Research on Network Security Evaluation System Based on Fuzzy Comprehensive Evaluation Method

Xuepeng Huang

Hubei University of Police, Wuhan, China

42482852@qq.com

Abstract. In today's world, the Internet has become an indispensable part of our daily life, work and study. In order to meet the growing needs of users, the network has been expanding, from inside and outside the network threat, is also a variety of threats in the network security. Based on the analysis of network security elements, the method of fuzzy mathematics is applied to the network security risk assessment and the network security risk is established by combining with the analytic hierarchy process (AHP) method, which is based on the network security risk assessment, which has many human factors and difficult to quantify the indicators. The fuzzy level comprehensive evaluation model of the model through the quantitative analysis of the risk value, you can intuitively show the system security posture.

Keywords: Network security, Fuzzy algorithm, Comprehensive evaluation, Security evaluation.

1 Introduction

With the development of network technology, the way of network security threat is endless. More and more network attack methods such as hacker attack, virus and loophole have been paid more and more attention by people. In order to ensure the safe operation of the network system, widely used in the network Firewall, IDS, vulnerability scanning system, security audit system and other security equipment[1]. Each kind of network equipment can produce a large number of security event information in use. Because these devices have the features of single function, fragmentation, and can not work together, these security event messages contain a large number of repeated alarms and false alarms. As the network size gradually increased, resulting in a massive alarm data, making it difficult for real-time administrator of the massive data processing, more difficult to identify the authenticity of the alarm and found hidden information in the attack intent. In practice, most of the security incidents are not isolated, there are some links between them. Security event correlation analysis is to analyze the relative relationship between security events and security events and operating environment, and process the data of relatively isolated network security events. Through filtering, aggregating, decrypting, and discovering the data hidden behind these events Events to provide a more reliable and valuable information for network administrators.

Network security assessment system is the need for network security data processing. Network security assessment has an important position in network security technology, its basic principle is to use a variety of methods for network systems may exist in the known security vulnerabilities to detect potential hackers to exploit the security risks, and according to the test results to the system[2]. Administrators provide detailed and reliable security analysis reports and bug fix recommendations for early action to protect system information resources.

2 Evaluation Model Construction

The establishment of network security evaluation system should be based on the relevant theoretical knowledge and actual situation, not only to reflect the theory of scientific and complete, but also in practical applications reflect the adaptability and operability. From the scientific nature of the network communication security evaluation system, the mathematic method is used to evaluate the integrity of the system, and the network communication security evaluation system is proposed[3]. In general, there are many factors in the construction of a safety evaluation system index, according to the characteristics of the characteristics of the entire network communication security evaluation system of the size of the degree of network communication security evaluation of the characteristics of variables classified indicators, which form a similar Tree-like structure. At present, most of the evaluation system is established in accordance with this idea[4]. In order to quantitatively and qualitatively analyze the security evaluation of network communication, the competency evaluation system established by this research finally satisfies the combination of feature qualitative and weight quantification. The evaluation steps are as follows:

Step 1: Set up the factor set. The factor set is a set of all the factors of the evaluation object. Let $U = \{U_1, U_2 ... U_n\}$.

Step 2: The establishment of evaluation sets. Evaluation set is the evaluation of the evaluation object may make a variety of evaluation results consisting of the evaluation level set..

Step 3: Set up the weight set. Firstly, the method of determining the weight class and the weight of the factors is Delphi method (expert survey method) and AHP method (Analytic Hierarchy Process). For the fuzzy operation, the weighted sum is 1.

Step 4: A fuzzy comprehensive evaluation.

Step 5: The second-level fuzzy comprehensive evaluation.

The one-factor evaluation matrix of the second-level fuzzy comprehensive evaluation should be the first-order fuzzy comprehensive evaluation matrix. If some sub-factor set U_i still contains more factors, U_i can be divided again, so there are three models. This division in turn, in fact, the impact of factors first sub-categories, and then sub-categories, so that reflects the level of the characteristics of

factors[5]. Evaluation, from the last divided the lowest level of factors, a level up to the evaluation, until the highest rating. Figure 1 shows the fuzzy comprehensive evaluation process.
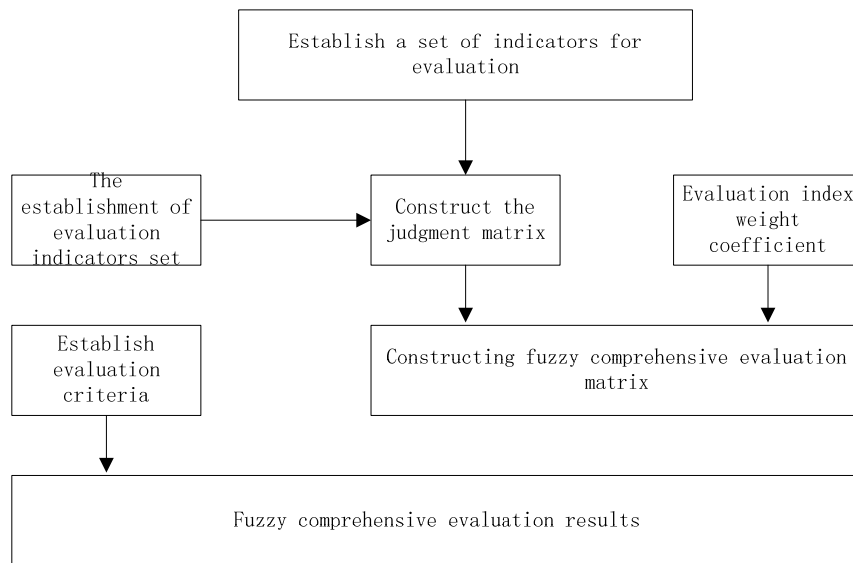
```
┌──────────────────────────────┐
│  Establish a set of indicators for │
│            evaluation              │
└──────────────────────────────┘
```

┌─────────────────┐   ┌──────────────────┐   ┌──────────────────┐
│   The   │   │ Construct the   │   │ Evaluation index │
│ establishment of│───────▶│ judgment matrix │   │   weight   │
│   evaluation   │   │   │   │   coefficient   │
│ indicators set │   └──────────────────┘   └──────────────────┘
└─────────────────┘

┌─────────────────┐   ┌──┐
│   Establish   │   │ Constructing fuzzy comprehensive evaluation │
│   evaluation   │   │   matrix   │
│   criteria   │   └──┘
└─────────────────┘

┌──┐
│   Fuzzy comprehensive evaluation results   │
└──┘

Fig 1. Illustration of the evaluation process of fuzzy synthetical decision process

3 Fuzzy Comprehensive Evaluation Method

The fuzzy comprehensive evaluation method is a method of quantifying the fuzzy index of the evaluated object by constructing the fuzzy judgment matrix, that is, determining its membership degree, and then using the fuzzy transformation principle to calculate the judgment matrix of the evaluation index. Because each factor has different influence on the evaluated object, it needs to assign different weights according to the influence of each factor, and then carries on the comprehensive operation according to the different fuzzy operator, and gives the comprehensive evaluation model[6]. This method can solve the problem that it is hard to quantify and fuzzy. It has the characteristic of strong system and clear result. It is mainly used to solve the problem of uncertainty.

(1) The establishment of fuzzy matrix

First of all, to construct a subset of fuzzy level, and then to be affected by each of the things to be quantified factors, that is, to determine the membership of each individual factor for the level of fuzzy membership, which can be achieved through several membership methods to quantify , Then the fuzzy relation matrix R can be obtained.

$$R = \begin{bmatrix} R \mid u_1 \\ R \mid u_2 \\ \cdots \\ R \mid u_p \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ r_{p1} & r_{p2} & \cdots & r_{pm} \end{bmatrix}_{p \cdot m}$$

（1）

(2) Determining the weight vector of evaluation factors

A reasonable determination of the weight vector of the evaluation factors is critical to the outcome of the assessment. In the fuzzy comprehensive evaluation method, the determination of weight vector is actually determined according to the influence degree of certain influence factor on the thing being evaluated[7]. So the weight coefficient of each factor is determined, but it should be normalized before synthesizing the weight vector .

(3) Synthesis of fuzzy comprehensive evaluation result vector

The result vector of fuzzy comprehensive evaluation is obtained by combining the weight vector *A* with the fuzzy evaluation matrix R by using the appropriate operator.

$$A \circ R = \left(a_1, a_2, \cdots\cdots, a_p\right) \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ r_{p1} & r_{p2} & \cdots & r_{pm} \end{bmatrix} = \left(b_1, b_2, \cdots\cdots, b_m\right) = B$$

（2）

(4) Fuzzy comprehensive evaluation of the results of vector analysis

The conclusion of the fuzzy evaluation vector s is given by using the maximum membership principle.

$$M = \max(S_1, S_2, \cdots, S_n)$$

(3)

4 Conclusion

Because of the complexity of the network structure and the diversity of the network equipment, we need to master and control the network security state. In this paper, the commonly used evaluation algorithm is studied, and a comprehensive evaluation method of network security based on fuzzy evaluation method is proposed. The algorithm and process of the method are described in detail. The weighted average method is used to analyze the results, and the multiple indexes can be compared and sorted. Then the multi-level model comprehensive evaluation method is used to evaluate the weight of each index. The results of the experiment show that the evaluation results of the method are in line with the actual situation, which is beneficial to the network managers to optimize the network resources, thus ensuring the normal operation of the network and improving the network security, and has good application prospect and popularization value.

Acknowledgement

References

[1] Dai Wenbin. Campus security management system based on Internet of things technology [D]. University of electronic science and technology. 2011.

[2] Wei Jianguo. The campus network security filtering model and the key algorithms [D]. Anhui University. 2013.

[3] Ceng Lihui, Xu Ying, Xu Haizhi, etc. The construction of digital campus of the research [J]. Computer and modern, 2004, (7):88-89.

[4] Zou Jingjing. Data mining technology in the application of digital campus [D]. Central south university. 2009.

[5] Zhao Chuang. Study on the scheme of construction of digital campus data warehouse [D]. Northeast normal university, 2009.

[6] Yao LinXiu. University digital campus construction scheme and implementation of technical feasibility study [D]. China University of geosciences (Beijing), 2006.

[7] Ge Suhui, Layer 3 switching technology application in campus network design to explore the [J]. China science and technology information, 2008, (20) 110-111.