Research on Security Situation Prediction of Equipment Support Information Network Based on Bayesian Network

Xi Li and Yu Lu
Information Engineering Department
Army Engineering University
Shijiazhuang 050003, China
lixi7780@aliyun.com
ylu@sina.vip.com

Sen Liu
The 54th Research Institute of CETC
Shijiazhuang 050200, China
ls_box1@126.com

Abstract—**According to the characteristics of equipment support information network, this paper proposes a network security situation prediction model based on attack graph and Bayesian network. This paper proposes a global attack graph generation algorithm based on the forward search algorithm, and proposes an optimization scheme to solve the attack loop problem. A method for calculating the node probability of attack graph is proposed by using Bayesian network. The experimental results show that the model can accurately predict the security situation of the equipment support information network. The calculation results are more objective and practical because of adding the equipment weight information.**

Keywords-equipment support information network; situation prediction; Bayesian network; attack graph

I. INTRODUCTION

Equipment support information network is the foundation to realize the information construction of equipment support, and it is a new network developed after the equipment support information resource has become an important strategic resource in the information age[1]. The security of the equipment support information network concerns the smooth operating of the equipment support business, and even affects the whole situation of the war. If we can accurately predict the security situation of the network and provide reliable security recommendations for network managers, it will be of great significance to enhance the combat effectiveness of the troops.

II. EQUIPMENT SUPPORT INFORMATION NETWORK SECURITY SITUATION PREDICTION MODEL

The security situation prediction model of equipment support information network proposed in this paper is based on attack graph and Bayesian network theory, as shown in Fig. 1. Attack graph describes the scene that the attackers use the vulnerabilities of the network and their dependencies to invade the target network. It shows the attacker's attack modes and paths. In 1998, Phillips et al proposed a network vulnerability analysis method based on state attack graph[2-4], which was used to solve the evaluation problem of network vulnerability; Schneier et al Proposed a security analysis method based on attack tree[5]; Clark et al proposed a qualitative and quantitative network security assessment method based on attack tree model[6]; Dewri used attack tree model to solve network security reinforcement problem[7]; On the basis of attack graph modeling, Cheng et al[8] studied the CVSS (Common Vulnerability Scoring System)[9], analyzed the relationship between CVSS vulnerability score and CVSS risk component, and described the association between vulnerabilities; Nwokedi et al[10] proposed a set of evaluation index based on attack path, and gave a method to quantify network security risk by using the combination of these indexes; Zeng et al[11] proposed an attack graph generation algorithm through the uncertain graph model. The algorithm starts from the attacker's target and generates the attack graph by reverse simulation.

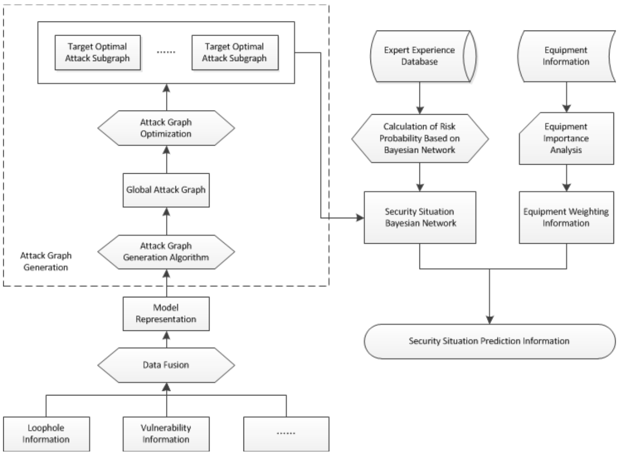

Target Optimal Attack Subgraph
......
Target Optimal Attack Subgraph
Attack Graph Optimization
Global Attack Graph
Attack Graph Generation Algorithm
Attack Graph Generation
Model Representation
Data Fusion
Loophole Information
Vulnerability Information
......
Expert Experience Database
Equipment Information
Calculation of Risk Probability Based on Bayesian Network
Equipment Importance Analysis
Security Situation Bayesian Network
Equipment Weighting Information
Security Situation Prediction Information

Figure 1. Security situation prediction model of equipment support information network

Bayesian network, also called probability belief network, is an effective tool for analysis and reasoning of uncertain events based on probability theory and graph theory[12]; Jia et al[13] proposed a method based on Bayesian network approximate reasoning to quantify the vulnerabilities of the network. The

978-1-5386-0497-7/17/$31.00 ©2017 IEEE

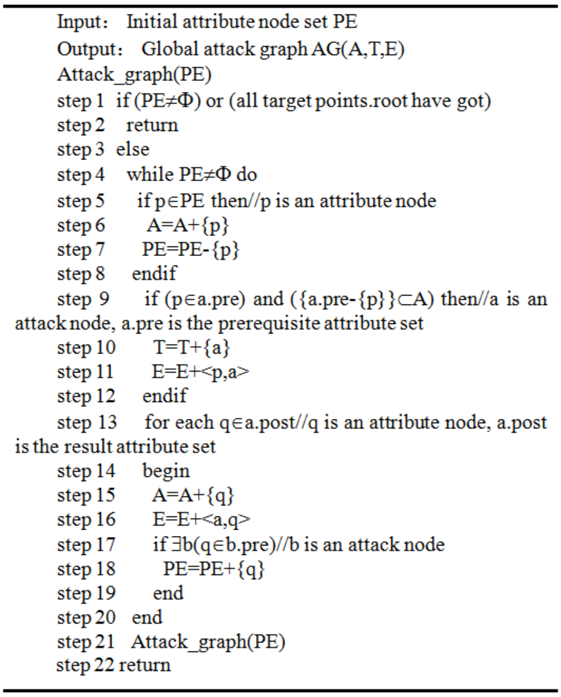
method can reflect the implicit interaction relationship between the known vulnerabilities of the network; Gao et al[14] proposed a dynamic risk assessment model based on Bayesian attack graph. Combining the real-time attack events observed by IDS, the Bayesian reasoning method is used to update the posterior probability of the single step attack behavior, so as to achieve the overall security evaluation of the target network; Wen et al[15] proposed a network security situation awareness method based on multi-source and multi-level information fusion. This method can fuse heterogeneous information quickly, perceive network security situation from all aspects, and provide a macroscopic view of network security status.

In this model, firstly, the loophole information, topology information and vulnerability information of the target network are collected and summarized by vulnerability scanning and analysis tool; The basic information is fused to form a kind of model representation; The attack graph generation algorithm is used to generate the global attack graph from the model data; Because of the existence of loops and other violation of monotonicity assumption[16] in global attack graphs, it is necessary to optimize different attack targets to form different target optimal attack subgraph; The accuracy of prediction using Bayesian networks depends on the rationality of the parameters, therefore, we need to use the expert experience database (such as the United States national vulnerability database, NVD) to calculate the risk probability. Because of the particularity of equipment support information network, it is necessary to evaluate the importance of different network equipment, therefore, the equipment weight information is added to the model; Using Bayesian network and network equipment weight information, we can predict the security situation of equipment support information network.

III. Attack Graph Generation

A. *Global Attack Graph Generation Algorithm*

The global attack graph depicts all the attack paths that can be used by attackers. In order to evaluate and predict the network security situation, we need to establish a global attack graph first. Global attack graph was originally constructed manually by domain experts, but this approach is inefficient for large and medium networks. At present, attack graph automatic generation algorithms are divided into two categories: forward search algorithm and backward search algorithm. The principle of forward search algorithm is that the attackers use the initial vulnerabilities and other elements of security information to search all possible attack behaviors and produce the corresponding attribute nodes and attack nodes until no new attacks are available. The principle of backward search algorithm is that starting from the target node, tracing back to the initial node, which can produce all the attack paths from the initial node to the target node . The algorithm ignores attacks that have nothing to do with attacking targets. The global attack graph generation algorithm designed in this paper adopts the idea of forward search algorithm, and the algorithm is as follows:



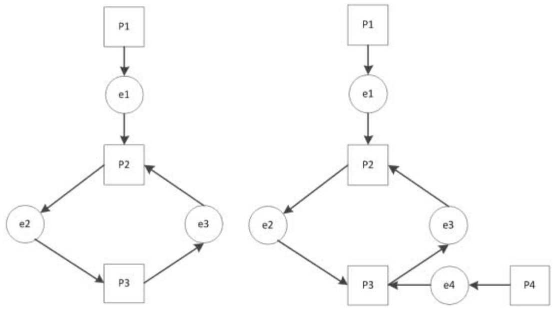
```
Input:  Initial attribute node set PE
Output:  Global attack graph AG(A,T,E)
Attack_graph(PE)
step 1  if (PE≠Φ) or (all target points.root have got)
step 2    return
step 3  else
step 4    while PE≠Φ do
step 5      if p∈PE then//p is an attribute node
step 6        A=A+{p}
step 7        PE=PE-{p}
step 8      endif
step 9      if (p∈a.pre) and ({a.pre-{p}}⊂A) then//a is an
attack node, a.pre is the prerequisite attribute set
step 10        T=T+{a}
step 11        E=E+<p,a>
step 12      endif
step 13      for each q∈a.post//q is an attribute node, a.post
is the result attribute set
step 14      begin
step 15        A=A+{q}
step 16        E=E+<a,q>
step 17        if ∃b(q∈b.pre)//b is an attack node
step 18          PE=PE+{q}
step 19        end
step 20    end
step 21    Attack_graph(PE)
step 22 return
```

Figure 2. Global Attack Graph Generation Algorithm

The core idea of the algorithm is to generate the global attack graph AG by recursively calling the Attack_graph() function. Algorithm step 1: setting the condition of function recursive completion, that is, the attribute node set PE is empty or the root permissions of all target nodes are obtained. The former, after a series of attacks, no more new attributes can be used by subsequent attacks, then the recursion is complete and the resulting attack graph is the global attack graph; The latter, if the root authority of all target have been gotten, which means getting maximum control of the entire network, there is no need to carry out subsequent attacks, recursion is completed. It can also avoid the loop attack to a certain extent. Step4-20: it is a loop, and the condition of ending the loop is whether the current attribute nodes are fully exploited by the attack nodes. Step 9-12: this is used to generate the attack node set T and the edge set E, where they are the edges of the prerequisite attribute nodes and the attack nodes. Step 13-16: this is used to supply the attribute node set A and the edge set E, where the added attribute node are the result attribute nodes, and the increased edges are the edges of the attack node and the result attribute node. Step 17-19: this is used to generate a new set of node attributes, the judgment is needed here whether the resulting attribute nodes can be applied by subsequent attacks, if they can, then added them to the collection as input parameters for the next round of recursion.

B. *Attack graph loop problem*

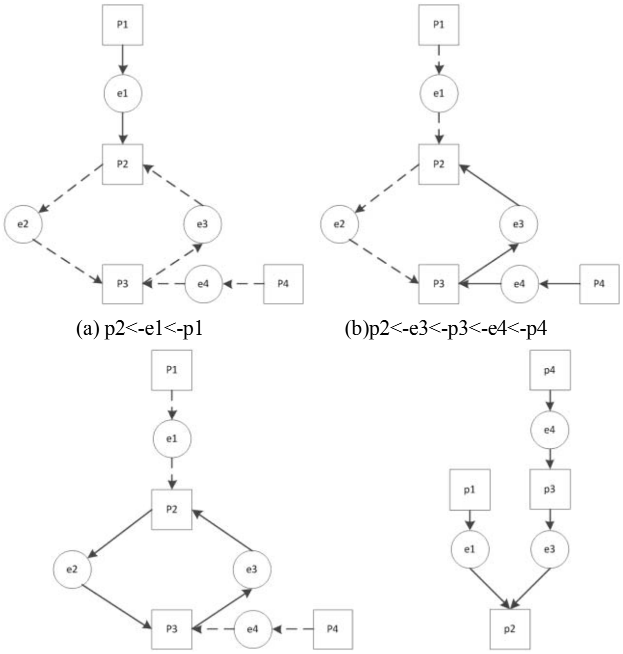
The loops may appear during the generation of the global attack graph, as shown in Fig. 3. In Fig. 3 (a), attribute nodes p2 and p3 are the prerequisite attributes for attack nodes a2 and a3. At the same time, they are the result attributes of e3 and e2, then an attack loop is formed. In practice, it is impossible for an attacker to use p2 to make e2 attack after the e3 attack, which is neither reasonable nor inconsistent with the monotonicity assumption. So the edge of e3 to p2 should be removed. In Fig. 3 (b), although there is a loop similar to the loop in Fig. 3 (a), the edge of e3 to p2 cannot be removed because it will result in the lack of attack path from e4 to e2 attack.



(a)loop 1 (b)loop 2

Figure 3. Attack loop

C. *Attack graph optimization*



(a) p2<-e1<-p1 (b)p2<-e3<-p3<-e4<-p4

(c) p2<-e3<-p3<-e2<-p2 (d)the optimal attack sub-graph of target p2

Figure 4. Attack graph optimization

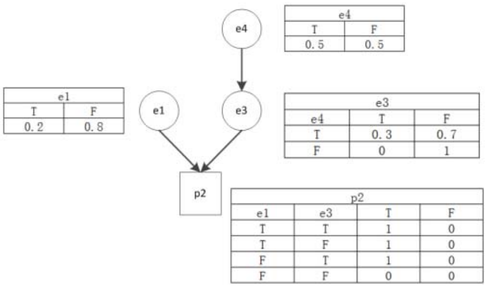
The attack loops are disadvantageous to the evaluation of network security situation, which will cause the infinite loop of attack paths, the damage value is accumulated continuously, and the judgment of network security situation is affected. The loop in Fig. 3(a) can be deleted, but the loop in Fig. 3(b) cannot be, so for the global attack graph AG, the loop cannot be simply deleted. In order to realize the optimization of global attack graph, this paper uses for reference the idea of document [17]. The optimized attack subgraph is generated by establishing the target node and reverse searching. The tracking set is introduced in the process of producing target optimal attack subgraph. The set records all the attribute nodes that have been generated by the current path. When the attribute node to be generated has been in the tracking set, it indicates that the loop will be generated and the attack behavior is invalid. In this way, the loop in Fig. 3 can be effectively avoided. For example, in Fig. 3(b), set p2 as the target node. Starting from p2, we can get three attack paths in reverse searching, as shown in Fig. 4. The solid line in the figure is the target attack path. According to the optimization principle, Fig. 4(c) is an invalid path, so for target node p2, the two paths p2<-e1<-p1 and p2<-e3<-p3<-e4<-p4 are available, as shown in Fig. 4(a) and (b). As a result, the optimal attack subgraph for the target node p2 can be generated, as shown in Fig. 4 (d). The algorithm is as follows:

```
    Input: target node d, child node of d dc, global attack
graph AG(A,T,E)
    Output: target optimal attack subgraph OSAG(A',T',E')
    Sub_attack_graph (d, dc, AG, OSAG)
    step 1  if d∈A then
    step 2      if A'≠Φ then
    step 3          E'=E'+{<d, dc>}
    step 4      if d∈A' then
    step 5          return
    step 6      else
    step 7          A'=A'+{d}
    step 8      AR=AR+{d}  //AR is the tracking set
    step 9      for each p∈d.parent
    step 10         Sub_attack_graph (p, d, AG, OSAG)
    step 11  if (d∈T) and (d.parent∩AR=Φ) then
    step 12     T'=T'+{d}
    step 13     E'=E'+{<d, dc>}
    step 14     for each q∈d.parent
    step 15         Sub_attack_graph (q, d, AG, OSAG)
    step 16  return
```

Figure 5. Attack graph optimization algorithm

IV. JOINT PROBABILITY CALCULATION BASED ON BAYESIAN NETWORKS

In attack graph, the realization of attack is the result of joint action of multiple attack nodes. These attack nodes do not exist in isolation, but depend on each other. Therefore, joint probability should be considered to calculate the probability of target generation.



e4	
T	F
0. 5	0. 5

e1	
T	F
0. 2	0. 8

e3		
e4	T	F
T	0. 3	0. 7
F	0	1

p2			
e1	e3	T	F
T	T	1	0
T	F	1	0
F	T	1	0
F	F	0	0

Figure 6. Schematic diagram of Bayesian network

According to the definition of attack graph, the non initial attribute nodes are the result nodes of attack. Under the premise of successful attack, the realization probability of direct followup attribute node is 100%. In order to facilitate the calculation of target occurrence probability, the optimal attack subgraph is simplified as an attack dependency graph, that is, omitting all attribute nodes. The attack dependency graph of Fig. 4(d) is shown in Fig. 6.

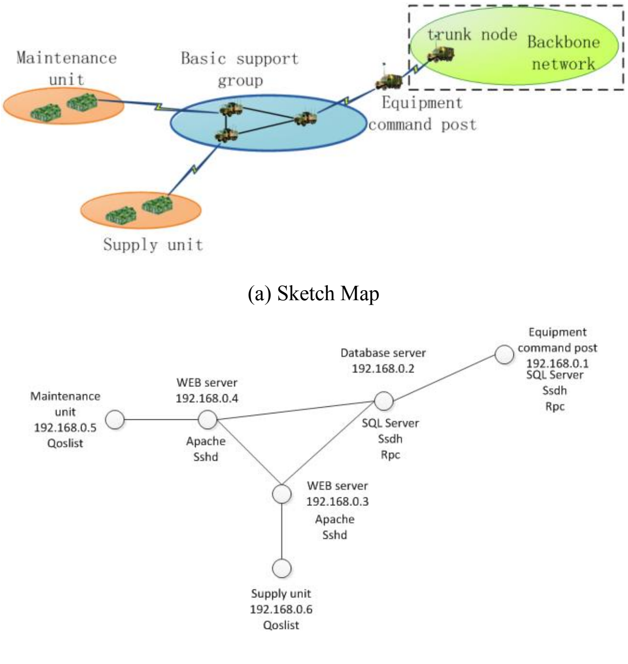
Set the realization probabilities of e1, e4, e3 are $P(e1)=0.2$, $P(e4)=0.5$, $P(e3|e4{=}T)=0.3$, then the CPT (Condition Probability Tables) of each node can be obtained. The resulting Bayesian network is shown in Fig. 6. Then, the probability of the target p2 can be calculated.

$$\begin{aligned}P(p2) &= \sum P(p2,e1,e3)\\ &= P(p2,e1,e3)+P(p2,e1,\overline{e3})\\ &\quad +P(p2,\overline{e1},e3)+P(p2,\overline{e1},\overline{e3})\\ &= P(p2|e1,e3)P(e1)P(e3)+P(p2|e1,\overline{e3})P(e1)P(\overline{e3})\\ &\quad +P(p2|\overline{e1},e3)P(\overline{e1})P(e3)+P(p2|\overline{e1},\overline{e3})P(\overline{e1})P(\overline{e3})\\ &= 1\times0.2\times0.15+1\times0.2\times0.85+1\times0.8\times0.15+0\times0.8\times0.85\\ &= 0.32\end{aligned} \tag{1}$$

□ $P(\overline{p2})=1-P(p2)=1-0.32=0.68$ □ □ □ □(2)

V. EXPERIMENT AND ANALYSIS

According to the prediction model proposed in this paper, the prediction information of the network security situation can be obtained by the realization probability of the target node and resource weight information. In order to illustrate this process better, this paper simulates a small scale equipment support information network, as shown in Fig. 7. The vulnerabilities information of each node are shown in Fig. 7 (b).



(a) Sketch Map

(b)Topology

Figure 7. Example of equipment support information network

The optimized global attack graph is generated by using the algorithm designed in this paper, as shown in Fig. 8. The semantics of each node are shown in TABLE I. Vulnerability information standard reference NVD.

The basic probability of the attack node in the attack graph is obtained by querying the Access Complexity value in the NVD. This value is provided by the CVSS. The cumulative probabilities of attack nodes can be calculated by using Bayesian networks, and the results are shown in TABLE II.

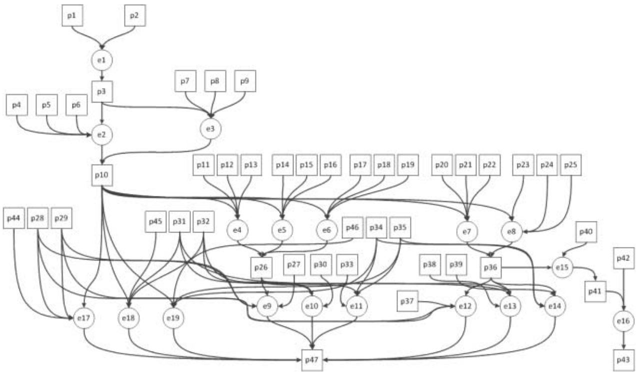


Figure 8. Global attack graph

TABLE I. SEMANTICS OF EACH NODE IN ATTACK GRAPH

ID	semantics	ID	semantics
p1	hasPrivilege(192.168.0.5,user)	p34	netService(192.168.0.1,RPC,TCP,135)
p2	vulnerability(192.168.0.5,Qoslist,CVE-2010-0961)	p35	vulnerability(192.168.0.1,RPC,CVE-2010-1039)
p3	hasPrivilege(192.168.0.5,root)	p36	hasPrivilege(192.168.0.3,root)
p4	netConnection(202.103.0.5,192.168.0.4, TCP,80)	p37	netConnection(202.103.0.2,192.168.0.1,TCP,22)
p5	netService(192.168.0.4,Apache,TCP,80)	p38	netConnection (192.168.0.2,192.168.0.1,TCP,1433)
p6	vulnerability(192.168.0.4,Apache,CVE-2010-2068)	p39	netConnection (192.168.0.2,192.168.0.1,TCP,135)
p7	netConnection (202.103.96.31,192.168.0.1,TCP,22)	p40	trust(192.168.0.3,192.168.0.6)
p8	netService(192.168.0.1,Sshd,TCP,22)	p41	hasPrivilege(192.168.0.6,user)
p9	vulnerability(192.168.0.1,Sshd,CVE-2011-2245)	p42	vulnerability(192.168.0.6,Qoslist,CVE-2010-0961)
p10	hasPrivilege(192.168.0.4,root)	p43	hasPrivilege(192.168.0.6,root)
p11	netConnection (192.168.0.4,192.168.0.2,TCP,1433)	p44	netConnection(202.103.0.2,192.168.0.1,TCP,22)
p12	netService(192.168.0.2,SQLServer,TCP, 1433)	p45	netConnection(192.168.0.2,192.168.0.1,TCP,1433)
p13	vulnerability(192.168.0.2,SQLServer,CVE-2011-0448)	p46	netConnection(192.168.0.2,192.168.0.1,TCP,135)
p14	netConnection (192.168.0.4,192.168.0.2,TCP,135)	p47	hasPrivilege(192.168.0.1,root)
p15	netService(192.168.0.2,RPC,TCP,135)	e1	L_BufferOverflow(192.168.0.5,Qoslist)
p16	vulnerability(192.168.0.2,RPC,CVE-2010-1039)	e2	R_BufferOverflow(192.168.0.5,192.168.0.4,Apache)
p17	netConnection (202.103.0.4,192.168.0.2,TCP,22)	e3	R_BufferOverflow(192.168.0.5,192.168.0.4,Sshd)
p18	netService(192.168.0.2,Sshd,TCP,22)	e4	R_BufferOverflow(192.168.0.4,192.168.0.2,SQL Server)
p19	vulnerability(192.168.0.2,Sshd,CVE-2011-2245)	e5	R_BufferOverflow(192.168.0.4,192.168.0.2,RPC)
p20	netConnection(202.103.0.4,192.168.0.3, TCP,80)	e6	R_BufferOverflow(192.168.0.4,192.168.0.2,Sshd)
p21	netService(192.168.0.3,Apache,TCP,80)	e7	R_BufferOverflow(192.168.0.4,192.168.0.3,Apache)
p22	vulnerability(192.168.0.3,Apache,CVE-2010-2068)	e8	R_BufferOverflow(192.168.0.4,192.168.0.3,Sshd)
p23	netConnection (202.103.0.4,192.168.0.4,TCP,22)	e9	R_BufferOverflow(192.168.0.2,192.168.0.1,Sshd)
p24	netService(192.168.0.4,Sshd,TCP,22)	e10	R_BufferOverflow(192.168.0.2,192.168.0.1,SQL Server)
p25	vulnerability(192.168.0.4,Sshd,CVE-2011-2245)	e11	R_BufferOverflow(192.168.0.2,192.168.0.1,RPC)
p26	hasPrivilege(192.168.0.2,root)	e12	R_BufferOverflow(192.168.0.3,192.168.0.1,Sshd)
p27	netConnection(202.103.0.2,192.168.0.1, TCP,22)	e13	R_BufferOverflow(192.168.0.3,192.168.0.1,SQL Server)
p28	netService(192.168.0.1,Sshd,TCP,22)	e14	R_BufferOverflow(192.168.0.3,192.168.0.1,RPC)
p29	vulnerability(192.168.0.1,Sshd,CVE-	e15	Trust_escalation(192.168.0.3,192.168.0.6)

	2011-2245)		
p30	netConnection (192.168.0.2,192.168.0.1,TCP,1433)	e16	L_BufferOverflow(192.168.0.6,Qoslist)
p31	netService(192.168.0.1,SQLServer,TCP, 1433)	e17	R_BufferOverflow(192.168.0.4,192.168.0. 1,Sshd)
p32	vulnerability(192.168.0.1,SQLServer,C VE-2011-0448)	e18	R_BufferOverflow(192.168.0.4,192.168.0. 1,SQL Server)
p33	netConnection (192.168.0.2,192.168.0.1,TCP,135)	e19	R_BufferOverflow(192.168.0.4,192.168.0. 1,RPC)

Using the results of TABLE II ,the node relations in Fig. 8 and the node semantics in TABLE I, we can get the root authority probability of each node in the experiment network. Combined with the equipment weight of each node, the risk value of each node and the security situation value of the whole network can be obtained, as shown in TABLE III. Among them, the equipment weight information is determined by industry experts according to the business and storage data of different nodes.

TABLE II. SUCCESS PROBABILITIES OF ATTACK NODES

attack node	basic probability	cumulative probability	attack node	basic probability	cumulative probability
e1	0.71	0.7100	e11	0.71	0.6389
e2	0.71	0.5041	e12	0.71	0.5567
e3	0.71	0.5041	e13	0.71	0.5567
e4	0.71	0.5354	e14	0.71	0.5567
e5	0.71	0.5354	e15	1.00	0.5567
e6	0.71	0.5354	e16	0.71	0.3953
e7	0.71	0.5354	e17	0.71	0.5354
e8	0.71	0.5354	e18	0.71	0.5354
e9	0.71	0.6389	e19	0.71	0.5354
e10	0.71	0.6389			

TABLE III. NETWORK EQUIPMENTS RISK AND SECURITY SITUATION

node	equipment weight	root probability	risk value	network security situation value
192.168.0.5	1	0.7100	0.71	16.18
192.168.0.4	3	0.7541	2.26	
192.168.0.2	5	0.8997	4.50	
192.168.0.3	3	0.7842	2.35	
192.168.0.1	6	0.9936	5.96	
192.168.0.6	1	0.3953	0.40	

VI. CONCLUSION

Experiments show that the equipment support information network security situation can be predicted by using the model proposed in this paper. The global attack graph can describe all kinds of attacks, preconditions and attack results. Because of the particularity of the equipment support information network, the equipment weights of the network need to be manually set, which may affect the calculation accuracy. However, after adding weights information, it can reflect the importance of different nodes, and the network security situation value has more practical significance and practical value.

REFERENCES

[1] YANG Xueqiang, HUANG Jun. Equipment Support Information Construction Introduction. Beijing: National Defense Industry Press, 2011, pp.145-146.

[2] C Phillips, L P Swiler. Agraph-based system for network vulnerability analysis. Proeeedings of the 1998 workshop on New security Paradigms, Charlottesville, Virginia, UnitedStates, 1998, pp.71-79.

[3] L P Swiler, C Phillips, T Gaylor. A Graph-Based Network Vulnerability Analysis System. Sandia National Laboratories, Albuquerque, New Mexico and Livermore, California, 1998.

[4] L P Swiler, C Phillips, D Ellis, et cl. Computer-Attack Graph Generation Tool. Proceedings: DARPA Information Survivability Conference and Exposition, Anaheim, California, 2001, pp.1307–1321.

[5] Schnerier B. Attack trees-modeling security threats. Dr Dobb, S Journal, vol. 12 ,1999, pp.21-29.

[6] K Clark, S Tyree, J Dawkins, et al. Qualitative and Quantitative Analytical Techniques for Network Security Assessment. Proc 2004 Information Assurance Workshop of the 5th Annual IEEE SMC, Hawaii, USA, IEEE Press, 2004,pp.321-328.

[7] R Dewri, N PoolsapPasit, I Ray, et al. Optimal Security Hardening Using Multi-objective Optimization on Attack Tree Models of Networks. Proc the 14th ACM Conference on Computer and Communications Security(CCS.07). Alexandria, Virginia, USA, ACM Press, 2007,pp.204-213.

[8] Cheng Pengsu, Wang Lingyu, Jajodia S, et al. Aggregating CVSS base scores for semantics-rich network security metrics.// Proc of the 2012 International Symposium on Reliable Distributed Systems, New Jersey: IEEE Press, 2012, pp.31-40.

[9] FIRST. Common Vulnerability Scoring System v3.0: Specification Document. https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf.

[10] Nwokedi Idika, Bharat Bhargava. Extending attack graph based security metrics and aggregating their application. IEEE Transactions on Dependable and Secure Computing, vol. 9, 2012, pp.75-85

[11] ZENG Saiwen, WEN Zhonghua, DAI Liangwei, et al. Analysis of Network Security Based on Uncertain Attack Graph Path. Computer Science, vol. 44 ,2017, pp.351-355.

[12] SHI Zhifu, ZHANG An. Bayesian Network Theory and Its Application in Military System. Beijing: National Defense Industry Press, 2012.

[13] JIA Wei, LIAN Yi-feng, FENG Deng-guo, et al. Bayesian Network Approximate Reasoning Based Method for Network Vulnerabilities Evaluation. Journal on Communications, vol. 29 ,2008, pp.191-198.

[14] GAONi, GAOLing1, HEYiyue1, et al. Dynamic Security Risk Assessment Model Based on Bayesian Attack Graph. Journal of SICHUAN University (Engineering Science Edition), vol. 48, 2016, pp.111-118.

[15] WEN Zhicheng, CHEN Zhigang, DENG Xiaoheng, et al. Network Security Situation Awareness Method Based on Multi-Source and Multi-Level Information Fusion. JOURNAL OF SHANGHAI JIAO TONG UNIVERSITY, vol. 49, 2015, pp.1144-1152.

[16] P Ammann, D Wijesekera, S Kaushik. Scalable, Graph-Based Network Vulnerability Analysis. Proceedings of the 9th ACM Conference on Computer and Communication Security, NewYork: ACM Press, 2002, pp.217-224.

[17] YAN Feng. The Technology Research of Network Security Risk Awareness Based on Attack Graphs. JILIN University, 2014.