Evaluation of Attack Effect in Ad Hoc Networks Based on Variable Weight TOPSIS Method

Linxi Guo[1], Bin Wu[1]
[1] *School of Cyberspace security, Beijing University of Posts and Telecommunications, No.10 Xitucheng Road, Beijing, China*

Keywords: Evaluation of attack effect, Variable weight theory, TOPSIS, Ad Hoc network security.

Abstract: Evaluation of Attack Effect in Ad Hoc networks is one of the key technologies for Ad Hoc network security applications. In order to solve the traditional attack effect evaluation with the constant weighted summation can't adjust the relevant weights in time to the change of the attack situation, which causes the limitation and one-sidedness of the judgment. This paper proposes an attack effect evaluation model based on variable weight theory. First, comprehensively considering the relevance of the attack's own complexity and the attack effect, establish an attack effect evaluation indicator system. Then, construct a state variable weight vector expression, so that the weights are adjusted accordingly with the change of the situation. Finally, combined with TOPSIS method, the attack effect evaluation model based on variable weight TOPSIS is constructed. The experimental simulations show that the evaluation results obtained by the model are scientific and reasonable, which makes up for the deviation caused by the decision of the constant weight, and provides a theory and method for the evaluation of the attack effect in Ad Hoc network.

1 INTRODUCTION

Compared with traditional wireless networks, Ad Hoc networks do not need infrastructure construction, and have a high coverage and high dynamic self-organizing network mechanism, which supports various devices to access and exit the network at any time, thus more in line with the actual mobile device networking. In addition, because of their robustness and low cost, Ad Hoc networks have broad application prospects in many fields such as intelligent transportation, disaster relief and military communications. However, the Ad Hoc network is a typical dynamic network with a flexible topology, and there is no unified security control center. Therefore, Ad Hoc networks are more vulnerable to various types of attacks such as eavesdropping, impersonation, tampering, etc., which may lead to greater security threats (Aarti, D.S. 2013).

A lot of researches have been done on Ad Hoc network attacks, but the number of studies on the evaluation of Ad Hoc network attacks is very limited. The evaluation of the effect of network attacks is an important part of network security. The evaluation of the network attack effect is an important part of network security. The evaluation results can not only test the effect and assessability of the specified attack (operation plan) scheme, but also measure the security of the network through simulated attacks, thereby improving the security protection capability of the network.

The research on the evaluation of network attack effect firstly determines indicator weights according to performance indicators of the target network. Then, according to the membership function of the attack effect, the comprehensive evaluation value is obtained by the linear weighted comprehensive method based on constant weights. Zeng, C. X.et al.(2016) applied fuzzy mathematics theory to analytic hierarchy process and established an evaluation model based on FAHP, thus avoiding the calculation of complex problems; Yuan, Z. and Jianguo, H. (2014) proposed an attack effect evaluation method based on network entropy, which relieved the subjectivity of the evaluation to some extent; Jajodia, S. et al.(2005) used gray theory into evaluate calculations so that the evaluation results implied the correlation between the evaluation indicators to some extent. In the study of the DoS attack effect evaluation of mobile Ad Hoc networks, the idea of variable power was introduced for this problem, but it was targeted for each specific attack

Guo, L. and Wu, B.
Evaluation of Attack Effect in Ad Hoc Networks Based on Variable Weight TOPSIS Method.
DOI: 10.5220/0008098602130221
In *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications (CTISC 2019)*, pages 213-221
ISBN: 978-989-758-357-5

(Chen, J. and Ma, T. 2012). The weight determination method, which undoubtedly increases the complexity of the evaluation, and the qualitative evaluation results obtained by the gray fuzzy evaluation model cannot measure the advantages and disadvantages of different attacks in the same category. In order to make the evaluation results more accurate and reasonable, the attack effect evaluation models are improved, and new evaluation models are continuously proposed, but there are still some problems, and the number of evaluation models that can be applied to Ad Hoc networks is extremely limited.

The commonly used constant weights vectors reflect the overall goodness of the attack effect evaluation to a certain extent, and the weight coefficient corresponding to each evaluation indicator reflects the importance of this indicator. Therefore, the constant weights vector will play a good role in most cases. However, regardless of the value of the evaluation indicator attribute, the weights vector remains unchanged, so the constant weights vector cannot objectively reflect the change of the state value of each attribute and the influence of the attribute relevance on the weights. There are many unreasonable phenomena in using the same weights vector in different attack scenarios, mainly in the following two types:

1) If the value of the indicator reaches a critical value, it will have a greater impact on the evaluation of the attack effect. For example, when the node corruption reaches a critical value, it will have a great impact on the reliability indicator of the node. The network reliability will be poor, and the corresponding security performance will be worse, especially when the destroyed node is a critical node. At the same time, when obtaining the attribute values of the attack effect evaluation, there may be cases where the individual indicator values are too low or zero. Assume that there are two evaluation indicators in the evaluation of Ad Hoc network attacks effect, namely network performance and security performance, and these two indicators are equally important, that is, the weight $w = (w_1, w_2) = (0.5,0.5)$. Then the comprehensive evaluation result is $D = 0.5u_1 + 0.5u_2$. From the evaluation results, the results of the attack effect obtained by the state vector $u = (0.1,0.9)$ and the state vector $u = (0.5,0.5)$ are the same. However, the actual situation is that the network performance of the target network with the state vector $u = (0.1,0.9)$ is already in a state of paralysis, and the network availability is significantly reduced. And the network and security performance of the target network with state vector $u = (0.5,0.5)$ are still within acceptable limits. The reason why the evaluation result is inconsistent with the actual situation is that the constant weight vector is independent of the value of each indicator, and it does not affect the influence of the indicator values on the comprehensive evaluation result.

2) When evaluating specific types of attacks, each type of attacks focuses on different network security performance metrics. For example, DoS attacks more affect the network performance of the target network, thereby destroying its reliability and availability. While obtaining information-based attacks more affect the security performance of the target network, thereby undermining its confidentiality. Therefore, different types of attack effects are not comparable.

In addition to the irrational problems caused by constant weighted summation, the current attack effect evaluation models are more subjective and focus on the attack results more than the process, ignoring the correlation between the complexity of the attack behavior and the effect of the attacks.

In order to solve the above problems, this paper innovatively proposes an attack effect evaluation model based on variable weight TOPSIS. The innovations of this paper mainly include the following points:

- This paper comprehensively considers the impact of attack complexity and proposes an attack effect evaluation indicator system suitable for Ad Hoc networks;
- This paper combines the variable weight theory based on punishment and incentive mechanism with the TOPSIS evaluation method, and proposes a state variable weight vector expression suitable for Ad Hoc network attack evaluation. The calculation formula appropriately adjusts the weight according to the attribute value of the attack effect indicator. Specifically, a penalty is imposed on the indicator weight of the attribute value that is low. While incentives are given to indicator weights with high attribute values. Therefore, this model solves the unreasonable problems brought about by the evaluation of constant weights.

Finally, we use the specific attack test in the simulation experiment platform and obtain the real and objective indicator data to verify the rationality and effect of the proposed model.

The rest of the paper is organized as follows. Section 2 proposes a standardized quantization method for indicators and establishes an evaluation system for attack effect. Section 3 describes in detail the method of determining the variable weight vector.

On the basis of using the analytic hierarchy process to determine the weight of the indicator constant, the construction and application of the state variable weight vector applicable to the evaluation are mainly studied. Then, in Section 4, the variable weight theory is combined with the TOPSIS method to describe the specific evaluation process of the variable weight TOPSIS model. Afterwards , in Section 5, the rationality and effect of the proposed model are proved by experimental simulation. Finally, Section 6 contains our conclusions.

2 ESTABLISH AN EVALUATION INDICATOR SYSTEM

The establishment of the evaluation model for Ad Hoc network attack effects can be divided into the following three steps: establishing an evaluation indicator system for attack effects, determining the weight value of the evaluation indicators, and using the comprehensive evaluation algorithm to calculate the evaluation results.

The evaluation indicator system is the infrastructure of the entire assessment process. Therefore, it is a basis for Mobile Ad Hoc Network Attack Effect of effective evaluation to establish a reasonable evaluation indicator system, which is an important basis to reflect the effect of the attack.

This paper proposes an evaluation indicator system of attack effect for Ad Hoc network, based on the correlation between attack complexity and attack effect, and gives a standardized quantification method of the indicators.

2.1 Ad Hoc Network Attack Effect Evaluation Indicator System

The basic idea of establishing the evaluation indicator system of attack effect for Ad Hoc networks is as follows: Firstly, according to the security vulnerabilities of Ad Hoc networks and the impact of common attacks, the basic evaluation indicators are selected, and the three-level indicator system of "target-criteria-indicators" is established (Lai C et al. 2015).

Considering the correlation between the complexity of the attack and the effect of the attack, this paper establishes an attack effect evaluation indicator system for Ad Hoc networks based on attributes of attack process and performance factors of attack results, as shown in Figure 1.

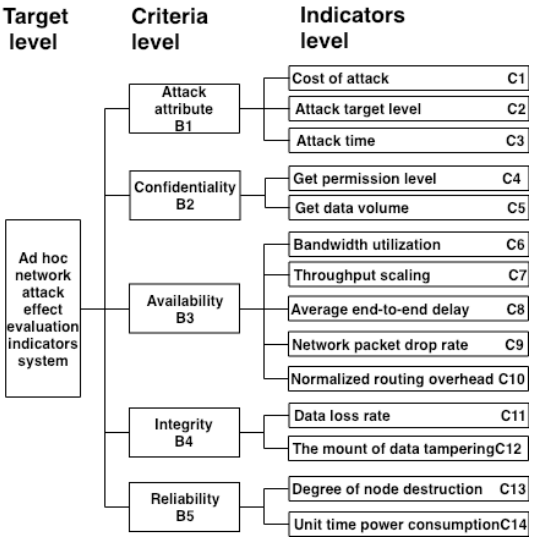

Figure 1: Ad Hoc network attack effect evaluation indicators system.

2.2 Standardized Quantification of Evaluation Indicators

2.2.1 Standardized Quantification of Qualitative Indicators

In order to quantitatively describe the effects of different types of attacks, qualitative indicators such as cost of attack, attack target level and get permission level need to be assigned from high to low, and the data sources can be obtained by experts. The specific scoring criteria are as follows:

- Cost of attack: It mainly refers to the technical requirements and the amount of equipment resources consumed to implement the attack. For this qualitative indicator, the possible states of the indicator can be listed and the reference segment value is assigned according to the degree of importance, as shown in Table 1.

Table 1: Quantitative reference value of Cost of attack.

Indicator state	Reference score
Number of malicious nodes	0~3
Resource and equipment consumption	0~3
Human resources	0~2
Financial consumption	0~4
Other	0~4

Then normalize, that is, the ratio of the initial attribute value to the reference total score value.

- Attack target level: It mainly refers to the importance of the network. It is a qualitative

indicator with order, which can be quantified according to the information, as shown in Table 2.

Table 2: Quantitative value of Attack target level.

Indicator state	Quantitative value
Single network	0.3
Partial network	0.5
Entire network	0.8

- Get permission level: It refers to the level of permission obtained through an exploit method during the attack process and quantifying it according to the degree of importance, as shown in Table 3.

Table 3: Quantitative value of Get permission level.

Indicator state	Quantitative value
Single network	0.3
Partial network	0.5
Entire network	0.8

2.2.2 Standardized Quantification of Quantitative Indicators

Different indicators have different dimensions, ranges of variation and confrontational problems. Therefore, they cannot be directly used for attack effect evaluation. It is necessary to dimensionless and normalize the original data of the indicator. In this paper, extreme value processing method will be used to standardize the results of dimensionless processing as [0,1]. Considering the problem of different confrontation among indicators, the indicators are divided into two types: benefit-oriented indicators and cost-oriented indicators, which are standardized and quantified separately:

- Benefit-oriented indicators: The greater the attribute value, the better the attack effect. For this type of indicator attribute value x_{ij}, the pre-treatment formula is:

$$a_{ij} = \frac{x_{ij} - \min(x_j)}{max\ (x_j) - \min(x_j)} \quad (1)$$

- Cost-oriented indicators: The smaller the attribute value, the better the attack effect. For this type of indicator attribute value x_{ij}, the pre-treatment formula is:

$$a_{ij} = \frac{\max(x_j)\ -\ x_{ij}}{max\ (x_j) - \min(\ x_j)} \quad (2)$$

Benefit-oriented indicators include attack target level, getting permission level, getting data volume, average end-to-end delay, network packet drop rate, normalized routing overhead, data loss rate, the amount of data tampering, degree of node destruction and unit time power consumption. Cost-oriented indicators include cost of attack, attack time, bandwidth utilization and throughput scaling.

3 VARIABLE WEIGHT THEORY TO DETERMINE INDICATORS WEIGHT

This paper focuses on the application of variable weight theory in the evaluation of attack effects, proposes a state variable weight vector expression suitable for the model and determines the value of the parameter, which is on the basis of determining the constant weight of indicators by AHP method. The state variable weight vector is the key of variable weight theory in practical application. And It is one of the most important innovation of this paper.

3.1 Determination of Constant Weight of Indicators Based on AHP

Analytic Hierarchy Process (AHP) is a method for determining the weight of indicators combined with qualitative analysis and quantitative analysis. It can quantify multiple uncertainties and fuzziness in the decision process. AHP requires that the problem to be solved be decomposed into several parts, each Parts are divided into different hierarchical structures. Compare each indicator at the same level and determine the weight of the indicator based on the importance of the indicator (Sun Z et al. 2012).

3.1.1 Constructing Judgment Matrix

According to the expert opinion, the pairwise comparison factors are quantified using the 1–9 ratio scale comparison table with reference to expert opinions, as shown in Table 4.

Table 4: 1–9 ratio scale comparison table.

Nine-scale	Meaning
1	ai is as important as a j
3	ai is a little bit important than a j
5	ai is obvious important than a j
7	ai is consuming important than a j
9	ai is extreme important than a j
Remarks: Take 2, 4, 6, 8 between adjacent judgment values	

According to Table 4 and the comparison of the advantages and disadvantages of each evaluation indicator, the following judgment matrix can be constructed:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad (3)$$

Where: $a_{ij}(i, j = 1, 2, \dots, n)$is the ratio of the i-th factor to the importance of the j-th factor. $a_{ij} > 0$ and $a_{ij} = 1/a_{ji}$.

3.1.2 Calculate Indicator Weights and Consistency Check

For all pairs of comparison matrices, consistency check is required. The purpose of consistency check is to avoid the self-contradictory phenomenon of subjective judgment.

Define $CR = \frac{CI}{RI}$. If CR<0.1, the judgment matrix is considered to satisfy the consistency, where $CI = \frac{\lambda_{max}-n}{n-1}$; λ_{max} is the maximum eigenvalue of the judgment matrix A; n is the order; RI is the average random consistency indicator. Table 5 gives the corresponding RI values of matrix 1-14.

Table 5: The value of the random consistency indicator RI(n).

n	1	2	3	4	5	6	7
RI	0	0	0.52	0.89	1.12	1.26	1.36
n	8	9	10	11	12	13	14
RI	1.41	1.46	1.49	1.52	1.54	1.56	1.58

When the judgment matrix satisfies the complete consistency, the eigenvector corresponding to the eigenvalue λ_{max} is the constant coefficient of the indicator $W = (w_1, w_2, \dots, w_n)^T$.

Since the judgment matrix is constructed by the subjective judgment of the expert, if it does not meet the consistency, the data need to be adjusted.

3.2 Determination Indicators Weight by Variable Weight Theory

The introduction of variable weight theory can solve the problem that the weights of indicators in constant weight assessment cannot be changed according to the change of the attack situation, leading to the decision bias. Therefore, how to apply variable weight theory to the field of attack effect evaluation, which can make the change of weight better reflect the attack situation, is the key of this paper.

3.2.1 Variable Weight Theory

Variable weights are relative to constant weights. The concept of variable weight vector and state variable weight vector were first proposed by Wang, P.X. (1985). It was emphasized that the weight of indicator should change with the change of attribute value of indicator in order to overcome the deviation caused by constant weight decision-making. Li, H. X. (1995) further gave the axiomatic definition of variable weight and state variable weight vector.

Let $U = (u_1, u_2, \dots, u_n)$ be the state variable and $w_j(u_1, u_2, \dots, u_n), (j = 1, 2, \dots, n)$ be the variable weight of the relative constant weight w_j. According to the variable weight theory, the variable weight vector satisfies the following axiom (Deqing, L. 2002):

1) Normalized condition:
$\sum_{j=1}^{m} w_j(u_1, u_2, \dots, u_n) = 1$;

2) Continuity: The variable weight vector $w_j(u_1, u_2, \dots, u_n)$ is continuous with respect to each independent variable $u_i(i = 1, 2, \dots, n)$;

3) Monotonicity: The variable weight vector $w_j(u_1, u_2, \dots, u_n)$ is monotonically decreasing (punitive variable weight) or increasing (incentive variable weight) with respect to the independent variable $u_i(i = 1, 2, \dots, n)$.

The variable weight vector x mainly relies on the construction of state variable weight vector s. According to the configuration level of attributes of attack effect evaluation indicator, the weight values of each indicator are adjusted. In addition to satisfying continuity and monotonicity, the state-varying weight vector also satisfies the Hadamard product:

$$W(U) = \frac{W \cdot S(U)}{\sum_{j=1}^{n} w_j S_j(U)} \quad (4)$$

According to the above definition, it can be seen that the purpose of the punitive state variable weight vector is to punish the low-level indicator attribute to ensure the balance of the evaluation indicator by increasing the weight of the indicator with the decrease of the state value; The purpose of the incentive state variable weight vector is to stimulate the high-level indicator attribute by increasing the indicator weight with the increase of the state value.

3.2.2 Constructing State Variable Weight Vector

The key to the application of variable weight theory to the actual variable weight problem lies in the construction and selection of the state variable weight vector $S(U)$. Therefore, the characteristics of the existing various types of state variable weight vectors and the requirements of equilibrium for the decision-making problem should be fully considered in practical applications. Next, after analysing the

evaluation process of attack effect for Ad Hoc networks, it is proposed that in order to meet the variable weight requirements proposed in this paper, the constructed state variable vector should satisfy the following characteristics:

1) The indicator value is too large or too small, and the weight is increased. If a certain indicator is too high in the evaluation process, which means that a certain performance indicator of the target network is too low or the attack cost is very small, it will affect the rise of the overall attack effect level regardless of the size of the constant weight. Therefore, the weight of the indicator needs to be increased. Similarly, if a certain attribute value is very low, which means that a certain performance of the target network is not affected by the attack or the attack cost is too high, it will also affect the overall evaluation level of attack effect to a certain extent even if the constant weight of this indicator is very small. So, the weight of the indicator also needs to be increased.

2) Incentive range is greater than punishment range. Due to the complexity of Ad Hoc networks, the relationship between the proposed attack effect evaluation indicators is relatively large and inevitably there are redundant indicators. By analyzing the value of single indicator separately, it is found that when the value of single indicator is high, such as the average end-to-end delay is too high, the overall attack effect is significantly improved. However, when the value of single indicator is low, the overall attack effect is not significantly reduced. Therefore, considering the balance of the evaluation indicator system, the state variable weight vector in the evaluation model of the attack effect of Ad Hoc network should satisfy the requirement that the incentive range is greater than the penalty range.

3) The punishment and incentive of the indicator with relatively large constant weight are also relatively large. The constant weight reflects the relative importance of each indicator attribute to a certain extent. The evaluation result of the attack effect is more dependent on the indicator with relatively large weight. Therefore, the state variable weight vector should be able to punish and motivate the indicators with relatively large constant weight.

In view of the advantages of exponential state variable weight vectors, such as obvious decision-making requirements, flexible parameter setting and strong model expansion ability, this paper constructs the expression of state variable weight vectors $S(U) = (S_1(U), S_2(U), \dots, S_n(U))$ as Equation 5 by drawing on the relevant research results of variable weight theory and satisfying the above three points of analysis.

$$S_j(u_j) = \begin{cases} e^{-\alpha n w_j (u_j - k\bar{u})}, & u_J \in [0, k\bar{u}] \\ 1, & u_J \in [k\bar{u}, \bar{u}/k] \\ e^{\beta n w_j (u_j - \bar{u}/k)}, & u_J \in [\bar{u}/k, 1] \end{cases} \quad (5)$$

Where: n is the number of indicators; $j = 1,2, \dots, n$; $\bar{u} = \frac{\sum_j^n u_j}{n}$ is the average attack effect indicator value; α, β are the penalty amplitude coefficient and the excitation amplitude coefficient respectively and $0 < \alpha < \beta$; $k \in [0,1]$ is the penalty threshold coefficient; when the value of the j-th indicator status value is not higher than the penalty threshold or not lower than the incentive threshold, the weight is increased by changing the weight to achieve the purpose of punishment or incentive. In practical applications, the evaluator should set α, β and k according to the specific requirements of the attack effect evaluation.

4 CONSTRUCTION OF VARIABLE WEIGHT TOPSIS EVALUATION MODEL

The basic principle of Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) is to rank the evaluation objects by means of the positive ideal solution and the negative ideal solution in the multi-objective decision problem. Theoretically, the positive ideal solution and the negative ideal solution are the optimal solution and the worst solution respectively, which are often not achieved in reality. When evaluating the attack effect of an attack scheme, the scheme should be judged from the distance between the two ideal solutions to determine the situation between the different schemes.

On this basis, the paper proposes a variable weight TOPSIS model.

4.1 Construction of Normalized Multi-Attribute Evaluation Matrix

There are m attack schemes to form a scheme set $V = \{V_1, V_2, \dots, V_m\}$, and n evaluation indicators constitute the indicator set $C = \{C_1, C_2, \dots, C_n\}$, then the evaluation sample value x_{ij} of $\boldsymbol{V_i}$ to C_j constitutes the multi-attribute evaluation matrix X.

$$\mathrm{X} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \quad (6)$$

4.2 Normalization of Evaluation Matrix

The indicators are divided into qualitative indicators and quantitative indicators. Qualitative indicators can be normalized according to the quantitative principles in Table 1, Table 2 and Table 3. The quantitative indicators can be further divided into benefit indicators and cost indicators, which are normalized according to formula (1) and formula (2) respectively to obtain the normalized matrix U as follows.

$$U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m1} & u_{m2} & \cdots & u_{mn} \end{bmatrix} \quad (7)$$

4.3 Determining Indicator Weights Based on Variable Weight Theory

Firstly, the AHP method is used to calculate the indicator constant weights, and the indicator constant weight coefficient vector $W = (w_1, w_2, \dots, w_n)$ is obtained. Then according to the state variable weight vector, that is, formula (5), the indicator weights $W(U_i) = (w_1(U_i), w_2(U_i), \dots, w_n(U_i))$ are calculated.

4.4 Establishing the Weighted Normalization Evaluation Matrix Based on Variable Weight Vectors

The weighted normalization evaluation matrix Y is obtained by multiplying the corresponding items of the matrix U and the matrix W(U), and is expressed as follows:

$$U = \begin{bmatrix} u_{11}w_1(U_1) & \cdots & u_{1n}w_n(U_1) \\ u_{21}w_1(U_2) & \cdots & u_{2n}w_n(U_2) \\ \vdots & \ddots & \vdots \\ u_{m1}w_1(U_m) & \cdots & u_{mn}w_n(U_m) \end{bmatrix} \quad (8)$$

4.5 Calculating the Closeness of Attack Schemes

1) Positive and negative ideal solutions are as follows:

$$\begin{cases} Y^+ = \{\max(y_{ij} | i = 1,2,\dots,m)\} = \{y_1^+, y_2^+, \dots, y_n^+\} \\ Y^- = \{\min(y_{ij} | i = 1,2,\dots,m)\} = \{y_1^-, y_2^-, \dots, y_n^-\} \end{cases} \quad (9)$$

2) The distance values between each attack scheme and the ideal solutions are as follows:

$$\begin{cases} d_i^+ = \sqrt{\sum_{j=1}^{n} (y_{ij} - y_j^+)^2} \\ d_i^- = \sqrt{\sum_{j=1}^{n} (y_{ij} - y_j^-)^2} \end{cases} \quad (10)$$

3) The closeness of each attack plan and positive ideal solution is calculated according to the following formula:

$$E_i^+ = \frac{d_i^-}{d_i^+ + d_i^-} \quad , 0 \le E_i^+ \le 1 \quad (11)$$

Where: E_i^+ represents the closeness degree of each evaluation scheme and the positive ideal solution, and also indicates the degree of distance from the negative ideal solution. Therefore, each scheme can be evaluated and ranked by sorting E_i^+ in descending order.

5 CASE ANALYSIS

5.1 Simulation Environment Setting

The simulation environment is established under NS2. The settings of network parameters and environment parameters in the scenario are shown in Table 6.

Table 6: Simulation parameters setting.

Network parameter	Set value	Scene parameter	Set value
Simulation area size	1000m*1000m	Channel attenuation model	TwoRayGround
Number of network nodes	60	Antenna type	Omni Antenna
Channel type	Channel/Wireless	PHY protocol	Phy/WirelessPhy
Channel bandwidth	2Mbps	MAC Protocol	MAC/802_11
Maximum movement rate	30m/s	Routing Protocol	AODV
Transmission distance	250m	Interface	Queue/droptail
Data packet size	512 Bytes	Wireless network interface	LL

At the beginning of the simulation, the initial energy of all nodes is consistent, the packet loss rate is maintained between 0% and 15%, and the attack duration is 300 seconds.

5.2 Quantitative Measurement of Indicators

1) In the simulation experiment analysis of the Hello flood attack scenario, the attack nodes are randomly selected. as shown in Figure 2. The attack payload is 20 kb/s, and the number of attack nodes is 4, 8, and 12. The normalized values of the indicators are as shown in Case 1, Case 2 and Case 3 in Table 7.

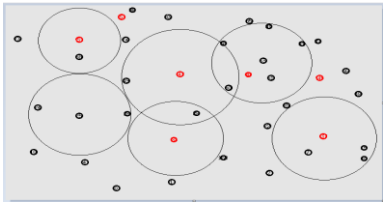

Figure 2: Simulation of the Hello Flood attack scenario.

2) In the simulation experiment analysis of the wormhole attack scenario, the attack nodes are randomly selected. as shown in Figure 3. The number of malicious nodes is 4 and 8. The normalized values of the indicators are as shown in Case 4 and Case 5 in Table 7.

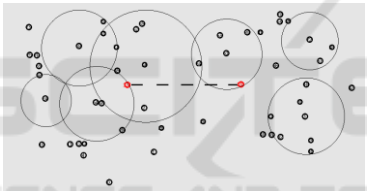

Figure 3: Simulation of the wormhole attack scenario.

Table 7: Indicator normalization values.

Indicator	Case1	Case2	Case3	Case4	Case5
Number of malicious nodes	4	8	12	4	8
C1	0.68	0.43	0.31	0.58	0.39
C2	0.30	0.30	0.30	0.30	0.30
C3	0.40	0.40	0.40	0.40	0.40
C4	0	0	0	0	0
C5	0	0	0	0.42	0.67
C6	0.33	0.43	0.62	0.38	0.44
C7	0.30	0.42	0.51	0.33	0.42
C8	0.17	0.26	0.33	0.46	0.46
C9	0.28	0.43	0.62	0.52	0.68
C10	0.15	0.20	0.42	0.16	0.22
C11	0.32	0.46	0.45	0.46	0.58
C12	0	0	0	0	0
C13	0.083	0.10	0.13	0.067	0.067
C14	0.11	0.17	0.24	0.087	0.10

5.3 Obtaining Indicator Weights Based on Variable Weight Theory

1) The basis weight of each indicator is determined based on the AHP method. The judgment matrix of the criterion level indicator $B = \{B_1, B_2, B_3, B_4, B_5\}$ based on the expert opinion is established as follows:

	B_1	B_2	B_3	B_4	B_5
B_1	1	1/5	1/6	1/5	1/4
B_2	5	1	1/2	1	2
B_3	6	2	1	2	3
B_4	5	1	1/2	1	2
B_5	4	1/2	1/3	1/2	1

CR=0.0145<0.1, which satisfies the consistency requirement, and the weights of the criterion layer can be calculated as W= (0.0901,0.224,0.301,0.224, 0.160). Similarly, the weights of each indicator layer can be calculated as shown in Table 8.

Table 8: Indicator weight values of each layer.

Aggressive indicator	W =(0.485,0.340,0.175)
Confidentiality indicator	W =(0.667,0.333)
Usability indicator	W =(0.222,0.097,0.169,0.384,0.128)
Integrity indicator	W =(0.667,0.333)
Reliability indicator	W =(0.5,0.5)

Finally, the resulting constant weight vector is W = (0.0441,0.0309,0.0159,0.149,0.0746,0.0668, 0.0292,0.0509,0.116,0.039,0.149,0.0746,0.08,0.08).

2) Determine the variable weight vector matrix. According to the variable weight state vector, set α=0.5, β = 0.9, k=0.7. Combining the formulas (5), (4) and the constant weight vector W, we can obtain the variable weight vector matrix as:

$$W(U)=\begin{bmatrix} 0.0511 & 0.0417 & 0.0398 & 0.0441 & 0.0384 \\ 0.0293 & 0.0282 & 0.0279 & 0.0283 & 0.0269 \\ 0.0153 & 0.0146 & 0.0143 & 0.0146 & 0.0138 \\ 0.1661 & 0.1642 & 0.1682 & 0.1699 & 0.1659 \\ 0.0767 & 0.0749 & 0.0753 & 0.0684 & 0.0774 \\ 0.0639 & 0.0643 & 0.0701 & 0.0613 & 0.0581 \\ 0.0277 & 0.0272 & 0.0270 & 0.0268 & 0.0254 \\ 0.0482 & 0.0465 & 0.0459 & 0.0478 & 0.0443 \\ 0.1099 & 0.1161 & 0.1361 & 0.1223 & 0.1348 \\ 0.0370 & 0.0356 & 0.0352 & 0.0363 & 0.0341 \\ 01415 & 0.1619 & 0.1370 & 0.1460 & 0.1557 \\ 0.0767 & 0.0749 & 0.0753 & 0.0763 & 0.0734 \\ 0.0790 & 0.0764 & 0.0757 & 0.0794 & 0.0765 \\ 0.0778 & 0.0735 & 0.0722 & 0.0785 & 0.0751 \end{bmatrix}^T$$

5.4 Comprehensive Evaluation Results and Analysis Based on Variable Weight TOPSIS Method

Based on the weighted vector matrix W(U), the weighted normalized evaluation matrix is further calculated to obtain the closeness of the attack scheme, as shown in Table 9. The rationality and effect of the variable weight TOPSIS evaluation model are verified by comparison with the calculation results of the constant-weight TOPSIS evaluation model.

Table 9: Closeness of each attack scheme.

	Case1	Case2	Case3	Case4	Case5
variable-weight TOPSIS	0.1892	0.3341	0.4938	0.5079	0.7562
constant weight TOPSIS	0.1673	0.3304	0.4919	0.4831	0.7835

Using variable weight TOPSIS evaluation method, the evaluation results rank of the attack effect is Case 1 < Case 2 < Case 3 < Case 4 < Case 5. If constant-weight TOPSIS method is used, the attack effect evaluation rank is Case 1 < Case 2 < Case 4 < Case 3 < Case 5. Comparative analyses of the results of different methods are as follows:

1) Case 1 < Case 2 < Case3 and Case 4 < Case 5 are satisfied simultaneously. It means that for the same attack scheme, the more malicious nodes, the better the attack effect. According to this, the rationality of the variable weight TOPSIS model has been confirmed.

2) Case 4 is a wormhole attack initiated by four malicious nodes. By establishing a fake malicious channel to steal data packets, the network performance and security performance of the target network are simultaneously reduced. In comparison, although Case 3 has more malicious nodes, the flood attack only affects the network performance of the target system. Therefore, the attack effect of Case 4 is stronger than Case 3. The evaluation results of variable weight TOPSIS model have shown that the proposed model solves the limitation of the problems in constant-weight TOPSIS model to some extent, and is a more effective evaluation method.

6 CONCLUSIONS

Aiming at the problem of attack effect evaluation of Ad Hoc networks, based on the comprehensive consideration of the correlation between attack complexity and attack effect, this paper constructs a comprehensive evaluation indicator system of attack effect. And by introducing the variable weight theory, an attack effect evaluation model based on variable weight TOPSIS is proposed. The model can reasonably adjust the weights based on the change of the attribute values of each indicator, and can obtain a more reasonable evaluation result. The proposed evaluation method overcomes the limitations of traditional attack effect evaluation methods and provides an effective reference processing method for Ad Hoc network attack effect evaluation.

REFERENCES

Aarti, D.S. 2013. Tyagi, “Study Of Manet: Characteristics, challenges, application and security attacks”. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.252-257.

Zeng, C. X., Quan-Yuan, W. U., Ai-Ping, L. I. and Jiang, R. 2016. Research on fahp based trojan attack effect evaluation. Chinese Journal of Network & Information Security.

Yuan, Z. and Jianguo, H. 2014. Estimation method for information support efficiency of network attacks based on system entropy. Journal of Pla University of Science & Technology.

Jajodia, S., Noel, S. and O’Berry, B. 2005. Topological analysis of network attack vulnerability. In Managing Cyber Threats. Springer, Boston, MA, pp. 247-266.

Chen, J. and Ma, T. 2012. DoS attack effect assessment method in mobile Ad Hoc network. Dianguang yu Kongzhi(Electronics, Optics & Control), 19(3), pp.86-89.

Lai, C., Chen, X., Chen, X., Wang, Z., Wu, X. and Zhao, S. 2015. A fuzzy comprehensive evaluation model for flood risk based on the combination weight of game theory. Natural Hazards, 77(2), pp.1243-1259.

Sun, Z. and Liu, M. 2012. Application of Fuzzy AHP Method in the Effect Evaluation of Network Attack. In 2nd International Conference on Electronic & Mechanical Engineering and Information Technology. Atlantis Press.

Wang, P.Z. 1985. Fuzzy sets and random colony shadow. Beijing: Beijing Normal University Press, pp. 93−102.

Li, H.X. 1995. Factor space theory and knowledge representation of Mathematical framework(VIII): variable weight synthesis. Fuzzy Systems and Mathematics, 9(3), pp.1−9.

Deqing, L. 2002. The properties and construction of state variable weight vectors. Journal of Beijing Normal University, 38(4), pp.455-461.