Research on Network Security Situation Assessment Technology Based on Fuzzy Evaluation Method

Dehua Kong¹, Huyuan li² and Hongyan dong¹*

¹School of computer science, Wuhan Donghu University, Wuhan, Hubei, 430212, China
²Department of Information Engineering, Wuhan Information Communication Vocational and Technical College, Wuhan, Hubei, 430212, China
*Corresponding author’s e-mail: kdh@wdu.edu.cn

Abstract. With the development of Internet technology and the continuous improvement of social informatization, the network has gradually become an indispensable part of people's production and life. The importance of network security has received more and more attention. A variety of security products have been applied to the network to strengthen and maintain the safe operation of the network. However, these security means can only play a specific role in a certain range, and lack of effective data fusion and collaborative management mechanism. In the face of many scattered information, network security managers cannot respond to security incidents in time. For the purpose of grasping the current situation and changes of network security, network security situation awareness technology came into being, it has become a new hotspot in network security research. This paper proposes a fuzzy comprehensive evaluation model which combines AHP and fuzzy evaluation method to evaluate network security situation.

1. Introduction

Today, we are in the information age, and the network has become an indispensable way of our daily life, work, and learning. In order to meet the growing demand of users, the network scale is expanding, and threats from the inside and outside of the network are threatening the security of the network in various ways. In order to have a safe working and learning network environment, we need to master the security state of the network and control it at any time. This is the main problem that every network manager is facing. So how to understand and master the security state of the network, which needs to evaluate the network state. Network security situation assessment has become a hot topic in the field of network security in recent years. Network security situation assessment has two levels of significance: one is to extract the security status information of the network in real time, process, merge, and analyse the relationship to understand the current operation state of the network. At present, the experts in the field of situation assessment have done a lot of research, and put forward a lot of evaluation models and evaluation algorithms, and achieved some achievements. The United States, Canada and other western countries have established situation assessment system and developed situation assessment software: in China, the National Defence University of science and technology, Harbin Engineering University, Beijing University of technology and so on have studied their own evaluation algorithms, and the above research has achieved certain results.
2. Analysis and comparison of evaluation methods

2.1. Common evaluation algorithms

2.1.1. Data fusion evaluation method Data fusion technology is a formal description of the methods and tools for data fusion from different data sources in the future. It is a key technology for processing multi data source information, also known as "information fusion". From the perspective of information theory, multi data source information can provide more information than single data source information, and it has more advantages. Data fusion is not a new concept[1]. With the development of advanced processing technology in recent years, the real-time data fusion has become a new research hotspot.

Data fusion is a data processing technology for data synthesis, which has been widely used in many subjects. Data fusion methods are divided into three categories.

- Data layer fusion, direct data source fusion: such as weighted average, neural network and other methods for data fusion.
- Feature layer fusion, using statistical characteristics and probability model for fusion: such as Bayesian estimation, Kalman filter, statistical decision theory, etc.
- Decision level fusion, based on rule-based reasoning fusion: such as fuzzy reasoning, evidence reasoning, knowledge rule reasoning, etc.

2.1.2. Bayesian Reasoning Generally, network security assessment is realized by evaluating the network security vulnerability[2]. The main method of this evaluation method is to scan the vulnerabilities in the network. The results of the evaluation are obtained by statistical analysis according to the scanning results, and the solution is given. This method has the disadvantages of long time consuming, large bandwidth consumption and influence the normal operation of the network. In fact, network security assessment can be evaluated at a higher level, and more extensive data sources are used to get more abundant evaluation results. At present, Bayesian reasoning method is also a feasible method for network security situation assessment.

2.1.3. Fuzzy comprehensive evaluation method Fuzzy comprehensive evaluation is a method which takes the fuzzy mathematics thought as the core, and uses the method of weighted synthesis of the fuzzy relation of the things to be evaluated[3]. It describes some fuzzy factors which are unclear in boundary, difficult to quantify and describe, so it is a method to evaluate. This method can solve the fuzzy and difficult to quantify problems well, and it has the characteristics of clear results and strong system, and is mainly used to solve the uncertainty problems.

2.2. Network security situation assessment method

Since the end of last century, many researches have been carried out on the network security situation assessment at home and abroad, and a variety of situation assessment methods have been designed. In the developed countries of the west, the United States and Canada have developed a series of relevant evaluation standards, methods, and technologies, and established the relevant certification system. The domestic evaluation of network security situation started late, but also studied some typical evaluation methods, and it can be used in some fields. At present, the typical research results at home and abroad are summarized as follows:

2.2.1. Evaluation method based on network traffic characteristics analysis This method is mainly implemented by net low technology. Net Flow is a packet exchange technology, which is proposed by Cisco. Its working mode is to record network data flow information. It can record the traffic information related to each TCP/IP transaction. This method mainly extracts sensitive data related to network attack to analyse the abnormal situation in traffic. It mainly analyses some traffic characteristic values related to network performance and service.
2.2.2. Situation assessment method based on hierarchical network 

At present, the analytic hierarchy process (AHP) is widely used in the evaluation and prediction of various industries, its main idea is to decompose complex problems, group them according to a certain dominant relationship, and finally form a hierarchical structure. This hierarchical structure is generally ladder like, and then through the construction of a series of related judgment matrices, calculation of matrix eigenvalues and matrix eigenvectors, and then through the consistency check. Finally, the evaluation and decision results are obtained.

3. Study on the comprehensive evaluation model based on analytic hierarchy process and fuzzy evaluation

The fuzzy theory was proposed by Professor L. a.zadeh of the United States in the mid-1960s. The theory is based on fuzzy sets in fuzzy mathematics, and mainly takes the processing of unclear boundary, fuzzy concept, and uncertainty as its main research objectives. And it quantifies this uncertain information through the fixed method, making it into data information that can be analysed and processed by computer. In practical application, this fuzzy theory can deal with and give perfect expression to the uncertain things which are difficult to describe in language and difficult to construct by mathematical model. Because of the characteristics of fuzzy mathematics theory, it has been widely used in many fields in recent years, and has achieved many gratifying results. The most widely used method to quantify fuzzy things is to use the membership principle, evaluate the membership of many factors of the evaluated objects, establish the fuzzy evaluation matrix and make a comprehensive evaluation.

3.1. Fuzzy comprehensive evaluation methods

Fuzzy comprehensive evaluation method is a kind of fuzzy index of the evaluated object. It is a quantitative method by constructing fuzzy judgment matrix to determine its membership, and then to calculate the judgment matrix of the evaluation index by using the fuzzy transformation principle. Because of the difference of the influence of each factor on the object under evaluation, it is necessary to assign different weights according to the influence of each factor, then carry out the comprehensive operation according to different fuzzy operators, and give the comprehensive evaluation model. This method can solve the difficult to quantify and fuzzy problems, and has the characteristics of strong system and clear results, which is mainly used to solve the uncertainty.

3.1.1. The establishment of fuzzy matrix

First, we should construct fuzzy level subset, and then quantify the factors that affect each evaluated object determine the membership degree of each single factor to the fuzzy subset of grade. This can be realized by several methods of membership quantification, and then the fuzzy relation matrix $R$ can be obtained, as shown in formula (1):

$$ R = \begin{bmatrix} R | u_1 \\ R | u_2 \\ ... \\ R | u_p \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & ... & r_{1m} \\ r_{21} & r_{22} & ... & r_{2m} \\ ... & ... & ... & ... \\ r_{p1} & r_{p2} & ... & r_{pm} \end{bmatrix}_{p \times m} \tag{1} $$

The establishment of fuzzy evaluation matrix is established by combining statistics and expert experience, that is, the actual situation of each index in the statistical network security situation index, and then gives the membership value according to the experience of experts, so as to establish the fuzzy evaluation matrix.

3.1.2. The determination of weight vector of evaluation factors

It is very important to determine the weight vector of the evaluation factors reasonably. In the fuzzy comprehensive evaluation method, the weight vector is actually determined according to the influence degree of an influence factor on the evaluated object. Therefore, the weight coefficient of each factor is determined, but the weight vector should be reduced before the weight vector is synthesized[4], as shown in formula (2):
\[ \sum_{i=1}^{p} a_i = 1, a_i \geq 0, i = 1, 2, \ldots, n \]  

(2)

3.1.3. Synthetic fuzzy comprehensive evaluation result vector

The synthesis of the result vector of fuzzy comprehensive evaluation is obtained by combining the weight vector \( A \) and the fuzzy evaluation matrix \( R \) through the appropriate operator, as shown in formula (3):

\[
\begin{bmatrix}
    r_{11} & r_{12} & \cdots & r_{1m_1} \\
    r_{21} & r_{22} & \cdots & r_{2m_2} \\
    \vdots & \vdots & \ddots & \vdots \\
    r_{p1} & r_{p2} & \cdots & r_{pm_p}
\end{bmatrix}
\begin{bmatrix}
    a_1 \\
    a_2 \\
    \vdots \\
    a_p
\end{bmatrix} =
\begin{bmatrix}
    b_1 \\
    b_2 \\
    \vdots \\
    b_m
\end{bmatrix} = B
\]  

(3)

3.2. AHP determination of weight

In the comprehensive evaluation, the most important problem is the determination of weight. Analytic hierarchy process is a very good and effective method for determining the weight coefficient. It is especially suitable for those complicated problems which are difficult to use quantitative characteristics for analysis. It will be difficult to quantify the factors through the division of ordered layers to make it organized, and objective things according to practical experience fuzzy judgment, to each layer of relative importance of quantitative expression, finally all elements of the relative order of the use of mathematical methods to determine[5].

4. Conclusion

This chapter mainly studies the network security situation assessment method. This paper first introduces the commonly used evaluation algorithm and the current main evaluation technology in network security situation evaluation, and then introduces the fuzzy comprehensive evaluation method in detail. The application of fuzzy evaluation method in the evaluation of network security situation shows that the weight plays an obvious role, and the use of fuzzy evaluation matrix has sufficient information and strong comprehensive degree, which has a good application prospect.

Acknowledgments

This article is supported by the Youth Fund Project of Wuhan Donghu Academy of Sciences in 2019, "Research on Product Recommendation Based on Web Space-Time Customer Behavior Trajectory" < No: 2019dhzk006>.

References

[1] Qu X.H, S X.M. (2018) Research on network security situation assessment technology based on analytic hierarchy process. Automation technology and application, 37: 43-45.
[2] Xu H. (2015) Research on some key technologies of network security situation assessment. Information and communication, 10: 160-161.
[3] Xu L.H. (2012) Research on network security situation assessment technology based on data fusion. Computer CD software and application, 19: 134-135.
[4] Fu Q, Miao C, Zhang H. (2017) Influencing factors and preventive measures of computer network security technology. Computer fan, 01: 17.
[5] Wei L, Dai F.F, Zhao S. (2020) "New infrastructure" defines a new paradigm of network security technology innovation. China information security, 125: 40-42.