Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2014, *8*, 685-688

Open Access

Vulnerability Assessment of Information System based on Weighted Directional Graph and Complex Network Technology

Chen Keming* and Wang Chunping

Mathematics and Computer Science Institute, XinYu University, JiangXi, 338004, China

Abstract: Bayesian equilibrium algorithm model of information vulnerability assessment was established, and it had introduced the weighted directional method in the model. Then it established an information system evaluation program for complex network, and designed the procedures of vulnerability assessment. In order to verify the validity and reliability of the model, complex network test platform was built, and the network data of the test platform was monitored. It had obtained the effect of different nodes on the network vulnerability of the complex network test platform through the calculation. It had verified the role of directed weights in the analysis of complex network, which had provided the theory reference for the vulnerability assessment of information system network.

Keywords: Bayesian, complex network, credibility, directed weights, information system, vu nnnnn lnerability.

1. INTRODUCTION

In recent years, the theory of complex network has become the hotspot for information system vulnerability research. Vulnerability assessment of large information system based on the complex network theory is a research method that explores the internal mechanism of the spread of cascading failure in the research and fault simulation of the topological properties of large information system. The vulnerability of complex network is studied with the weighted directional method, and the test platform of complex network is built. In order to verify the validity of weighted directional method on the detection of complex network, the vulnerability of different nodes is detected on the testal platform, and it obtains the vulnerability assessment results of different network nodes.

2. OVERVIEW ON THE VULNERABILITY ASSESSMENT OF COMPLEX NETWORK INFORMATION SYSTEM

The traditional complex network theory based vulnerability assessment of information system generally considers the network nodes, without considering the direction or weights of the nodes, which has led to the failure of accurately measuring, so it needs to establish related model with the actual complex network to improve the reliability of vulnerability analysis.

Fig. (**1**) shows the topology model designed in the paper for the vulnerability assessment of complex network information. The actual complex network model is linked with the topological model through the model in Fig. (**1**). Using the directed weights to calculate the effect of different network nodes on the system vulnerability has improved the reliability of information analysis.

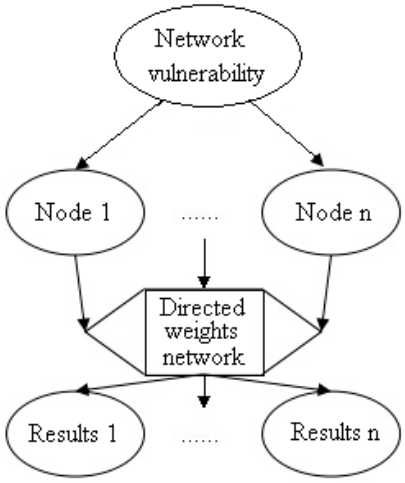

Fig. (1). Vulnerability analysis models of directed weights directional network information system.

3. VULNERABILITY ASSESSMENT MATHEMATICAL MODEL OF DIRECTED WEIGHTS INFORMATION OF COMPLEX NETWORK

For the complex network, the assessment process of information systems is relatively complex, because complex network nodes are randomly distributed. The weighted directional method is used to improve the random distribution of the nodes. Assuming that the input information of the node in network is set as P_i, the basic information of system is P_b, then the weight r of the node i is defined as that.

$$r = P_i / P_b \tag{1}$$

The weight r of the node i represents the power characteristics of node i, which has reflected the importance of this node to contain the information in the network. The

1874-110X/14

value is greater, the contained amount of information is larger. Once a fault occurs, the node will cause a huge harm to the system. Assuming that the signal source of information system has two status of the 0 and 1, the emission probability of 0 is 0.55, and the emission probability of 1 is 0.45 emission. The signal received by signal termination is 0 or 1 or "not clear", then the probability matrix can be written as following.

$$\begin{bmatrix} 0.9 & 0.05 & 0.05 \\ 0.05 & 0.85 & 0.1 \end{bmatrix} \tag{2}$$

According to the probability model, a complex stochastic network is assumed as shown in Fig. (**2**).

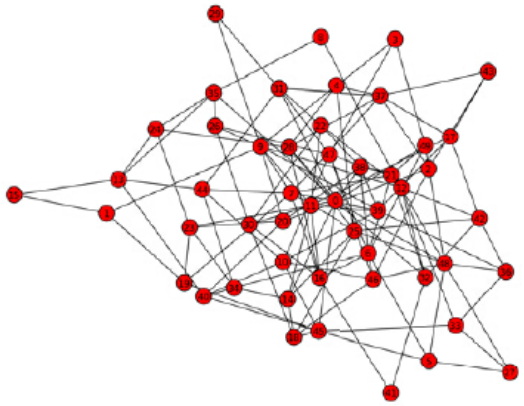

Fig. (2). Schematic diagram of complex network.

Figure 2 shows a schematic diagram of complex network in the information system. The weighted directional graph can change the random to be Have to use the full weight of the random graph can become regularized, as shown in Fig. (**3**).

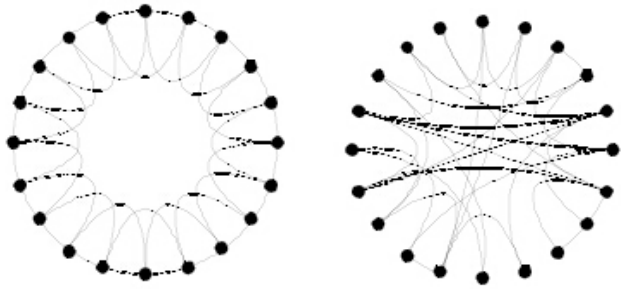

Fig. (3). Schematic diagram of network regularization.

Fig. (**3**) shows the regularized process of complex network by using directed weights. If the Bayesian formula is used to solve, the emitted signal of 0 is recorded as A, the emitted signal of 1 is recorded as $\overline{A}$, and the received signal of 1 is recorded as B, then the probability of receiving 1 is respectively as following.

$$P(A/B)=\frac{P(A)P(B/A)}{P(A)P(B/A)+P(\overline{A})P(B/\overline{A})}$$
$$P(\overline{A}/B)=\frac{P(\overline{A})P(B/\overline{A})}{P(A)P(B/A)+P(\overline{A})P(B/\overline{A})} \tag{3}$$

Assuming that the accurate rate of decision-making is set as $p(y_j|x_i)$ that shows the accuracy of information value y_j under the condition of x_i. Then the posterior Bayesian formula can be expressed as that.

$$p(y_j|x_i)=\frac{p(y_j|x_i)p(x_i)}{\sum_{i=1}^{n}p(y_j|x_i)p(x_i)} \tag{4}$$

General Procedures of Bayesian vulnerability assessment are shown as follows.

Algorithm: PBNEStrategy_generation(RA-DGM, Utility)

Input: RA-DGM, Utility

Output: PBNEStrategy

Description:

```
for(x=0;x<a;x++)
 { maxAS[x][num]="Utility[x][0]";
maxUti[0]=Utility[x][0][1][0];
maxUti[1]=Utility[x][0][1][1];
for(y=1;y<b;y++)
.....
```

4. VULNERABILITY ASSESSMENT OF COMPLEX NETWORK INFORMATION SYSTEM

The test network environment of information system has been built to verify the validity and reliability of the vulnerability assessment model and algorithm for Bayesian information system designed in the second part, and Bayesian scheme has been used to carry out the vulnerability assessment of network environment, as shown in Fig. (**4**).

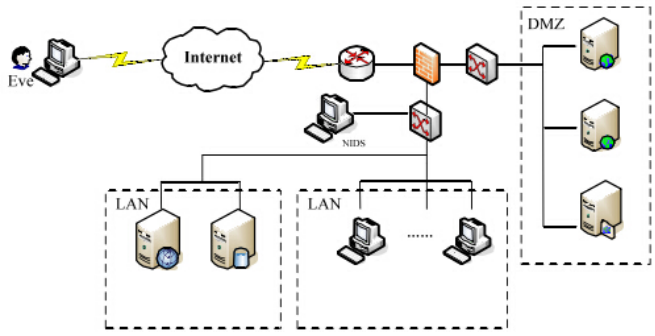

Fig. (4). Testal network of information system.

The complex network of the information system is composed of 57 network equipments. DMZ region consists of 3 servers, which can provide information exchange for the external network and local area network, and can meet the requirement of two Web servers running at the same time, to achieve a balanced configuration and to provide a SSH server. Internal network of information system is divided into two parts. One part is the server group, and the other one is the user group. The server group is made up of three servers, including backup server, data server and file server.

Table 1. Vulnerability assessment of information system.

Line Sorting	The Node i	The Node j	The Number of Attacks	Attack Probability
1	5	8	1	0.001
2	12	11	2	0.002
3	9	6	1	0.001
4	15	13	3	0.003
5	17	9	1	0.001

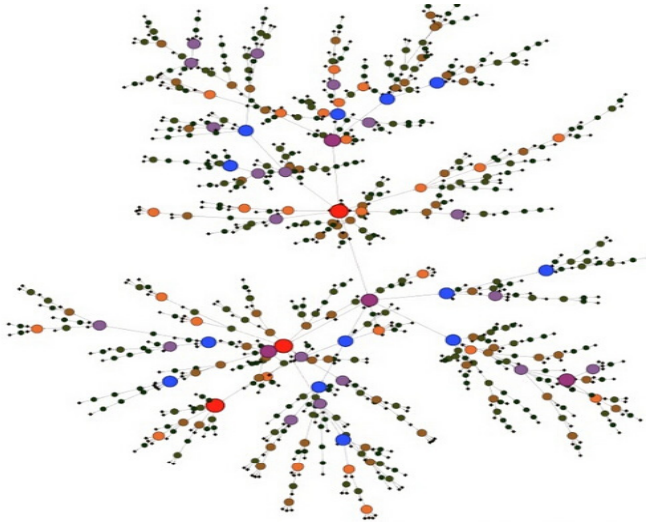

Fig. (5). Complex network detection results nephogram.

Fig. (**5**) shows the detection results of complex network in the information system. As shown in Fig. (**5**), from the red to the blue, it represents the degree of network vulnerability, in which the red represents the highest vulnerability, and the blue represents the lowest vulnerability. The detection results are deployed in the form of curves, as shown in Fig. (**6**).

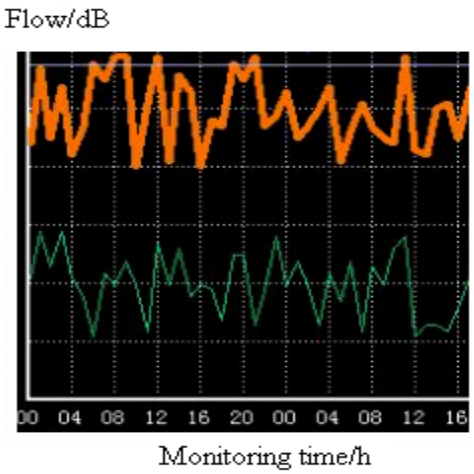

Fig. (6). Vulnerability detected curve of information system.

Fig. (**6**) shows the detected curve of information vulnerability over the time changing. In order to visually display the detected results, the results of curve is listed as shown in Table **1**.

Table **1** shows the vulnerability detected results of complex network in the information system. The detection circuit is divided into five parts, including two kinds of nodes of i and j. The detection results show that the highest number of attacks is in the line3 with highest attack probability and higher vulnerability. The vulnerability of line 1, 3 and 5 is relatively reduced, and the network security performance of information system is good.

CONCLUSION

In this paper, the assessment model of the vulnerability for information system is improved by using Bayesian equilibrium algorithm. The mathematical evaluation model of combined complex network information systems is established through the combination of weighted directional algorithm, and the algorithmic routine of network vulnerability assessment is designed. In order to verify the validity and reliability of the model and the algorithm, the test platform of complex network is built, and the vulnerability of network is detected with the weighted directional method, which has got the probability distribution nephogram of network vulnerability and the curve of network performance with time changing. At the last, the effect of different nodes of the network on the vulnerability of system is calculated with directed weights. And the results shown that the attacked number of different nodes and the attacked probability have improved the credibility of information analysis, which has provided theory reference for the research of information system vulnerability.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Chunzi Wang, Guangqiu Huang. Network attack-defense situation awareness based on dynamic game with incomplete information. Computer Engineering, Vol. 36 (20),(2010), p.125-127.

[2] Chunzi Wang, Guangqiu Huang. Network attack-defense strategy based on rough Bayesian game. Journal of computer applications, Vol. 31 (3), (2011), p.784-789.

[3] Xiaogang Chen, Ke Sun, Jiayi Cao. Structural vulnerability analysis of large power grid based on complex network theory. Transactions of China electrotechnical society, Vol. 22 (10), (2007), p.138-144.

[4] Yaonian Liu, Qian Mu, Kefei Kang, Yibin Lin, Jing Yu, Ying Wang. Identification of vulnerable lines in power grid based on the weighted reactance betweenness index. Power system protection and control, Vol. 39 (23), (2011), p.89-93.

[5] Yang Zheng, Wenying Liu, Zhiwei Wen, *et al.* A real-time searching system for cascading failure of power grids based on small-world network. Power system technology, Vol.34 (7), (2010), p.58-63.

[6] Ming Ding, Pingping Han. Vulnerability assessment to small-world power grids based on weighted topological model. Proceedings of the CSEE, Vol. 28 (10), (2008), p.20-25.

[7] Guangqiu Huang, Jincheng Wang. Consistent varying-weight fuzzy Petri net attack model based on both-branch fuzzy sets. Journal of computer applications, Vol. 29 (2), (2009), p.529-533.

[8] Meng Qian, Handong Mao, Li Yao. Network security analysis model based on logic exploitation graph. Computer Engineering, Vol. 35 (9), (2009), p.147-149.

[9] Sisi Chen, Yifeng Lian, Wei Jia. Assessment methods of the vulnerability states based on Bayesian network. Journal of Graduate University of Chinese Academy of Sciences, Vol. 25 (5), (2008), p.639-647.

[10] Haixia Zhang, Purui Su, Dengguo Feng. A network security analysis model based on the increase in attack ability. Journal of computer research and development, Vol. 44 (12), (2007), p.2012-2019.

[11] Weiming Li, Jie Lei, Jing Dong. An optimized method for real-time network security quantification. Chinese journal of computer, Vol. 32 (4), (2009), p.794-803.

[12] Mixia Liu, Yuqing Zhang, Yi Hong. Modeling and analysis of network survivability based on fuzzy inference. Journal of communications, Vol. 30 (1), (2009), p.32-37.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014