International Core Journal of Engineering Volume 5 Issue 10, 2019
ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

Security risk assessment based on dynamic fuzzy Petri net in Ad Hoc network

Zhaoyi Chen[1, a], Xiufeng Gao[1, b]

[1] Campus of Shijiazhuang, AEU, Shijiazhuang 050000, China.

[a]handan50511@163.com, [b]402158021@qq.com

Abstract

Ad Hoc network has the characteristics of no center, no infrastructure and so on, and its security is facing severe challenges. In this paper, we propose a fuzzy Petri-net model to assess the security risk of the Ad Hoc network. By introducing the strategy of transition threshold and certainty factor, the index weight and evaluation index system can be adjusted automatically and flexibly, improving the accuracy and adaptability of the evaluation model. To improve calculation speed, an inference algorithm of fuzzy rule is put forward by making full use of the characteristics of Petri net and matrix parallel operation. Finally, we carried out the experiment of network attacks, and the experimental results show that the model is feasible and effective.

Keywords

Ad Hoc, Petri-net, Attacks, Assessment, Security risk.

1. Introduction

An Ad Hoc network is a network that forms among peers for a common purpos, which has been widely used in military communications and other occasions where communication needs to be temporarily established [1]. Ad Hoc network has the characteristics of no hub, multi-hop routing, and dynamic topology, which is more vulnerable to various security threats than traditional networks [2]. The security of Ad Hoc networks has been the focus of research, but there is less research on the assessment of the security risk of the Ad Hoc. Y. Zhang, Z. Wei and W.Gao [3, 4] have studied the survival, reliability and secure routing protocol of Ad Hoc network, but did not quantify the security risk. Z.F. Li, H.Y. Fan and other scholars [5, 6, 7], combined with the Ad Hoc network application, analyzed and studied the anti-destruction, communication capability and efficiency of tactical communication network, and put forward the evaluation model of hierarchical analysis method, but these index systems could not be automatically adjusted with the change of application scenarios. For example, when the Ad Hoc network is attacked by a black hole, its packet loss rate increases, but parameters such as end-to-end delay do not change significantly, and if the indicator weight remains the same, the impact of the packet loss rate on the assessment results cannot be fully reflected.

In view of this problem, an evaluation model based on dynamic fuzzy Petri-net is proposed, which has the ability to graphically describe Petri network, fuzzy system reasoning and dynamic adjustment of index structure. Petri-nets are mathematical modeling tools used to analyze and simulate concurrent systems. The system is modeled as a directed graph with two sets of nodes: the set of places that represent state or system objects and the set of events or transitions that determine the dynamics of the system [8].

1.1 Contribution

Our main contributions are as follows.

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

(1) We propose a dynamic fuzzy Petri-net model to assess the security sisk of Ad Hoc net under network attacks.

(2) The dynamic transition threshold and certainty factor are introduced in the model, and the dynamic adjustment of indicator weight and indicator architecture is realized, so that the security risk assessment can be carried out on different types of attacks, and the accuracy, sensitivity and adaptability of the assessment are improved.

1.2 Assessment process

The assessment process of this model is as follows

(1) First of all, the Ad Hoc network security index is analyzed, and the dynamic fuzzy Petri-net model is constructed, which is the premise of the assessment results.

(2) The indicator data are obtained and the initial state matrix and the initial weight matrix of the Petri-net model are calculated.

(3) Finally, fuzzy reasoning is carried out to calculate security risk value and analyze the assessment results.

2. Dynamic fuzzy petri-net

2.1 Related definitions

2.1.1 Definition of the model

A dynamic fuzzy petri-net can be defined as a 10-tuple: $\mathrm{DFPN}=(\mathrm{S},\mathrm{T},\mathrm{D},\boldsymbol{IN},\boldsymbol{OUT},\boldsymbol{R},\boldsymbol{\rho},\boldsymbol{\theta},\boldsymbol{\mu})$,where

(1) $\mathrm{S}=\{s_1,s_2,...,s_n\}$is a finite set of places.

(2) $\mathrm{T}=\{t_1,t_2,...,t_m\}$is a finite set of transitions.

(3) $\mathrm{D}=\{d_i\}$is a finite set of proposition. |S| = |D|.

(4) $\boldsymbol{IN}=\{in_{ij}\}:S\times T\to\{0,1\}$ ($i=1,2,...n$, $j=1,2,...m$)is the input function, a mapping from places to transitions. The set of input of t_j is defined as $\bullet t_j$.

$$\boldsymbol{IN}=\{in_{ij}\}=\begin{cases}in_{ij}=1, & s_i \text{ is input of } t_j\\ in_{ij}=0, & s_i \text{ is not input of } t_j\end{cases} \tag{1}$$

(5) $\boldsymbol{OUT}=\{out_{ji}\}:T\times S\to\{0,1\}$ ($i=1,2,...n$, $j=1,2,...m$)is the output function, a mapping from transitions to places. The set of output of t_j is defined as $t_j\bullet$.

$$\boldsymbol{OUT}=\{out_{ji}\}=\begin{cases}out_{ji}=1, & s_i \text{ is output of } t_j\\ out_{ji}=0, & s_i \text{ is not output of } t_j\end{cases} \tag{2}$$

(6) $\boldsymbol{R}=\{r_{ij}\}$ ($i=1,2,...n;\ j=1,2,...q$)is a marking of the Petri-net, where r_{ij} is a fuzzy number defined in the universe of discourse [0, 1], indicating the probability of place s_i being on j-level. $\boldsymbol{R}(0)$ is the initial marking.

(7) $\boldsymbol{\mu}=\{\mu_j\}:T\to[0,1]$ ($j=1,2,...m$)is the set of certainty factor, a mapping from transitions to real values between zero and one, where μ_j is the certainty factor of transition t_j for its output place.

(8) $\boldsymbol{\theta}=\{\theta_j\}:T\to[0,1]$ （ $j=1,2,...m$ ）is the threshold matrix, a mapping from transitions to real values between zero and one, where θ_j is the threshold of transition t_j .

(9) $\boldsymbol{\lambda}=\{\lambda_j\}:T\to[0,1]$ （ $j=1,2,...m$ ）is the set of truth values, a mapping from places to real values between zero and one, where λ_j is the value of the input place of transition t_j for it.

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

(10) $\boldsymbol{\rho}=\{\rho_j\}:T\to[0,1]$ （ $j=1,2,...m$ ）is an initial importance function of transitions, a mapping from transitions to real values between 0 and 1, where ρ_j is the weight of transition t_j for its output place.

2.1.2 Production rule

Usually, in a Petri-net network, the places are denoted by circles, and the transitions are denoted by rectangles [9]. DFPN can be used to establish an intuitive graphical production rule model, as shown in Figure. 1 and Formula (3).

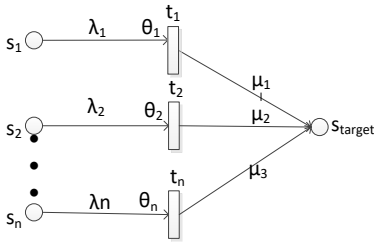

Figure 1. Production rule

$$r(s_{target})=\sum_i \mu_i \times r(s_i),\quad \lambda_i \geq \theta_i \tag{3}$$

2.1.3 Matrix operation

To express the matrix operation more clearly, accurately and succinctly. To express the matrix operation more clearly, accurately and succinctly, we define two special operators:

(1) $\oplus$: $\boldsymbol{\alpha}_{m\times 1}=\boldsymbol{\lambda}_{m\times 1}\oplus\boldsymbol{\theta}_{m\times 1}=\{\alpha_j\}=\begin{cases}\alpha_j=1, & \lambda_j>\theta_j\\ \alpha_j=0, & \lambda_j\leq\theta_j\end{cases}$,

(2) $\otimes$: $\boldsymbol{B}_{n\times m}=\boldsymbol{A}_{n\times m}\otimes\boldsymbol{\mu}_{1\times m}\Leftrightarrow b_{ij}=a_{ij}\times\mu_j,(i=1,2,...,n;\ j=1,2,...,m)$

2.1.4 Risk level

Referring to the Guidelines for the Classification of Security Protection of Computer Information Systems, this paper sets five levels of security risk, ranging from low to high is "low", "moderate", "medium", "high" and "extreme". The range of network performance degradation for each risk level is shown in Table 1. The median value of all levels form vector $Q=[0.1,0.3,0.5,0.7,0.9]$.

Table 1. Risk levels

level	Low	moderate	medium	High	extreme
values	[0,0.2]	(0.2,0.4]	(0.4,0.6]	(0.6,0.8]	(0.8,1]

2.2 DFPN model

We assess the security risk by studying changes in Ad Hoc's network security performance. For Ad Hoc network security, some scholars have studied the relationship between network attacks and end-to-end delay, round-trip time, packet loss rate, throughput and other indicators [10]. Based on the security attributes of the information system, we assess the security risk of Ad Hoc from the perspective of network availability, reliability, information confidentiality and integrity. According to the Petri-net structure, we use the indicators as the places, the change of the indicators as the marking for building the Petri-net model. DFPN is shown in the Figure. 2. The places of the DFPN model relating to the indices are listed in Table 2, where s_i $(i=1,2,...18)$ indicates the corresponding places in the DFPN model.

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

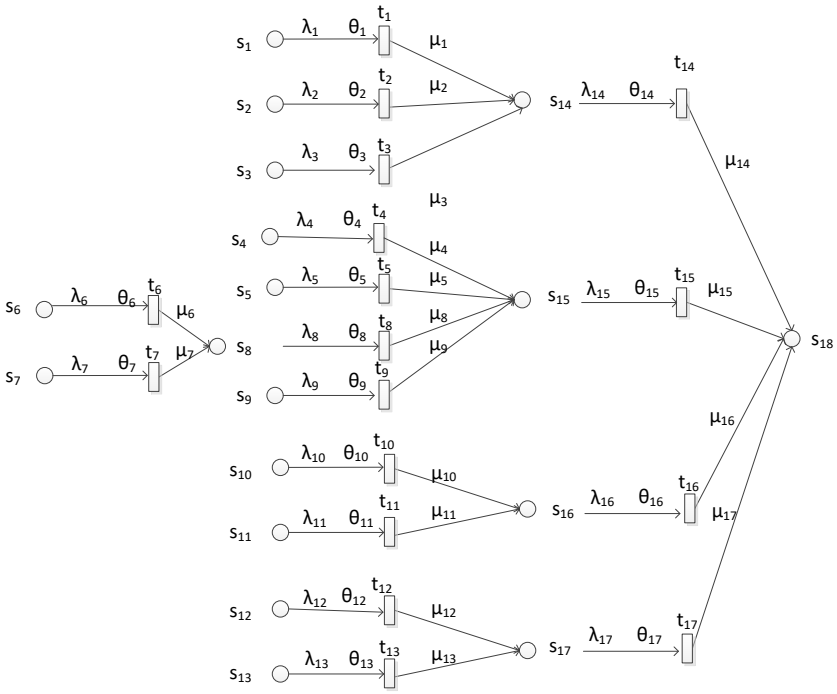

Figure 2. DFPN model

Table 2. Places of the DFPN model.

Name	Places	Name	Places	Name	Places
s_1	End-end delay	s_7	Route establishment time	s_{13}	Data tampering rate
s_2	Delivery rate	s_8	Route stability	s_{14}	Availability
s_3	Throughput	s_9	Time required for network recovery	s_{15}	Reliability
s_4	The percentage of node failures	s_{10}	Success rate of identity spoofing	s_{16}	Confidentiality
s_5	Message forwarding rate	s_{11}	Amount of data stolen	s_{17}	Integrity
s_6	Cost of routing protocols	s_{12}	Data loss rate	s_{18}	The harm level of the Ad Hoc network

In the DFPN model, each place corresponds to an indicator. According to the network characteristics and the historical data of the network operation, we can adjust the change threshold matrix $\boldsymbol{\theta}$. If we raise a change threshold, you can block the effect of small changes in the indicator on the overall evaluation.

3. Assessment process

3.1 Data initialization

Because the indicator has different volumes, standardized indicator data is required before the assessment value can be calculated. In this paper, the indicator data is standardized by triangular membership function [11]. Based on the five risk levels defined earlier, the probability of data x belonging to the i-level in the triangle member function is shown by the formula (5).

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

$$f_i(x)=\begin{cases}\dfrac{x-v_{i-1}}{v_i-v_{i-1}}, & (v_{i-1}\le x<v_i)\\ \dfrac{v_{i+1}-x}{v_{i+1}-v_i}, & (v_i\le x<v_{i+1})\\ 1, & (0\le x<v_1 \ \ or \ \ v_5\le x)\\ 0, & (\text{others})\end{cases} \tag{5}$$

In the formula (5), v_i is a value for the i-level, which generally takes the median value of the level. In the case of throughput degradation, we can set $v=[0.1,0.3,0.5,0.7,0.9]$, when throughput drops by 15%, its membership matrix is $f(x)=[0.75,0.25,0,0,0]$, and the probability of belonging to the "low" level is 0.75. The result of a fuzzy assessment is a vector that indicates the degree of membership of the data to different risk levels. If an assessment value is required, we use a weighted method to quantify the fuzzy assessment results.

3.2 Weight matrix

In the evaluation model, different metric weights result in different assessment results. We initialize the indicator weights using the fuzzy hierarchy analysis method [12] and use the weight matrix as the ρ in Petri-net.

First, according to the relative importance of the indicator, the fuzzy judgment matrix $\boldsymbol{A}$ is constructed.

$$\begin{aligned}&\boldsymbol{A}=\{a_{ij}=(0.1,0.2,...,0.9)\}\\ &\begin{cases}a_{ii}=0.5, i=1,2,...,n\\ a_{ij}+a_{ji}=1, i,j=1,2,...n\end{cases}\end{aligned} \tag{6}$$

In the formula (6), a_{ij} indicates the relative importance of factor i and factor j. If a_{ij} is 0.5, it means that two factors are equally important to the same conclusion proposition, and if a_{ij} belongs to $(0.5,0.9]$, it indicates that factor i is more important than factor j, and vice versa.

Second, based on the judgment matrix, the calculation formula for the indicator weight vector is as follows:

$$\boldsymbol{\rho}=\left\{\rho_i=\frac{\sum_{j=1}^{n}a_{ij}+\frac{n}{2}-1}{n(n-1)}\right\} \tag{7}$$

Taking the integrity attribute as an example, x_1 and x_2 represent s_{12} and s_{13}, respectively. According to the expert assessment, we build fuzzy judgment matrix $\boldsymbol{A}=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}=\begin{bmatrix}0.5 & 0.7\\ 0.3 & 0.5\end{bmatrix}$, and get the weight vector $\boldsymbol{\rho}=[0.6 \quad 0.4]$, which means that the weight of data loss is 0.6, while the weight of data tampering is 0.4.

3.3 Assessment algorithm

The algorithm is the method of calculating the value of risk, which directly affects the performance and calculation speed of the model. By the definition and structure of DFPN model, the input matrix $\boldsymbol{IN}$ and output matrix $\boldsymbol{OUT}$ can be derived. Get the data of indicators, so that we can get the initial state matrix $\boldsymbol{R}(0)$. According to the network state and expert knowledge, the thresholds of transitions $\boldsymbol{\theta}$ can be determined. Based on the information given, we put forward our assessment algorithm as follows:

Step 1: Initialization. Establish the matrixes $\boldsymbol{IN}$, $\boldsymbol{OUT}$, $\boldsymbol{R}(0)$, $\boldsymbol{\theta}$ and $\boldsymbol{\rho}$.

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

Step 2: Let $k=0$, where k represents the times of iteration.

Step 3: Compute the certainty factor of the places.

$$\boldsymbol{\lambda}=\boldsymbol{IN}^{\mathrm{T}}\times\left(\boldsymbol{R}(k)\times\boldsymbol{Q}^{\mathrm{T}}\right) \tag{8}$$

Step 4: Compare the thresholds of transitions with $\boldsymbol{\lambda}$.

$$\boldsymbol{Z}=\boldsymbol{\lambda}\oplus\boldsymbol{\theta} \tag{9}$$

Step 5: Compute the certainty factor of the transitions $\boldsymbol{\mu}$.

$$\mu_j=\frac{z_j\times\rho_j}{\sum_{i=1}^{m}out_{i(tj\bullet)}\times\rho_i\times z_i} \tag{10}$$

If $z_j=0$, then $\mu_j=0$, which means that the transition t_j won't happen. At the same time, the indicator system changes, and $\boldsymbol{\mu}$ can also be understood as a new weight matrix. For an output place $t_j\bullet$, the sum of its certainty factor is still 1, that is $\sum_{i=1}^{m}out_{i(tj\bullet)}\times\mu_i=1$.

Step 6: Compute new marking $\boldsymbol{R}(k+1)$

$$\boldsymbol{R}(k+1)=\boldsymbol{R}(k)+\boldsymbol{OUT}\times\left(\left(\boldsymbol{IN}^{T}\times\boldsymbol{R}_k\right)\otimes\boldsymbol{\mu}\right) \tag{11}$$

Step 7: If $\boldsymbol{R}(k+1)\neq\boldsymbol{R}(k)$, let $k=k+1$, go back to Step 2; otherwise, end assessing.

At the end of the assessment process, the marking of place s_{18} in $\boldsymbol{R}(k)$ is the assessment result of the security risk of Ad Hoc.

4. Simulation

4.1 Simulation setup

We used OMNeT ++ [13] to simulate cyberattacks with the network topology shown in Figure. 3. Table 1 shows values of the most important setup parameters.

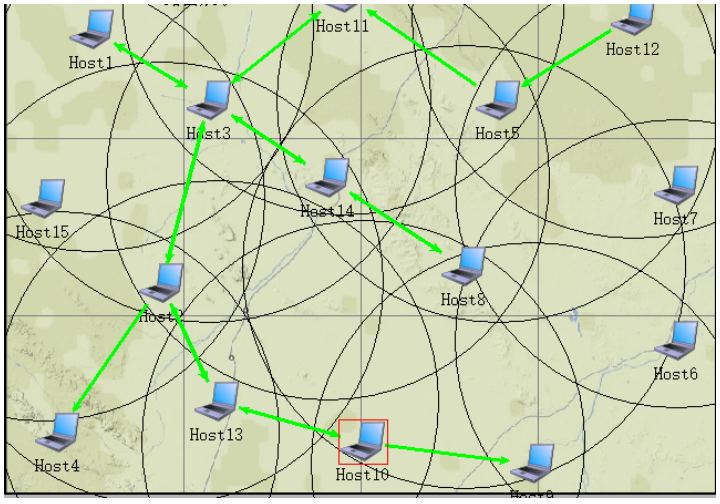

Figure 3. network topology

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

Table 3. Simulation parameter

Parameter	Value	Parameter	Value
Network area	800m×600m	Routing protocol	AODV
Number of nodes	15	Data message type	UDP
Simulation time	30s	Message size	Random in [1000B，2000B]
Propagation model	Free Space	MAC Protocol	EEE802.11b
Carrier frequency	2.4 GHz	RTS threshold	2346Bytes

4.2 Simulation scenario

To test the accuracy of the model, we simulated the Ad Hoc under different attacks. The experimental scenario is shown in Table 4. In the experiment, UDP data messages are sent from Host1 to Host8, Host8 to Host1, Host9 to Host2, Host10 to Host11, and Host12 to Host4. The node starts sending messages at a random time in interval $[0s,1s]$, with a sending interval of 0.2s.

Table 4. Simulation scenario

Scenario	Attack type	Attack node	Attack parameter
1	none		
2	Black Hole Attack	Host14	
3	RERQ flood attack	Host14	Send RERQ at 0.05s intervals
4	Shut down	Host14	
5	randomly drop packets	Host14	Drop packets at a 40% probability
6	Black Hole Attack	Host15	

4.3 Simulation results

We simulate the scenarios described in the previous section, each with a simulation time of 30s. For some metrics, the resulting figures are very similar. In such cases, we show only representative and important results in Table 5, and the real-time delivery rate under different attacks in Figure. 4.

Table 5. Simulation results

Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6
s_2(%)	99.55	19.93	74.92	98.46	81.54	80.53
s_1(ms)	17	36	89	23	21	16
s_1(104Bps)	2.87	1.53	1.90	2.81	2.02	2.13
s_5(%)	100	55.6	95.97	100	94.22	92.54
s_7(ms)	12	169	1242	89	98	11
s_6(number)	69	101	6889	107	284	76

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

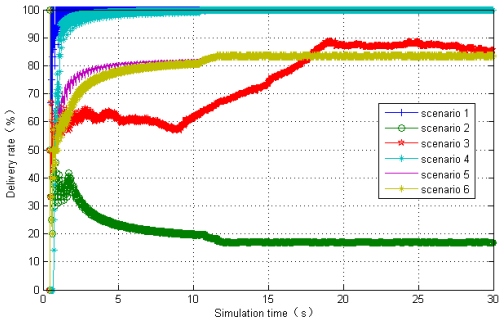

Figure 4. Real-time delivery rate

5. Assessing the results of the experiment

We use the DFPN model presented in this paper to calculate the experimental results, and then assess the security risk of the network. To understand the evaluation algorithm better, we demonstrate the evaluation process using the black hole attack of Scenario 2 as an example.

5.1 Simulation results

For ease of calculation, the change threshold θ_j ($j \in [1,17]$) is set to 0.1. According to the experimental environment and the relative importance of each indicator, the initial weight matrix can be obtained as $\boldsymbol{\rho}^{\mathrm{T}}=[0.25\ \ 0.42\ \ 0.33\ \ 0.32\ \ 0.28\ \ 0.6\ \ 0.4\ \ 0.18\ \ 0.22\ \ 0.6\ \ 0.4\ \ 0.55\ \ 0.45\ \ 0.32\ \ 0.28\ \ 0.22\ \ 0.18]$ by using the formula (7). Using formula (5), we can make fuzzy transformation of the experimental data to get the initial state matrix $\boldsymbol{R}(0)$ of the DFPN model.

According to the assessment algorithm, the first iteration of operations is carried out. Through the formula (8,9,10), we can get the certainty factor of the transitions, $\boldsymbol{\mu}^{\mathrm{T}}(1)=[0\ \ 0.56\ \ 0.44\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]$. After the first iteration, the state matrix of DFPN is updated to $\boldsymbol{R}(1)$. Finally, after 4 iteration according to the algorithm, we find that $\boldsymbol{R}(4)=\boldsymbol{R}(3)$. That is, the Ad Hoc network's security risk is assessed as $\boldsymbol{R}_{18}(3)=[\,0.1299, 0.1354, 0.3987, 0.168, 0.168]$, and the evaluation value after fuzzy quantization is 0.5218. The security risk of the Ad Hoc is "medium", for the probability of being in "medium" is highest. Moreover, for network availability attribute (s_{14}), the damage caused by this attack is high, for the probability of risk rating of "medium", "high" and "extreame" is 0.912. The assessment result is in line with the reality, because in the experiment, the black hole attack results in a large number of packet loss, which seriously affects the network service availability.

$$\boldsymbol{R}(0)=\begin{bmatrix}1.0&0&0&0&0\\0&0&0&0.5&0.5\\0&0.2&0.8&0&0\\1.0&0&0&0&0\\0&0.23&0.77&0&0\\1&0&0&0&0\\0.83&0.17&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}\quad \boldsymbol{R}(1)=\begin{bmatrix}1.0&0&0&0&0\\0&0&0&0.5&0.5\\0&0.2&0.8&0&0\\1&0&0&0&0\\0&0.23&0.77&0&0\\1&0&0&0&0\\0.83&0.17&0&0&0\\0.83&0.17&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0.088&0.352&0.28&0.28\\0&0.23&0.77&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}\quad \boldsymbol{R}(3)=\begin{bmatrix}1.0&0&0&0&0\\0&0&0&0.5&0.5\\0&0.2&0.8&0&0\\1&0&0&0&0\\0&0.23&0.77&0&0\\1&0&0&0&0\\0.83&0.17&0&0&0\\0.83&0.17&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0.088&0.352&0.28&0.28\\0.3248&0.2065&0.4687&0&0\\0&0&0&0&0\\0&0&0&0&0\\0.1299&0.1354&0.3987&0.168&0.168\end{bmatrix}$$

5.2 Comparison and analysis

At present, fuzzy AHP is widely used in risk assessment. We use the same data and the initial weight matrix to assess the result of Scenario 2 with the fuzzy AHP [14], and the assessment result of the

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

damage of the attack is $\boldsymbol{R}_{18}$=[0.2166 ,0.0426 , 0.1488,0.0672,0.0672]. The probability of this assessment result being "low" is the highest. Compared with the result of DFPN, this assessment result has a lower risk level, which cannot reflect the serious impact of black hole attack on network availability. Because, in the process of fuzzy hierarchy evaluation, indicators with small data changes still have weight (such as message transmission delay), and the evaluation system is not dynamically adjusted, so that other major affected indicators (such as message reachabilit) cannot be fully reflected.

We adjust the transition threshold value to 0, and use DFPN and fuzzy AHP to assess the attack harm. The evaluated value after fuzzy quantification is shown in Figure. 5. It can be seen that the gap of evaluation value obtained by fuzzy analytic hierarchy process is small, and the evaluation sensitivity is not as good as that of model DFPN.

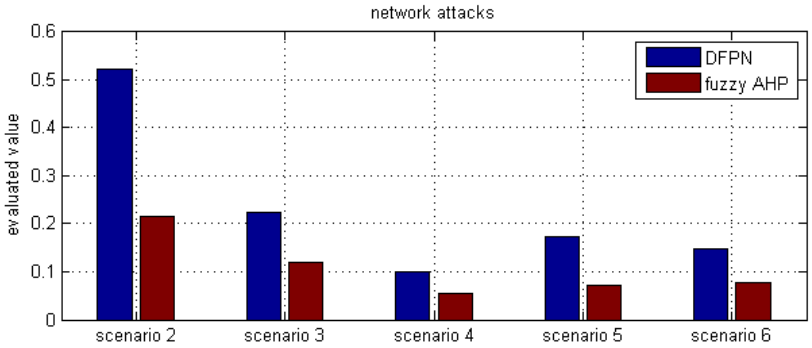

Figure 5. Evaluated value of security risk

6. Conclusion

In this paper, we propose DFPN model to assess the security risk of the Ad Hoc network, which improves the accuracy, sensitivity and adaptability of the assessment.

(1) The index system structure is dynamically adjusted to make the model more adaptable. In the DFPN model, we can set the transition threshold matrix flexibly. When the change of some index data is small or even unaffected, the corresponding transition will not be triggered, which shields the influence of this index on the final assessment result and achieves the purpose of automatic and flexible adjustment of index architecture.

(2) Dynamicly adjust the certainty factor of the transitions to make the assessment more reasonable. The certainty factor of the transitions is not fixed, but automatically adjusted according to the formula (10), so as to highlight the impact of major factor indicators on the assessment results.

References

[1] Parvinder Kaur,Dalveer Kaur,Rajiv Mahajan. Wormhole Attack Detection Technique in Mobile Ad Hoc Networks[J]. Wireless Personal Communications,2017,97(2).

[2] Revathi Venkataraman, M. Pushpalatha. Security in Ad Hoc Networks: an Extension of Dynamic Source Routing In Mobile Ad Hoc Networks[P]. Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on,2006.

[3] Z.F. LI, C.Bao, B.X. Han. Research on risk evaluation index system of tactical Internet information security[J]. Communication technology, 2013,46(05):78-80.

[4] H.Y. Fan. Effectiveness evaluation model and method of Ad Hoc tactical communication network[D]. Cheng du: University of electronic science and technology, 2013.

[5] Y. Zhang, X.B. Tan, X.L. Cui, et al. Network security situational awareness based on Markov game model[J]. Journal of software, 2011,22(03):495-508.

[6] Z. Wei, C.H. Xia, B. He, et al. A mobile Ad Hoc network survivability model modeling and simulation verification method[J]. Computer science, ,2013,36(07):1465-1474.

[7] Y. Gao, Y. Wang, H. Feng. Reliability assessment for Ad Hoc networks[J]. Radio communication technology, 2011,37(02):7-9+18.

ISSN: 2414-1895 DOI: 10.6919/ICJE.201909_5(10).0026

[8] J.F. Zhou, Genserik Reniers, L.B. Zhang. A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry[J]. Chemical Engineering Science, 174 (2017) 136–145.

[9] W.J. Li The Algorithm of Color Petri Nets Transform into the Place/ Transition Nets and its Implementation[A]. Proceedings of the 11th International Symposium on Distributed Computing and Applications to Business,Engineering & Science（DCABES 2012）[C], Wu han, 2012:5.

[10] Kasturiniva Das, Amar Taggu. A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014.

[11] Kundu, Krishan. Image Denoising Using Patch Based Processing With Fuzzy Triangular Membership Function[J]. International Journal of Computer Science Issues (IJCSI),2015,12(3).

[12] Udaya Dayanandan,Vivekanandan Kalimuthu. Software Architectural Quality Assessment Model for Security Analysis Using Fuzzy Analytical Hierarchy Process (FAHP) Method[J]. 3D Research,2018,9(3).

[13] Kaur, R.,Sangal, A.L.,Kumar, K.. Modeling and simulation of DDoS attack using Omnet++[P]. Signal Processing and Integrated Networks (SPIN), 2014 International Conference on,2014.

[14] M. Fatih Ak,Muhammet Gul. AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis[J]. Complex & Intelligent Systems,2019,5(2).