guided learning. Guided learning is also called supervised learning. The training samples of guided learning are input-output pairs (pi, di), I = 1, 2,... n, where pi is the sample input (usually) and di is the corresponding sample output, also known as teacher signal. By adjusting the free parameters of each neuron, the network can produce the desired behavior. Unsupervised learning is also called unsupervised learning or self-organizing learning. Guided learning does not provide teacher signals, but only stipulates learning methods or some rules. The specific learning content varies with the environment of the system, and the system can automatically find the characteristics and laws of the environment.

For guided learning, assuming that the expected output corresponding to input x is d and the weight is $w(t) =(w_1,w_2,...,w_n,\theta)^T$, the content of neuron learning algorithm is to determine the weight adjustment amount $\triangle w(t)$ of neurons and obtain the weight adjustment formula:

$$w(t+1) = w(t) + \eta \Delta w(t) \quad (3)$$

Among them, η Called the learning rate, the value of $\triangle w(t)$ is generally related to x, d, w.

The purpose of network security situation prediction is to obtain the future development state of the network. The future network state is related to the historical state and the current state, and its development process has a certain trend. Therefore, trend feature is an important factor that should be considered in situation prediction model. Therefore, this paper introduces the trend correction factor into the situation prediction model to guide and correct the trend prediction direction. Its core idea is to adjust the trend correction factor based on the trend change direction of the predicted value and the actual value. When the two change directions

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

are the same, the trend correction factor selects parameter h; when the two change directions are different, the trend correction factor selects parameter g. The formulas of h and g are shown in (4).

$$f_{DP}(t)=\begin{cases} g & if\ \left(y_d(t)-y_d(t-1)\right)\left(y(t)-y(t-1)\right)\le 0 \\ h & otherwise \end{cases} \quad (4)$$

Where, t represents the number of iterations, f_{DP} (t) represents the correction factor of t, h represents the smaller correction factor, and g represents the larger correction factor. In order to make the prediction result more accurate and ideal, this paper adds a correction factor to the Elman neural network, and proposes a double feedback Elman neural network based on double regulation factors. The objective function is determined by formula (5).

$$E(k)=\frac{1}{2}\left(y_d(k)-y(k)\right)^T\left(y_d(k)-y(k)\right) \quad (5)$$

The error function is determined by formula (6).

$$E_{DP}(k)=\sum_{t=1}^{k} f_{DP}(t)E(t) \quad (6)$$

V. CONCLUSION

With the wide application of new technologies such as Internet of things and cloud computing, the network structure is becoming more and more complex, and the difficulty of network security management is increasing. How to solve the security management of complex networks through intelligent means has become a problem to be solved. Network security situational awareness can intelligently analyze and make comprehensive decisions on complex information systems, and improve the management efficiency and effect of complex networks. Therefore, network security situational awareness has become one of the research hotspots in the field of information security. This paper has done some research on network security awareness model, situation assessment method and situation prediction method, but the work is not perfect and needs further research in the future work.

REFERENCES

1. Jiang Wei, Fang Binxing, Tian Zhihong. Network Security Evaluation and Optimal Active Defense Based on Attack Defense Game Model. Acta Computer Sinica, 2009, 32 (004): 817-827
2. Miao Yongqing. Stochastic Model Method and Evaluation Technology of Network Security. China Science and Technology Investment, 2017, 4: 314

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.207-214
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

3. Yi Hua Zhou, Wei Min Shi, Wei Ma. Research on Computer Network Security Teaching Mode for Postgraduates Under the Background of New Engineering. Innovation and Practice of Teaching Methods, 2020, 3 (14): 169
4. Bao Xiuguo, Hu Mingzeng, Zhang Hongli. Two Quantitative Analysis Methods for Survivability of Network Security Management Systems. Acta Communication Sinica, 2004, 25 (9): 34-41
5. Yang Yi, Bian Yuan, Zhang Tianqiao. Network Security Situation Awareness Based on Machine Learning. Computer Science and Application, 2020, 10 (12): 8
6. Li Zhiyong. Hierarchical Network Security Threat Situation Quantitative Assessment Method. Communication World, 2016, 23: 70-70
7. Hu Wenji, Xu Mingwei. Analysis of Secure Routing Protocols for Wireless Sensor Networks. Journal of Beijing University of Posts and Telecommunications, 2006, 29 (s1): 107-111
8. Wei Yonglian, Yi Feng, Feng Dengguo, Yong W, Yifeng L. Network Security Situation Assessment Model Based on Information Fusion. Computer Research and Development, 2009, 46 (3): 353-362
9. Xu Guoguang, Li Tao, Wang Yifeng. A Network Security Real-time Risk Detection Method Based on Artificial Immune. Computer Engineering, 2005,31 (12): 945-949
10. Li Weiming, Lei Jie, Dong Jing. an Optimized Real-time Network Security Risk Quantification Method. Acta Computa Sinica, 2009 (04): 793-804