Network Security Situation Assessment Based on FAHP

JI Feng-zhu[1 a], ZHOU Yun-ting[1], TANG Qi-jie[1], HU Fang-xiang[1] and MA Shao-feng[1]

[1] Xichang Satellite Launch Center, XiChang, SiChuan 615000, China

[a]381361706@qq.com

Keywords: FAHP; Information Security; Risk Assessment

Abstract. In order to solve the problem of methodology subjectivity, long modeling time and low classification accuracy in the information security risk assessment, a network security situation assessment model based on FAHP has been proposed in this paper. Via building a network security index system, using the analytic hierarchy process to calculate the weight of each evaluation index, taking fuzzy method to establish network security situation to determine the consistency of the moment, a comprehensive assessment of network security situation has been achieved. Examples show that FAHP not only improves the accuracy of network security situation assessment, but also is more objective at the same time.

Introduction

Network security assessment is the basis for the development and adjustment of network security policy. In order to develop an effective network security strategy, assessing the network security situation accurately is necessity. According to the lack of traditional network security assessment methods [1-4], a situation assessment algorithm based on fuzzy analytic hierarchy process network has been proposed. The algorithm can effectively help network administrators understand the current security status of the network system, and can clearly grasp the trends of network security status.

Principle of Network Security Situation Assessment

The principle of Network security situation assessment is based on the frequency, quantity, and different levels of the threat of network security incidents, converging network security information into a network can show the value of the health situation by weighting. Then assess network security in the future trends based on historical and current value of network security situation. And set up its influence factors as $\{x_i, i=1,2,\cdots,m\}$, network security level as $\{y_i, i=1,2,\cdots,k\}$. So the mathematical model of network security situation assessment can be presented as:

$$y_i = f(x_{i1}, x_{i2}, \cdots, x_{im}) \tag{1}$$

Since comprehensive network security situation is the result of many factors, randomness and uncertainty. Fuzzy analytic hierarchy process (FAHP) is proposed based on the Analytic Hierarchy Process (AHP). FAHP is an integration of theory and analytic hierarchy process advantages of fuzzy, fully integrated with fuzzy comprehensive evaluation method. Using fuzzy consistent judgment matrix, while building the assessment index system weight can make the random and uncertain system has a strong learning ability, and improve the accuracy of network security situation assessment.

Network Security Situation Assessment Model

Establish evaluation index system. According to the Requirements for network security situation assessment, analysis associated with each evaluation index, affiliation, and builds the structure model

of network security situation assessment. Decompose evaluation system; establish a system of evaluation index system by using the idea of decomposition. The basic level of FAHP is the same as AHP, which can be divided into the target layer, criterion layer and index layer. A network system is chosen for the study in this paper, using AHP to evaluate their network security posture [5-8]. Establish the network security situation evaluation system based FAHP. Target layer can be evaluated for risk score network system, guidelines layer includes four factors, value alarm class, vulnerability class, measure class and consequence class, index layer is constructed index value of 13 points, respectively, as follows: the number of alerts, confidence, severity, and correlation and etc. And the connections can be shown as Fig.1.

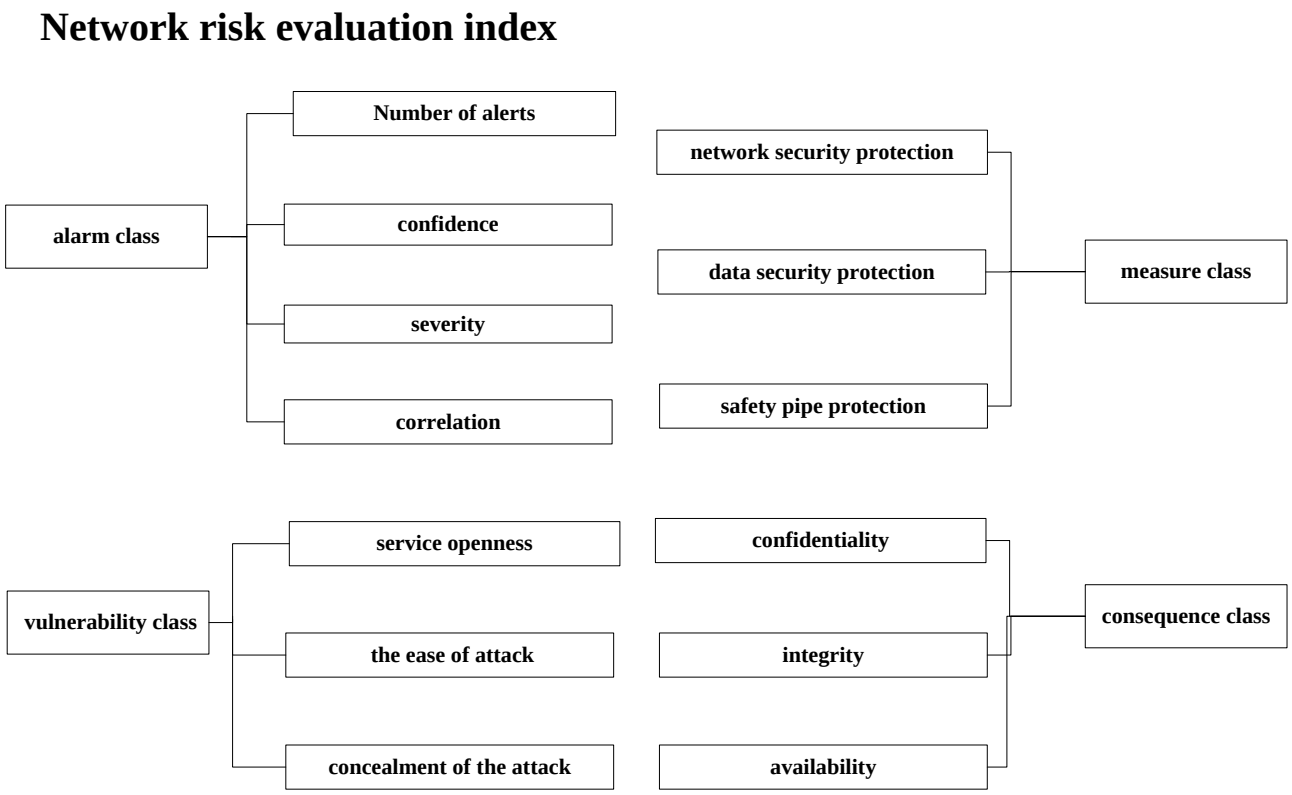

Fig.1 Network security situation assessment index system

Construct the fuzzy comprehensive evaluation model. Judge the elements of first layer as a criterion for comparing elements of the second level, and determine their relative importance according to the assessment scale. Establish judgment matrix: $C=(c_{ij})_{n\times n}$(c_{ij} indicates the degree of importance of factor i and factor j relative to the target value), when $i=j$, $c_{ij}=1$. The relative weight of each weight factor W_i may be expressed as:

$$W_i=\sum_{i=1}^{n}c_{ij}\Big/\sum_{j=1}^{n}\sum_{i=1}^{n}c_{ij} \tag{2}$$

Establish the fuzzy judgment matrix. According to the status of the network security situation, assess the level selects several sets consisting of an assessment, which means network security situation is about to be represented by a set, U={safe, in general, more dangerous, dangerous}. Rate each contestant by Delphi Method, score range in the interval (0, 1). The sum and contestant index is "*1*". Construct the fuzzy set and determine the membership according to the characteristics of the network security situation assessment indicators.

$A_1, A_2, \cdots, A_n$ are several clear collections, seeking the union of these collections . And set the domain as E, which can be expressed as:

$$E = \bigcup_{i=1}^{n} A_i \tag{3}$$

Choose any $k(k = 1, 2, \cdots, n)$ sets from $A_1, A_2, \cdots, A_n$. And seek their intersection. There are C_n^k such intersections those are:

$$A_{i_1 i_2 \cdots i_n}^{(m)} = A_{i1} \bigcap A_{i2} \bigcap \cdots \bigcap A_{ik} \; ; m = 1, 2, \cdots, C_n^k \tag{4}$$

Among them, $i_1, i_2, \cdots, i_k$ are any several k counts from $1, 2, \cdots, n$, so the union set of the intersection of C_n^k can be shown as follows：

$$B_k = \bigcup_{m=1}^{N} A_{i_1 i_2 \cdots i_n}^{(m)}, N = C_n^k \tag{5}$$

Based on the decomposition theorem, for each set B_k , multiplicity k / n With the collection of B_k to get the fuzzy set $B_k k / n(k = 1, 2, \cdots, \mathrm{n})$, Its membership function is as follows:

$$u_{(k/n)B_k}(e) = \begin{cases} \dfrac{k}{n}, e \in B_k \\ 0, e \notin B_k \end{cases} \tag{6}$$

On these n fuzzy sets, do set operation, a fuzzy set $\tilde{A}$ can be constructed:

$$\tilde{A} = \bigcup_{k=1}^{n} \frac{k}{n} B_k \tag{7}$$

A collection of membership function of set $\tilde{A}$ is membership function of the maximum function of n in (4), which can be saved as $u_A(e)$, and shown as follows:

$$u_A(e) = \max_{1 \le k \le n} \left\{ u_{\frac{k}{n} B_k}(e) \right\}, \forall e \in E \tag{8}$$

Establish the fuzzy relationship matrix of U to V. Construct the fuzzy mapping $f : U \to F(V)$, $u_i \to f(u_i) = (r_{i1}, r_{i2}, \cdots, r_{im}) \in F(V)$. $F(V)$ is on the fuzzy set of V , mapping f says factors to evaluate the support of concentrated all the comments. Set $R_i = \{r_{i1}, r_{i2}, \cdots, r_{im}\}$, $i = 1, 2, \cdots, n$. So get U to V the fuzzy relation matrix R .

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{i1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{i1} & r_{i2} & \cdots & r_{im} \end{bmatrix} \tag{9}$$

Among them, r_{ij} is an expert on the safety index level of j risk score, $0 \le i \le I$; $0 \le j \le J$.

Using the formula establishes the network security situation assessment factors evaluation matrix:

$$B_i = W_{ij} \square R_i \ (0 \le i \le I) \tag{10}$$

Then the normalized processing factors evaluation indexes, network security situation assessment matrix: $B = (B_1^T, B_2^T, \cdots, B_I^T)^{\mathrm{T}}$, using the matrix W based on the weight vector and fuzzy matrix B for matrix multiplication, get the fuzzy subset S :

$$S = W \cdot B \tag{11}$$

Since the available network security situation assessment can be valued from S , in order to provide the basis for reasonably network security management decisions, the networks safe level can be determined.

Value the network security situation assessment. And the network security situation assessment values can be expressed as follows from parts above:

$$f = S \cdot X^T \tag{12}$$

To assess the concentration of the corresponding score vector, score the results are shown in table 1. Comprehensive the knowable above, based on the fuzzy analytic hierarchy process (AHP), the network security situation assessment process as table is shown in figure 2.

Table 1 Score of network security situation assessment

scoreY	Risk level	Evaluation score
95	Safe	>90
80	Less safer	80～90
65	In general	60～79
50	Little dangerous	40～59
35	Dangerous	<40

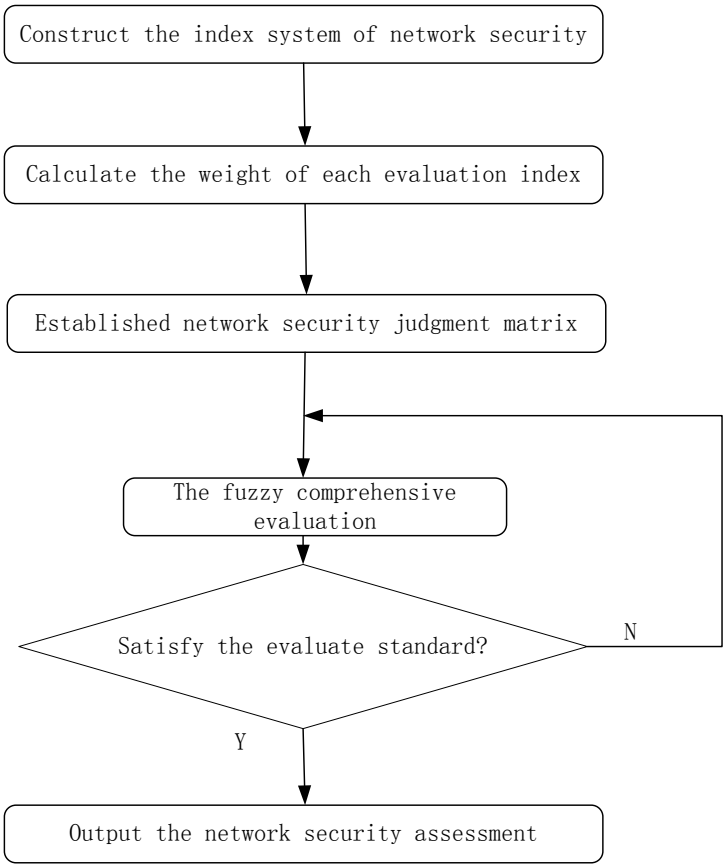

Fig.2 Network security situation assessment process

Simulation Study

To verify the feasibility and validity of the model, a practical network application service system is worked as the research object of concrete in this paper, 4 hosts in a network by Huawei S5700 switches are linked together. And one of the hosts is as the data acquisition server, and then connects it to another local area network (LAN) by using switches. And set a host of the local area network (LAN) as against the host.

Assess the network security situation based on fuzzy analytic hierarchy process (AHP). Fuzzy comprehensive evaluation result set as S = (0. 369, 0. 343, 0. 176, 0. 093, 0. 019) ; then value Network security situation assessment $f = S \cdot X^T$ = (0. 339, 0. 373, 0. 176, 0. 094, 0. 019) × (95, 80, 65, 50, 35) T= 79.25. Table.1 shows that the level of network security situation for the general, which shows that the network security status owe ideal, need to further strengthen the security of network management and monitoring. Research results show that the conclusion and the network security situation after the match, so as to show the effectiveness of evaluation model and scientific.

Summary

Fuzzy hierarchy evaluation model based on risk factors affecting the safety of network situation compare each two judgments, get the network security situational risk level. In the end test the performance of the model through the application experiment. Results show that the network security evaluation method can not only conclude different environmental conditions and indicators, At the same time, it fully consider the objective attributes of each evaluation index, so it can judge the real-time dynamic network security situation assessment quickly and accurately, and implement decision-making and system security management of network security effectively.

References

[1] FENG Dengguo, ZHANG Yang, ZHANG Yuqing. Survey of information security risk assessment [J].Journal of China Institute of Communications, 2004,25(7): 10 - 18.(in Chinese)

[2] ZHAO Dongmei, ZHANG Yuqing, MA Jianfeng. Comprehensive Risk Assessment of the Network Security[J].Computer Science, 2004,31(7): 66-69. (in Chinese)

[3] CAO Juying，ZHAO Yuelong.Novel method for information security risk assessment based on Dempster -Shafer evidence reasoning. Computer Engineering and Applications,2009，45（11）: 129-131. (in Chinese)

[4] DANG Depeng, MENG Zhen. Assessment of information security risk by support vector machine [J].Journal of Huazhong University of Science and Technology: NaturalScience Edition,2010,38(3): 46-49. (in Chinese)

[5] Gordon L，Loeb M，Lucyshyn W and Richardson R． CSI/FBI Computer Crime and Security Survey[R]. Computer and Security Institute，2006,11(1) : 1-27

[6] LIU yan. Improved information security risk assessment model research [J]. J.Changchun Inst.Tech. (Nat.sci. Edi.),2012,13(1):123-125(in Chinese)

[7] ISO/IEC 17799:2005 Information technology security techniques-Code of practice for information security management.

[8] LI Jianhong, LI Guangzheng. Application Study on Evaluation Method of Network Security[J]. Computer simulation,2011,21(7):165-168(in Chinese).