Network attack evaluation model based on directed weighted complex network and fuzzy AHP method

Luchen Chi[*], and *Bin* Wu

Beijing University of Posts and Telecommunications, China

Abstract. At present, most of the network attack effect evaluation is based on mathematical theory. The calculation process is influenced by artificial judgment, and the research on the dependence and influence between indicators is not sufficient, so the index weight setting is too subjective. This paper proposes a network attack effect evaluation model based on directed weighted complex network, and constructs an index architecture based on attribute-attack type-atomic function-evaluation index four-layers subnetwork. The index importance calculation method is given by combining the complex network theory with the traditional fuzzy analytic hierarchy process. Finally, taking the password cracking attack as an example, it is proved that this method is helpful to explore the impact mechanism of indicators on attributes, fully considers the relationship between indicators, simplifies the index system and improves the evaluation efficiency.

1 Introduction

In the process of the network attack effect evaluation, construction of evaluation index system is the key step. At present, the common attack effect evaluation methods are based on mathematical theory. For example, Liu Jin[1] and others proposed the analytic hierarchy process. But the weakness is too complex. Wang Huimei[2] and others applied rough set theory to the network attack effect evaluation, considering the relationship between different indicators, but they can't know the correlation degree among different indicators. Zhong Yuan[3] proposed an evaluation method based on entropy, which is a way to get the attack effect index through entropy difference. However, the way can’t avoid human judgment error in calculation process. Jajodia[4] proposed a method based on grey system theory , but some historical data are required in weight determination.

To sum up, the main problems of traditional methods are as follows. firstly, the selection for indicators is redundant. Secondly, the research on the dependence and impact among indicators is not sufficient, so the index weight setting is too subjective. As a new interdisciplinary subject, complex network theory can solve the above problems by analyzing network's structural characteristics and evolution laws from holistic methodology[5,6].

[*] Corresponding author: 674695773@qq.com

2 Relevant concepts

2.1 Complex network theory

The complex network model consists of nodes and edges, in which nodes represent the research objects in the real system and edges represent the relationship between objects [7]. Its advantage is that it can clearly describe the complex topological relationship between nodes. Compared with the traditional research paradigm, whose indicator weight setting is too subjective due to not considering the correlation between indicators. Therefore, it's a good way to establish the indicator architecture through the complex network. Meanwhile its special properties can provide objective measurement standards for the dependence effect and integrity which is necessary to be paid attention to in network attack effect evaluation process.

2.2 Fuzzy analytic hierarchy process

Fuzzy analytic hierarchy process [8,9] is a subjective evaluation method, which solves some problems in analytic hierarchy process. Fuzzy analytic hierarchy process is an improvement of analytic hierarchy process (AHP). Aiming at the problems of consistency test in AHP, fuzzy ideas are introduced into analytic hierarchy process. The fuzzy analytic hierarchy process used fuzzy consistent matrix to determine the weight of the index.

3 Network attack effect index system model based on weighted complex network

A set of comprehensive and quantifiable evaluation index system is the core for the network attack effect evaluation. According to the actual attack effect, this paper constructs a directed weighted complex network index system based on attribute-attack type-atomic function-evaluation index four-layers subnetwork. Its basic structure is illustrated in Fig.1.

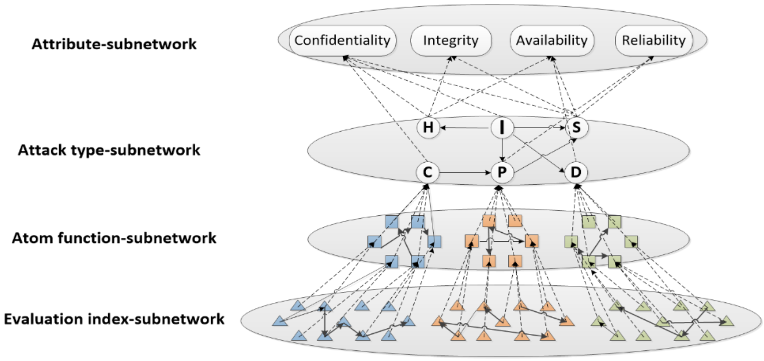

Fig. 1. The Structure Model of Directed Weighted Complex Network Index System.

According to the principles of information security, the attribute subnet can be divided into four parts, which are confidentiality, integrity, availability and reliability. According to the main steps in network attack process, the attack type subnet is divided into the following six parts. They're information collection, password cracking, permission change, denial of attack, Trojan horse and worm and virus utilization. According to the actual network attack effect, the atomic function subnet is divided into a variety of atomic functions with clear meanings. According to the measurement standard of attack effect, the evaluation index subnet is divided into several specific evaluation indexes. The association within and between each subnet is represented by a directed edge. Take password cracking as an example, the index system is shown in Table 1.

Table 1. Password crack indicators.

Atom Function	Evaluation Index
System Password Crack(C1)	System Password Crack Accuracy(C11)
	System Password Crack Rate(C12)
	System Password Crack Complexity(C13)
Database Password Crack(C2)	Database Password Crack Accuracy(C21)
	Database Password Crack Rate(C22)
	Database Password Crack Complexity(C23)
Website Management Password Crack(C3)	Website Management Password Crack Accuracy(C31)
	Website Management Password Crack Rate(C32)
	Website Management Password Crack Complexity(C33)

4 Index importance algorithm based on index-attribute correlation matrix

4.1 Construct correlation matrix

In this paper, we use nodes to represent the evaluation indexes, and the directed edges to represent the association between the evaluation indexes and then construct the internal incidence matrix based on the evaluation index subnet, which is represented by $\mathrm{V}c_{ij}$, $\mathrm{V}d_{ij}$, $\mathrm{V}h_{ij}$, $\mathrm{V}i_{ij}$, $\mathrm{V}p_{ij}$ and $\mathrm{V}s_{ij}$ respectively. $\mathrm{V}c_{ij}$ represents the impact from an evaluation index to another under the password cracking subnet. When the matrix element is 1, it represents there is an impacting relationship between the corresponding nodes, while 0 means that there is no correlation. Take $\mathrm{V}c_{ij}$ as an example, which is shown as follows.

$$Vcij = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

We use Nodes to represent atomic functions, and the directed edges to represent the association between different atomic functions based on the atomic function subnet, which is represented by $\mathrm{C}ij$, $\mathrm{D}ij$, $\mathrm{H}ij$, $\mathrm{I}ij$, $\mathrm{P}ij$ and $\mathrm{S}ij$ respectively, where $\mathrm{C}ij$ represents the impact of an atomic function on another atomic function under the password cracking subnet,When the matrix element is 1, it represents there is an impacting relationship between the corresponding nodes, while 0 means that there is no correlation. Take $\mathrm{C}ij$ as an example , which is shown as follows.

$$Cij = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We construct an external incidence matrix based on atomic function subnet, which is represented by A_{CP} , A_{ID} , A_{IH} , A_{IP} , A_{IS} and A_{PS} . It describes the association between atomic functions under different attack type subnets. A_{CP} represents the impact from an atomic function under password cracking attack subnet on another atomic function under permission change subnet. When the matrix element is 1, it represents there is an impacting relationship between the corresponding nodes, while 0 means that there is no correlation. Take A_{CP} as an example, which is shown as follows.

$$Acp = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

4.2 Determine basic meta path

The concept of the meta path is an extension of edge in network theory, which was first proposed by sun[11]. A meta path contains a series of relationships based on different nodes. In this paper, we define the basic meta path as a route which starts from an evaluation index to a specific attribute. For example, $V_I \rightarrow$ I $\rightarrow P \rightarrow S \rightarrow A$ represents that the attribute is affected by information detection, permission change and Trojan and worm attack type. The index architecture proposed in this paper includes the following basic meta paths, which are shown in Table 2.

Table 2. The basic meta path in the network attack effect index system

Id	Basic meta path	Id	Basic meta path
1	$V_C \rightarrow C \rightarrow A$	8	$V_I \rightarrow I \rightarrow H \rightarrow A$
2	$V_C \rightarrow C \rightarrow P \rightarrow A$	9	$V_I \rightarrow I \rightarrow P \rightarrow$A
3	$V_C \rightarrow C \rightarrow P \rightarrow S \rightarrow A$	10	$V_I \rightarrow I \rightarrow P \rightarrow S \rightarrow A$
4	$V_D \rightarrow D \rightarrow A$	11	$V_I \rightarrow I \rightarrow S \rightarrow$ A
5	$V_H \rightarrow H \rightarrow A$	12	$V_P \rightarrow P \rightarrow A$
6	$V_I \rightarrow I \rightarrow A$	13	$V_P \rightarrow P \rightarrow S \rightarrow A$
7	$V_I \rightarrow$ I $\rightarrow D \rightarrow A$	14	$V_S \rightarrow S \rightarrow$A

For a certain attribute, the basic meta path represents the effect generation ways from corresponding indicators through the index architecture. From this perspective, the number of basic meta paths from one index to a certain attribute can reflect the index importance to some extent. Hence, we can take the number of basic meta paths as a measure to select the important indicators to the evaluation system, and construct the network attack evaluation index system.

4.3 Index-attribute correlation matrix

Taking the basic meta path $V_I \rightarrow I \rightarrow P \rightarrow S \rightarrow A$ as an example, when there are no loops in the network, the correlation matrix A_{IA} from the DDoS evaluation index to the attribute under the path $V_I \rightarrow I \rightarrow P \rightarrow S \rightarrow A$ can be calculated by

$$A_{IA} = A_{VIVI} A_{VI\,P} A_{PP} A_{PS} A_{SS} A_{SP} \tag{1}$$

Where, $A_{PP} = I + Pij + Pij^2 + . . . + Pij^{np+1}$, Pij^2 is the two-step reachable matrix[12] among the evaluation indexes under permission change subnet, and $p^{np+1}ij$ is the np+1-step reachable matrix among the evaluation indexes under permission change subnet. np is the length of the longest path in the evaluation index nodes under permission change subnet, s.t.$pnp+1^{ij} = 0$. The elements in the final index-attribute correlation matrix A_{IA} can be regarded as a representation of the correlation degree from the evaluation index to the attribute, which can help to indicate the index importance.

4.4 Index importance sort algorithm

Most traditional evaluation methods, such as AHP, present the index system according to experts experience which is based on relationships in vertical direction among indicators. And it can't avoid human subjective effect on the evaluation result. However, the actual network attack effect is affected by many factors, it is also necessary to consider the correlation in the horizontal direction among indicators, that is, the impact among neighbor nodes or even other nodes in the whole network. Based on the calculation of the correlation matrix, the importance of a certain indicator can be defined as equation (2) shows.

$$\varepsilon_{ij} = \varpi_i \times Q_{Vij} \tag{2}$$

Where, ε_{ij} is the correlation from the index i to attribute j, i is the index weight discussed by expert and calculated by AHP method. Q_{Vij} is defined in the index-attribute correlation matrix. For a certain evaluation index, there maybe many mapping paths from it to the attribute. We can get the final index-attribute correlation strength by calculating the sum of the index-attribute correlation in different index-attribute mapping paths. In other words,

$$M_{V_{CA}} = \sum_{k=1}^{2} M_{(V_{CA})k} \tag{3}$$

Also take the password cracking attack type as an example, the results are shown in Table 3. From experts' point of view, the system password importance order is: accuracy > speed > complexity. However, considering the attack process referred from results of the index-attribute correlation matrix M_{VCA} □ The importance order is: complexity > accuracy = speed. Compared with the improved method in this paper, the importance from each evaluation index to different attributes is different. Therefore, in this paper it can consider the impact of the actual attack process on the index weight, and at the same time reduce human subjective impact by combining above two methods. Besides, the impact of evaluation indexes such as web management password cracking accuracy on the reliability is nearly zero, which can be ignored when evaluating the reliability of network attack. Therefore, this method can simplify the index system and improve the evaluation efficiency.

Table 3. Importance degree from the password cracking evaluation index to the attribute

Indicator	Weight	Confidentiality	Integrity	Availability	Reliability
C11	0.1245	0.498	0.6225	0.1245	0.3735
C12	0.1845	0.738	0.9225	0.1875	0.5535
C13	0.0625	0.75	0.9375	0.1875	0.5625
C21	0.1055	0.1055	0	0	0.1055
C22	0.1669	0.1669	0	0	0.1669
C23	0.0525	0.1575	0	0	0.1575
C31	0.1032	0.1032	0	0	0
C32	0.1579	0.1579	0	0	0
C33	0.0425	0.1275	0	0	0

5 Conclusion

This paper proposes a network attack effect evaluation model based on directed weighted complex networks. Firstly, a four-layers subnetwork model of attribute-attack type-atomic function-evaluation index is established. Then the correlation matrix between evaluation indexes and attributes is calculated according to matrix reachability theory, on which the index importance method is proposed. Finally, taking password cracking attack as an example, analyze the relationship among indicators. This method combines expert experience and theoretical operation. On the basis of traditional methods, it can fully consider the relationship between indicators, explore the impact mechanism of indicators on attributes, simplify the index system and improve the evaluation efficiency. What's more, the analysis process is based on matrix operation and has low computational complexity. In the next step, the index system and its correlation matrix can be further improved according to the network attack process. In addition, the determination threshold of the index importance is also the potential development in the future.

I would particularly like to acknowledge my supervisor, Bin Wu, for his valuable guidance throughout my studies. You provided me with the tools that I needed to choose the right direction and successfully complete my dissertation. This work is supported by Science and Technology Research and Development Program of China State Railway Group Co., Ltd. (K2020S001).

References

1. J. Liu, Y. J. Wang, Y. R. Zhang, M. Xian, and S. P. Xiao. Application of analytic hierarchy process to network attack effect evaluation. Application Research of Computers (2005)
2. Wang. Huimei, Wang. Yongjie, Zhang. Yirong, and Xian. Ming. Research of network attack effect evaluating based on rough set. Application Research of Computers, 24(**6**):118–120(2007)
3. Zhong. Yuan and Hao. Jianguo. Estimation method for information support efficiency of network attacks based on system entropy. Journal of PLA University of Science and Technology(Natural Science Edition), 015(**002**):127–132(2014)
4. S. Jajodia. Topological analysis of network attack vulnerability. In International Conference on Privacy(2006)
5. Wang. Xiaofan, Li. Xiang, and Chen. Guanrong. Complex Networks Theory and Applications (in Chinese). Tsinghua University Press(2006)
6. Zeng. Xianzhao. Network Science (in Chinese). Military Science Press(2008)
7. Zhou. Tao, Bai. Wenjie, Wang. Binghong, Liu. Zhijing, and Yan. Gang. A brief review of complex network. Physics(2005)
8. T. L. Saaty and K. P. Kearns. The Analytic Hierarchy Process. Analytical Planning(1985)
9. D. Y. Chang. Applications of the extent analysis method on fuzzy ahp. Eur J Oper Res, 95(**3**):649–655(1996)
10. Y. Sun and J. Han. Mining heterogeneous information networks: a structural analysis approach. ACM SIGKDD Explorations Newsletter, 14(**2**):20–28(2013)
11. H. Yuan and D. Wang. Calculating the shortest paths by matrix approach. In International Symposium on Neural Networks(2010)