

Application of Fuzzy AHP Method in the Effect Evaluation of Network Attack

Zhicheng Sun^{1, a}, Mingyuan Liu^{2, b}

¹Hebei College of Industry and Technology, Department of Computer Technology, Shijiazhuang, China

²Shijiazhuang No.25 Hige School, Dean's Office Shijiazhuang, China

^ahbszc@126.com, ^b 7677968@163.com

Keywords: network countermeasure; network attack; effect evaluation

Abstract. For effect evaluation on the network attack (NA), the essentiality of the application of analytic hierarchy process (AHP) and Fuzzy synthetic evaluation method (Fuzzy AHP method) were introduced. With the help of AHP method, an index system was established, and then a judgment matrix was constructed, and the weight of each index was calculated as well. Meanwhile the normalization model of the evaluation index was presented. The Fuzzy synthetical evaluation model was analyzed, also the method to calculate the membership matrix was presented, and the application of the Fuzzy2AHP method in the effect evaluation of network attack was illustrated.

Introduction

With the rapid development of computer network technology, the network in various fields is applied widely. Especially in military field, the network has everything. It is because of this network is more and more big dependence, enabling the network and combat contact also more and more close, the network has become a new battlefield space. In the future net fight, how to effectively protect your network, maximum limit destroy enemy network became a prominent problem. Therefore, the theory of network attack in-depth study and network attack effect of the objective measurement and evaluation has the extremely vital significance.

Establish the evaluation index system

Here to network attack effect evaluation as target layer (A), according to each evaluation index (C) and assessment criteria (B) the correlation of different levels are formed into A multi-level structure model, as shown in figure 1.

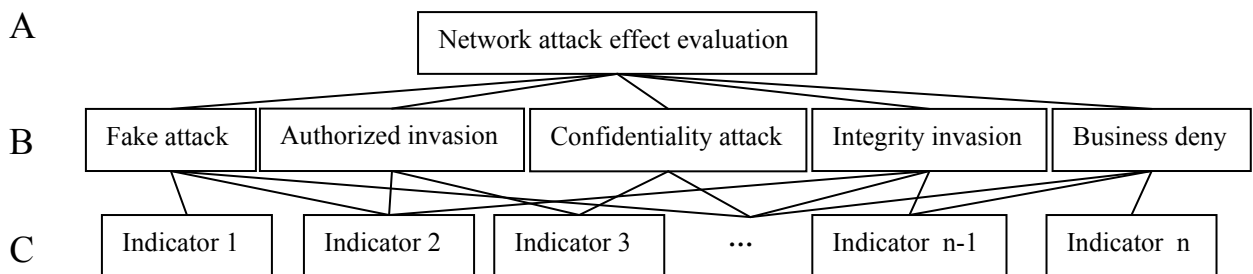


Figure 1. Network attack effect evaluation hierarchy

The model of each index and assessment criteria correlation can be expressed as:

$$X_R(c_i, b_j) = \begin{cases} 1 & \text{when } c_i R b_j \\ 0 & \text{when } c_i \bar{R} b_j \end{cases}, R \text{ is C to B's binary relation.}$$

Use AHP to determine the weights of assessment indices

Establish judgment matrix, calculation the single weight and inspection consistency.

According to the assessment criteria b_i ($1 \leq i \leq 5$) on the target a important degree, using 1 ~ 9 scale method as a more standard, contrast to each other, using Delphi method to determine matrix element value, in order to structure the judgment matrix B.

$$B = (b_{ij}) = \begin{vmatrix} b & b_1 & b_2 & b_3 & b_4 & b_5 & M_i & \bar{\omega}_i & \omega_i \\ b_1 & 1 & 1/3 & 2 & 1/3 & 4 & 8/9 & 0.9767 & 0.1317 \\ b_2 & 3 & 1 & 7 & 1 & 9 & 189 & 2.8529 & 0.3847 \\ b_3 & 1/2 & 1/7 & 1 & 1/7 & 2 & 1/49 & 0.4592 & 0.0619 \\ b_4 & 3 & 1 & 7 & 1 & 9 & 189 & 2.8529 & 0.3847 \\ b_5 & 1/4 & 1/9 & 1/2 & 1/9 & 1 & 1/648 & 0.2740 & 0.0369 \end{vmatrix}$$

$$M_i = \prod_{j=1}^5 b_{ij}, \bar{\omega}_i = \sqrt[5]{M_i}, \omega_i = \frac{\bar{\omega}_i}{\sum_{j=1}^5 \bar{\omega}_j}, \sum_{j=1}^5 \bar{\omega}_j = 7.4157, \sum_{i=1}^5 \omega_j = 1.$$

Using root method to calculate judgment matrix's maximum characteristic root λ_{\max} :

$$\lambda_{\max} = \sum_{i=1}^5 \frac{d_i}{n\omega_i} = \sum_{i=1}^5 \frac{B\omega_i^T}{n\omega_i} = 5.0235.$$

Compute random consistency ratio C_R and check the consistency: $C_R = C_I / R_I$ and $C_i = (\lambda_{\max} - n) / (n - 1) = 0.0059$. R_I is the average random consistency index, the value of 5 order matrix is 1.12. $C_R = 0.0059 / 1.12 = 0.00527 < 0.1$, showing that the consistency of judgment matrix is satisfied, the weight without logic errors, we can obtain the relative weight of b_i to a:

$$\omega = (\omega_1, \omega_2, \omega_3, \omega_4, \omega_5) = (0.1317, 0.3847, 0.0619, 0.3847, 0.0369)$$

According to the evaluation index c_j to assessment criteria b_i 's correlation, use the same method to establish c_j to b_j judgment matrix and weight for each event.

Calculate the synthesis weights. In order to get the hierarchical structure of each level of all factors relative to the overall goal of the comprehensive weight, need will be calculated each single weight proper combination. According to the established in this article, this model has A, B and C three levels.

Known B layer on A layer's relative weight is $\omega^{(1)} = (\omega_1^{(1)}, \omega_2^{(1)}, \dots, \omega_m^{(1)})^T$, C layer on B layer's relative weight is $\omega_j^{(2)} = (\omega_{ij}^{(2)}, \omega_{2j}^{(2)}, \dots, \omega_{nj}^{(2)})^T$, $j = 1, 2, \dots, m$. Among them are not affected by b_i dominant index weight is 0. Then comprehensive weight of C layer to the total target is:

$$\omega_i^{(0)} = \sum_{j=1}^m \omega_j^{(1)} \times \omega_{ij}^{(2)}, i = 1, 2, \dots, n. \text{ Thus, the C layer each index to the total target of}$$

comprehensive weight vector is $\omega^{(0)} = (\omega_1^{(0)}, \omega_2^{(0)}, \dots, \omega_n^{(0)})^T$.

Through the above calculation, and obtained A - B, B - C single weight and evaluation index on the target of comprehensive weight.

Quantitative attack effect evaluation index**Quantification of quantitative index.**

(1) The values of indicators of the dimensionless normalized model.

This paper through using exponential function to establish a nonlinear dimensionless processing model, this model can reasonably reflect the different characteristics of index change trend. Here need to consider two kinds of circumstances.

When the index value's increasing leads to the optimal effect greater: $F(V_i) = e^{(V_i - V_{i\max}) / (V_{i\max} - V_{i\min})}$;

When the index value's decreasing leads to the optimal effect greater: $F(V_i) = e^{(V_{i\min} - V_i) / (V_{i\max} - V_{i\min})}$.

$F(V_i)$ is the index i 's dimensionless normalized index value, $V_{i,\min}$ is the minimum of i , $V_{i,\max}$ is the maximum of i .

(2) Quantification of attack effect.

In the attack effect in the process of quantification, the network attack before and after the index c_i difference value as attack effect evaluation of a metric.

When the index value and attack effect is inversely proportional, in this indicator of attack effect can be expressed as: $\Delta H = -lbE_2 - (-lbE_1) = -lb(E_2 / E_1)$.

When the index value and attack is proportional to the effect, in this indicator of attack effect can be expressed as: $\Delta H = -lbE_1 - (-lbE_2) = -lb(E_1 / E_2)$.

Obviously, if $E_1 = E_2$, the $\Delta H = 0$, show that attack without any effect. E_2 change more severe, shows that the effect of the attack the more obvious, ΔH is bigger also, visible ΔH can be used as a description of the attack effect.

Quantization of the qualitative index.

In the process of qualitative the quantification index, experts can reference Table 1 to measure attack effect.

Table 1. Attack effect hierarchies

Attack effect description	Network damage / %	ΔH score reference range
No effect	<5	$0 < \Delta H < 0.07$
General	5-20	$0.07 < \Delta H < 0.32$
Good	20-50	$0.32 < \Delta H < 1$
Obviously	50-80	$1 < \Delta H < 2.32$
Very good	>80	$\Delta H > 2.32$

Application analysis

In OPNET simulation environment, use two attacks on the same network is simulated attacks, won the evaluation index of the relevant data. Here is the result of 2 times to attack, using Fuzzy-AHP method to evaluate the network attack effect analysis.

(1) According to the results of the assessment index system, the evaluation factor set identified as :

$$U = \{u_1, u_2, \dots, u_m\} = \{c_1, c_2, \dots, c_{11}\}$$

According to attack effect good or bad sequence will comment set identified as :

$$V = \{v_1, v_2, \dots, v_m\} = \{\text{very good, obviously, good, general, no effect}\}$$

The corresponding fraction set is:

$$S = \{s_1, s_2, \dots, s_m\} = \{100, 80, 60, 40, 20\}.$$

(2) According to attack effect grade, in attack effect quantification value interval determined the five characteristic value: $\Delta H_i (i=1,2,\dots,5)$, that is 2.32, 1, 0.32, 0.07, 0. According to the calculation and expert analysis, according to the membership degree method to determine the have been obtained respectively, and two against the membership degree matrix are P_1 and P_2 .

(3) According to the obtained above each evaluation index weight value and membership degree and $t_i = \sum_{i=1}^n \omega_i \times r_{ij}$ to calculate the two network attack effect evaluation results:

$$T_1 = (0.247 \ 0, \ 0.412 \ 3, \ 0.225 \ 2, \ 0.115 \ 4, \ 0);$$

$$T_2 = (0.382 \ 0, \ 0.485 \ 0, \ 0.133 \ 0, \ 0, \ 0).$$

(4) Using the weighted average method to comprehensive evaluation set processing, get first network attack effect evaluation results is:

$$\psi_1 = T_1 \times S^T = 73.5$$

The second network attack effect evaluation results is:

$$\psi_2 = T_2 \times S^T = 85.$$

Conclusion

In this paper, the network attack effect evaluation method is preliminary and evaluation method of the model is set up and the selection of the element is a complicated process, especially for the practical application more should careful. Hope that through the network attack the thorough research, to evaluate the effect of network attack, and to formulate rational network security measures and effective network enemy attack strategy to provide the theory basis and practice method.

References

- [1] Satty T L. The analytic hierarchy process [M]. New York : McGraw2Hill , 1980.
- [2] Kaufman A, Gupta M M. Int roduction to fuzzy arithmetic: theory and applications [M]. New York : Van Nostrand Reinhold , 1985.
- [3] Julisch, K. Mining Alarm Clusters to Improve Alarm Handling Efficiency. in: Proceedings 17th Annual Computer Security Applications Conference. New Orleans, LA, USA: IEEE Comput. Soc, 2001. 12.
- [4] Goodall, J. R., Lutters, W. G., Komlodi, A. The Work of Intrusion Detection:Rethinking the Role of Security Analyst. in: Proceedings of the Tenth Americas Conference on Information Systems. New York: 2004.
- [5] Ammann, P., Wijesekera, D., Kaushik, S. Scalable, Graph-based Network Vulnerability Analysis. in: Proceedings of 9th ACM Conference on Computer and Communications Security (CCS 2002): 2002.
- [6] ARDA. Advanced Research and Development Activity. Exploratory Program Call for Proposals 2006. USA. 2005.
- [7]Yanmei Li, Jingmin Wang, Shuangtao Li. The Fuzzy Neural Network Model of Smart Grid Risk Evaluation Based on Bayes. Journal of Computers. Vol.6,No.1,2011,1 :90-97.