Network Security Classification Assessment Based on Fuzzy Mathematics

Jiaqi Li [1,3, a *], Ning You [1,3,b], Jianyi Liu[1,3,c] and Ru Zhang[1,2,3,d]

[1] National Engineering Laboratory for Disaster Backup and Recovery

[2]Key Laboratory of Trustworthy Distributed Computing and Service

[3] Beijing University of Posts and Telecommunication, Beijing, China

[a] shijinqi@bupt.edu.cn, [b] youning1223@163.com, [c] liujy@bupt.edu.cn, [d]zhangru@bupt.edu.cn

Keywords: safety classification; push-pull combination; dynamic assessment; fuzzy mathematics.

Abstract. Because of the complexity and uncertainty of network security, the static and single direction of network security protection has been unable to adapt to the changing network environment. Through scientific results of other researchers, we proposed a push-pull combination and multi index of fuzzy comprehensive evaluation algorithm of network security classification based on the fuzzy mathematics thought. And starting from the point of view of classification, extracted the parameters in the network equipment, and then established a grade evaluation model. Finally we verified the feasibility and practicability of this model by the experiment.

Introduction

With the rapid development of network technology, and human dependence on the growing network, network security incidents happened constantly, so that the security threat of computer network is more and more serious. How to perceive protection requirements in real-time and make protection strategies becomes more important. Rationality and feasibility of system protection strategy largely depends on the accuracy of the preliminary needs analysis process. The current means of ensuring network security almost use static single demand access mechanism is difficult to meet the security requirements of the new situation. Aiming at the acquisition and defense technology dynamic network security situation has become a new hot research in the field of network security.

The network security assessment methods before has gradually evaluated from the network topology graph to attack topology, SSARE tools, multi-source data fusion method, and the current asynchronous data stream. And after the evaluation method of hierarchical network situation, computer security risk assessment methods based on elevation of privilege model are also presented [1].

At present, although the network security demand evaluation method has a certain amount of research results, we are still in the exploration stage, and there are still a lot of difficulties to overcome. The purpose of this study is mainly from the point of view of data integration and demand classification, improving the traditional mathematical algorithm requirement, and using the classification evaluation to obtain the final demand for network security level, giving the most intuitive network security status to user, and eventually send the network security demand through grade eight safety aspects to the strategy, then ultimately make the whole network protection decision, effectively protect the network security.

Basic principles of network security classification model

Logic of Model structure. Due to the current popular network security policy is basically a unilateral way: the push type strategy issued. That is, the protection system provides a static protection to the network according to the established level of protection. However, the protection strategy of this push-type can't adapt to the changeable network environment. Therefore, this paper proposes a dual direction of network security model. That is, the model uses the push-pull technology, timely and accurately access to different equipment, grading and different protection demand of task scenarios, supporting the whole network protection ability and network communication relationship adjustment.

The main workflow of the model is as flows: First, the model obtains status information by the security analysis. And then assesses classification of information through the network security model. Finally generates strategy the corresponding grades and issued by the strategy library.

Thought of Fuzzy Mathematics. Based on the study of literature and research status, we proposed the method according to the theory of fuzzy mathematics to solve network security rating service. The research of Fuzzy mathematics object is the uncertainty, and the network security attribute also has the characteristics of uncertainty and ambiguity. Using the weighted average method to calculate the integrated network security level is simple, and the operation rate is relatively high. The network security grade service can also be thought of as a process of inference that is evaluating different source to the information, and issuing the corresponding policy according to the evaluation results. And fuzzy mathematics is a better solution for logic reasoning [2-3].

The flow diagram of the method in this algorithm shown in Fig. 1:

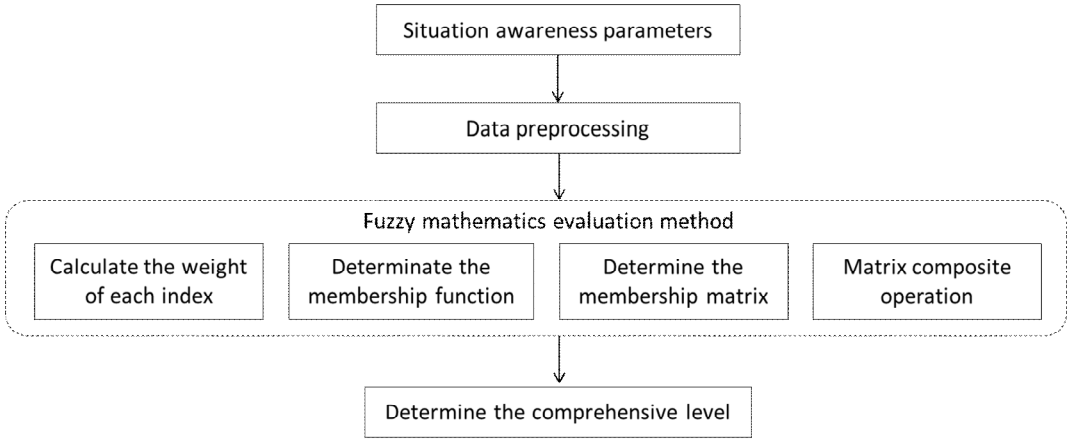

Fig 1. process of fuzzy mathematics algorithm

As can be seen, this method first obtained the weight information of each index from the weight information table, and converted the information into digital matrix of the system required in the data preprocessing module. With the data base we can calculate the level of comprehensive security according to the fuzzy evaluation algorithm aimed to these two aspects.

Constructing dynamic network security classification model

Establish the classification evaluation index system of network security. Because of the complexity of network elements, we need to evaluate the network security situation from different levels and directions. According to the research on the elements of the network environment in the literature [4], we summarize the network security assessment for eight elements: (1) Data confidentiality; (2) Data integrity; (3) Identity authentication; (4) Traffic filtering; (5) Access control; (6) Availability service; (7) Non repudiation; (8) Port security (scan times); Based on these eight indexes, we divided each index into eight levels. The lower level shows the better situation and the higher shows the worse. Membership is the degree that the index belongs to which level in a moment, the greater membership numerical value means the larger possibility belonging to this level.

Based on the quantitative classification theory in the Literature [5], the standard values for each level of eight indexes are shown in Table 1.

TABLE I. STANDARD VALUE FOR THE ELEMENTS CLASSIFICATION

Elements \ Level	L1	L2	L3	L4	L5	L6	L7	L8
Data confidentiality (bit)	≤ 32	≤ 64	≤ 128	—	≤ 256	≤ 512	≤ 1024	> 1024
Data integrity (%)	≤ 20	≤ 45	≤ 50	≤ 75	≤ 80	—	≤ 95	> 95
Identity authentication(s)	≥ 20	≥ 15	—	—	≥ 10	—	≥ 5	< 5
Traffic filtering(MB/S)	≤ 10	≤ 15	≤ 20	≤ 25	≤ 30	—	≤ 35	> 35
Access control (%)	≤ 10	≤ 20	≤ 40	≤ 50	—	≤ 70	≤ 90	> 90
Availability service(times/s)	≤ 5	≤ 10	≤ 20	≤ 30	—	—	≤ 45	> 45
Non repudiation (%)	≤ 20	≤ 35	≤ 40	—	≤ 60	≤ 65	≤ 70	> 70
Port security scan(times/s)	≤ 1	≤ 3	≤ 5	≤ 7	≤ 10	≤ 15	≤ 18	> 18

Steps.

The first step: determine the membership. The method used by the system to determining the membership is mainly based on the distance between the actual data and the standard data. Specific expression is:

$$M_i = \begin{cases} 1 & C_i \leq E_i \\ \frac{E_{i+1} - Ci}{E_{i+1} - E_i} & E_i < C_i < E_{i+1} \\ 0 & C_i \geq E_{i+1} \end{cases} \quad (1)$$

Where the M_i represents the membership value of the i^{th} level, and the E_i represents the standard value of the i^{th} level, and C_i represents the actual value of the i^{th} level.

The second step: Structure the fuzzy matrix according to the membership. We construct the fuzzy matrix R according to the classification of each index:

$$R = \begin{pmatrix} m_{1,1} & \cdots & m_{1,8} \\ \vdots & \ddots & \vdots \\ m_{8,1} & \cdots & m_{8,8} \end{pmatrix} \quad (2)$$

Among them: m_{ij} means the membership of $i^{th}(1 \leq i \leq 8)$ index belongs to class $j(1 \leq j \leq 8)$ of network security. And when the level corresponding to an index does not exist, the elements corresponding to this index and the level of the matrix are 0.

The third step: determine the weight of each index. The weight of each index should be determined by situation analysis [6].Situation analysis is that in a certain space and time condition, in the dynamic and complex environment, apperceiving the continuous change of the network environment through the situation awareness tools, and analyzing the security trends in time and spatial domains. Comprehensive judge the security requirements should priority processed, and make the correct decision. According to the formula (1), the weight of each index is obtained:

$$w_i = \frac{p_i}{\sum_{j=1}^{8} p_j} \times 100\% \quad (3)$$

Where the p_i represents the i^{th} value in the whole network.

Normalized the weight of the results, making the weight of the sum equals 1, and named this normalized weight matrix $W = (w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8)$.

The fourth step: Assess the level, and make a decision. We have already obtained the current level of each index and the weight of each index in the network environment. Now we need to use matrix multiplication to combine these two factors, to determine the grade of each index:

$$S' = W \times R = (w_1, w_2, \cdots, w_8) \times \begin{pmatrix} m_{1,1} & \cdots & m_{1,8} \\ \vdots & \ddots & \vdots \\ m_{8,1} & \cdots & m_{8,8} \end{pmatrix} \quad (4)$$

Normalize S' to obtain the final classification vector S:

$$S = (s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8) \quad (5)$$

Determine the comprehensive level according to the results of the final vector, the corresponding subscripts of the maximum value in the vector is the integrated rank number.

Experimental illustration

Now, we will analyze the security environment variables of the network by the situation awareness module [7], and finally get the eight element values as shown in Table 2.

TABLE II. NETWORK ENVIRONMENT INDEX VALUE

Data confidentiality (bit)	Data integrity (%)	Identity authentication (s)	Traffic filtering (MB/S)	Access control (%)	Availability service (times/s)	Non repudiation (%)	Port security scan (times/s)
120	40	8.6	24	93	25	36.4	8

Step 1,2: We can construct membership matrix:

$$R = \begin{pmatrix} 0 & 0.875 & 0.125 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.28 & 0 & 0.72 & 0 \\ 0 & 0 & 0.8 & 0.2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \\ 0.333 & 0.667 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.467 & 0.533 & 0 \end{pmatrix}$$

As the matrix shows, the port securities scan needs the 8th level protected.

Step 3: We can construct weight vector:

$$W = (0.336, 0.122, 0.026, 0.073, 0.284, 0.076, 0.051, 0.025)$$

Step 4: We can calculate the final grade vector:

$$S = R \times W \xrightarrow{Normalization} (0.2875, 0.1417, 0.0132, 0.0763, 0.2226, 0.0598, 0.1019, 0.0970)$$

Obviously the maximum value of the vector is 0.2875, and the current level of network security is the 1st level. Does the 1st level can protect this network? Because the port security needs the highest protection as the matrix R showed, so we will use port-attack software, the DDOS attack software to prove it. The different of static protection and dynamic protection is shown as Fig. 3.

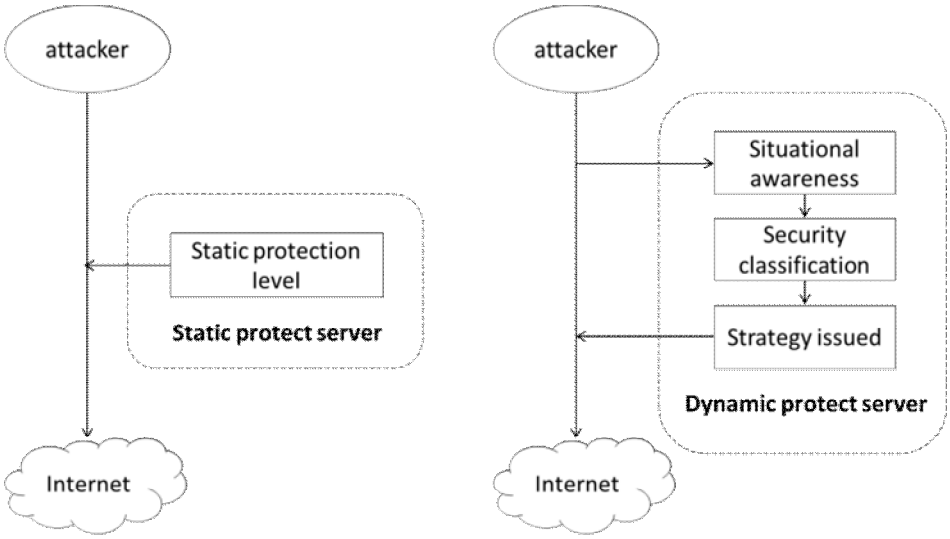

Fig 2. The difference of static and dynamic protection mechanism

First we use DDOS attack software to attack this network with 8th level static protection. Found that the attacking is failed.
Then we reduce the static protection level to 7th, and attack the network. Found that the attacking is success.
Now we use the 1st level dynamic protection, and try to attack it. Found that the attacking is failed. It proves that although the current network security level is lower, the network still can resist the highest level, the port attack, through resource adjustment. That's to say, the 1st level dynamic protection can provide the protect server that the 8th level static protection can provide while the 7th can't.
It can be seen that the protection strategy's efficiency of the dynamic classification protection model is higher than the static protection model to resist the possible attack. So the protect costs of the entire network can be reduced, and the protection efficiency can be improved. So when the network environment is constantly changing, the system only needs to perceive the value of the eight elements from Situational. Awareness of network security, then the system can automatically modify the protection level, so that dynamic changes to adapt to the network environment safety.

Conclusion

Dynamic protection and requirements elicitation of network security have made certain research, but is still in the exploration. The goal of this article is that from a classification point of view we can extract index parameter of the equipment and establish a reasonable way to change level of network. Then we can improve the way of classification and establish a efficient operating environment.
Experimental results show that the method is feasible and effective, and it can dynamically analyses the safety states of the network and timely delivered information to strategy management. Thus, the purpose of real-time and fast protection of the whole network security is achieved.

Acknowledgment

This work was supported by the Beijing Higher Education Young Elite Teacher Project (YETP0448) and NSF of China (U1433105).

References

[1] Liu Zhonghua, "Research on service oriented network situational assessment method", Harbin Engineering University, TP393.02 TP311.1, April 2013

[2] Chuang Liu ; Lam, Xian Zhang ; Hongyi Li "Relaxed stability conditions based on Taylor series membership functions for polynomial fuzzy-model-based control systems" Fuzzy Systems

(FUZZ-IEEE), 2014 IEEE International Conference on, 6-11 July 2014, doi: 10.1109/FUZZ-IEEE.2014.6891557

[3] Tang, Chenghua ;Yu, Shunzheng, A dynamic and self-adaptive network security policy realization mechanism, Network and Parallel Computing, 2008. NPC 2008. IFIP International Conference on. 18-21 Oct. 2008. Doi: 10.1109/NPC.2008.41

[4] Liu P, Zang W. "Incentive-based modeling and inference of attacker intent, objectives, and strategies," Proceedings of the 10th ACM Computer and Communication Security Conference (CCS'03). Washington, DC,pp. 179-189, 2003.

[5] Yao Shuping, Gu Yingyan, "Network security situation quantitative evaluation based on the classification of attacks in attack-defense confrontation environment", Control and Decision Conference, 2009. CCDC '09. Chinese, 17-19 June 2009, doi: 10.1109/ CCDC. 2009. 5195279

[6] Liu Mixia, Zhang Qiuyu, Zhao Hong, Yu Dongmei. "Network Security Situation Assessment Based on Data Fusion". Knowledge Discovery and Data Mining, 2008. WKDD 2008. First International Workshop on. 23-24 Jan. 2008. Doi: 10.1109/WKDD.2008.35.

[7] Xiumei Wei, Xuesong Jiang, "Comprehensive analysis of network security situational awareness methods and models", Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on. 23-24 Dec. 2013. Doi: 10.1109/IMSNA.2013.6743245