International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.161-172
http://dx.doi.org/10.14257/ijsia.2014.8.6.15

The Network Attack Model based on Hierarchical Expanded Stochastic Petri Net

Yongfu Zhou

Heyuan Polytechnic,
HeYuan 517000, china,
afuyours@126.com

Abstract

In the paper, a global network attack model based on Hierarchical Expanded Stochastic Petri Net (HESPN) is presented. The model is suitable for the cooperative attack simulation and can describe both macroscopic network attack and microcosmic host attack synthetically. The dissertation represents model generation algorithm and digs for potential attack relationships among hosts according to the definition of rough path. Then utilize ant colony algorithm to find k-critical vulnerable paths after expanding sub Petri net. By analyzing rough paths and accurate paths synthetically, a network risk evaluation method is proposed.

Keywords: *Network Security, Attack Model, Threat Evaluation, Attack and Defense Strategy, Object Petri net*

1. Introduction

Aiming at the existing problems in the network attack model, this paper puts forward the whole network attack model of a Hierarchical Expanded Stochastic Petri Net (HESPN). It is more suitable for modeling large complex network [1-2]. Compared with the attack graph model, the model has the following advantages:

(1) To have more strong attack process and network state description ability. Coordinated attacks on distributed system can be modeled; articulate weaknesses use complex logic and timing relationships of host attack

(2) Extended the definition of random Transitions in SPN, so that the model can reflect the attack cost and attack benefit comprehensive influence on the attacker decision.

(3) From the fundamental solution is to the problem of exponential growth in the attack graph state. In the guarantee to host leak state comprehensive description of the situation, the design of the network object and hierarchical structure can effectively control the state of the network scale

(4) Generation model is more convenient. Generation of network attack path need not search the network state, only need to the attack rule base in the known state domain to add attack Transitions.

(5) The model generation algorithm in simulation of multi target attack time and space complexity is superior to the degree, it can generate an integrated Petri net model for multiple target attack, save the target to attack rules library search time matching.

In this paper proposed the whole network attack modeling method to aim to help the defenders grasp each kind of aggressive behavior, according to some key attack path and weak nodes forward defense measures [3-4].

ISSN: 1738-9976 IJSIA

2. The Definition of Network Attack Model

2.1. Hierarchical Structure of the Whole Network Attack Model

Hierarchical expansion will describe the complex network attack system Petri net, which can effectively reduce the number of nodes in each layer of the network, at the same time the object creation the sub-graph reuse possible [5-6]. The network attack model is abstracted into two aspects, macro attack and micro attack: from the macro perspective to study on the relationship of the various nodes attack domain network, mining path by using network vulnerabilities; from the microscopic point of view of a node on the leak and risk evolution. The network attack and host attacks are by combining research, which can effectively grasp of what nodes in the whole network is the network leak and the leak in which the key setting and service is worthy of attention, so as to lay the foundation for network defense. The hierarchical structure of Petri net can be a good solution to the problem of macro attack and micro attack [7-8]. In this paper, the modeling approach is taken from top to bottom, the top Petri net description is on attack relationship of nodes in the network domain, while ignoring the nodes on the details of the attack, the leak of use and risk communication focus on the remote network attacks. In the lower Petri net, the hosts on the local attacks were modeled respectively, with detailed description of host attack state evolution. The macro and micro subnet network are integrated to achieve full network attack description of complex network system.

2.2. The Attack Efficiency of Transition

Transition is on behalf of aggressive behavior in Petri network, the attacker to Transition should be selected with a certain probability. If the network has many published public attack tools and source code, which can directly get simple attacks are more likely to be taken at the same time hackers, who are destructive and can bring huge gains attack mode is often the attacker favored means [9].

This paper presents the concept of attack effectiveness. Each attacker will come to judge the efficiency and ability to attack various feasible attack scheme based on information collected before the attack, to attack to find one or several attack strategies from the efficiency of the highest, in the rational case, this selection mode is consistent with the actual situation.

Definition 1: on attack t, APPR (t) (Attack Performance Price Ratio) is used to measure the attack efficiency variables, the unit cost benefit is the AI (t) attack Income and AC (t) attack cost ratio:

$$APPR(t) = \frac{AI(t)}{AC(t)} \quad (1)$$

Definition 2: on attack t, AIR (t) (Attack Income Ratio) is used to measure the attack ability variables, it reflects the degree of benefit attacker the Transition is triggered, attack of all selectable gain Transitions in the proportion of income:

$$AIR(t) = \frac{AI(t)}{\sum_{i=0}^{n} AI(t_i)} \quad (2)$$

Definition3: on attack t, AEP (t) Attack (Efficiency-Performance) is consolidated results of attack efficiency and attack capability. Its value is product of APPR (t) and AIR (t)

$$AEP(t) = APPR(t) \cdot AIR(t) \quad (3)$$

The attack effectiveness AEP introduced into each Transition, instead of traditional concept of time delay stochastic Petri net, it is as the judgment basis of the decision of attack. Different attackers have the number of different resources, different knowledge and experience, defensive performance of the attacked nodes and provide resources also differ in thousands of ways, so the cost per attack costs and benefits have random, attacked the price is a random variable, if the attack price is higher, the probability of aggression is greater. Distribution function of attack price is decided jointly by the attack cost and attack benefit variables, the two random variables are also follow their own distribution.

2.3 Hierarchical Extended Stochastic Petri Net

The whole network attack model are defined as the extended stochastic Petri net with hierarchical structure, hierarchical structure uses expression of object network. Object net [10] is by means of object oriented technology to express Petri network. The top of base nodes are as object, enclosed subnet in the object, subnet specified locations are to represent the object associated with the outside, the place called interface library. Transitions token is sent by the outside world to the interface library to call the object's methods and pass appropriate operands. Subnet extracts tokens from these positions to represent the object's response. In order to reflect the level, object interior also allows the inclusion of object. The hierarchical Petri net every transition is associated with an attack effectiveness of random variables, HESPN is defined as follows:

Definition 4: hierarchical extended stochastic Petri net

$$\mathrm{HESPN}=(O,P,T,\phi,Tok,H,I(t_i),O(t_i)). \quad (4)$$

3. Construction Method of the Whole Network Attack Model and Path Nining

3.1. Construction Method of the Whole Network Attack Model

The initial state set (ISS) corresponds to the node of Initial, it is an internal only contains special object interface library, it is composed of all network host services and leak information. Host, Webserver, FTPserver, DBserver and SMTPserver are node types in the network. Various classes contain multiple instances; each instance is as the object in the network, 6 kinds of state is the interface library in the VS. Various nodes of known connections and trust relationship transform into Transitions in the network, by Initial objects and NARS reasoning is to get attacked relationship of network nodes.

Each object can be extended subnets, describe the relationship of host interface States, such as the HostA node is as shown, the remaining nodes can also be extended.

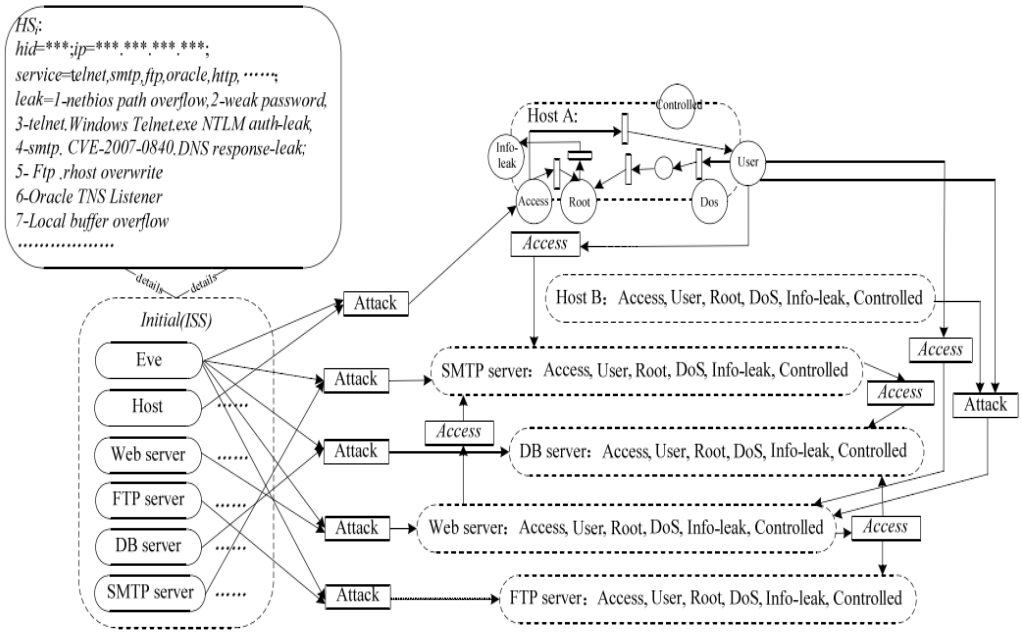

Figure 1. Diagram of the Whole Network Attack Petri Net

3.2. Mining Method of k Key Vulnerable Path

Looking for the accurate path the attacker may take in the whole network attack model has an important guiding significance for establishment of defense strategy. In the complex network system, generating all the accurate path is not necessary, the attacker will always choose low cost and benefit big strategic attack. This paper presents k key fragile path mining method based on the ant colony algorithm. The algorithm can find K in the rough attack in Petri network (k>=1) has precise attack path with maximum probability.

3.2.1. Information Update Rule of Transitions. Tok in the HESPN net operation, encountered the following three cases to stop:

(1) Run to the target database.

(2) $Num\_obj > Max\_obj$ in the Token .

(3) No Transition can be triggered. When all tokens have been terminated, the Transition in Tok sequence records are pheromone updating reward and punishment.

Set the token object library collection is $tok_{target} = (tok^1_{target}, tok^2_{target}, ..., tok^h_{target})$ .The remaining token sets are $tok_{rest} = (tok^1_{rest}, tok^2_{rest}, ..., tok^l_{rest})$.

For any token $tok_i^{num} \in tok_{target} \cup tok_{rest}$. Take the following update rule. If $t_j \in tok_i^{num}$

$$\tau^{new}(t_j) = \begin{cases} \tau^{old}(t_j) + \tau^{pra}(t_j) \\ \tau^{old}(t_j) - \tau^{pun}(t_j) \\ \tau^{old}(t_j) \end{cases} \qquad (5)$$

3.2.2. The Path Selection. When multiple Transitions fight for a token, token is according to a certain probability selection Transitions will be excited, this probability is determined by the effectiveness, Transition attack pheromone concentration.

$$P_{t_j}^{k} = \begin{cases} \dfrac{\tau(t_j)^{\alpha}\phi(t_j)^{\beta}}{\sum_{s \in allowed_k} \tau(t_s)^{\alpha}\phi(t_s)^{\beta}} \\ 0, \quad otherwise \end{cases} \tag{6}$$

3.2.3. Introduced Random Perturbation Token. In order to prevent the algorithm to fall into a local optimum, introducing random disturbance token in the initial database, in the lower information path there was the right to choose. According to the principle [11], the disturbance token each search step, generate a random number to determine the next step is to disturbance the original search rules. This paper designs random perturbation rule is as follows:

$$P_{t_j}^{k} = \begin{cases} \dfrac{F(\tau(t_j))}{\sum_{s \in allowed_k} F(\tau(t_S))} \\ \text{According to the formula 6 choice} \end{cases} \tag{7}$$

3.3. Network Risk Assessment based on Rough Path and Precise Path

In all the path RAP records, if there is an object node frequency is high, it is the opportunity is greater, the risk is the higher. Node utilization rate (NUR) is a measure of the degree of importance of a network node intermediary target library from the initial part of the library. When the target node has multiple, in the global network, any object of O_i utilization rate is

$$NUR(O_i) = \frac{\sum_{O_j \in U}^{M} N_{O_j}(O_i)}{\sum_{O_j \in U}^{M} N_{O_j}} \tag{8}$$

In addition, the introduction of leak threat degre**e** (LTD) is to assess the importance of the leak of the nodes. Basis value of LTD is node utilization rate (NUR (O_i)), efficiency of the node. O_i is the higher, O_i on the possibility of being attacked is greater. The added value of vulnerability threat degree is decided on node leak appear accurate path in the number and location of effectiveness. The more is the number of leak in k critical path, the efficiency value is greater, degree of node threat is the higher.

Leak $leak_k$ threat of objet O_i is obtained by Formula9

$$LTD(O^{i}_{leak_k}) = NUR(O) + \sum_{O_j \in U}^{M} \sum_{O^{i}_{leak_k} \in ap_i}^{M} \frac{G_{ap_i}}{\sum_{i=1}^{k} G_{ap_i}} \tag{9}$$

4. Experiment Design and Discussion

In order to illustrate the method of establishment and analysis of the whole network attack model, the network environment structure is as shown in Figure 2

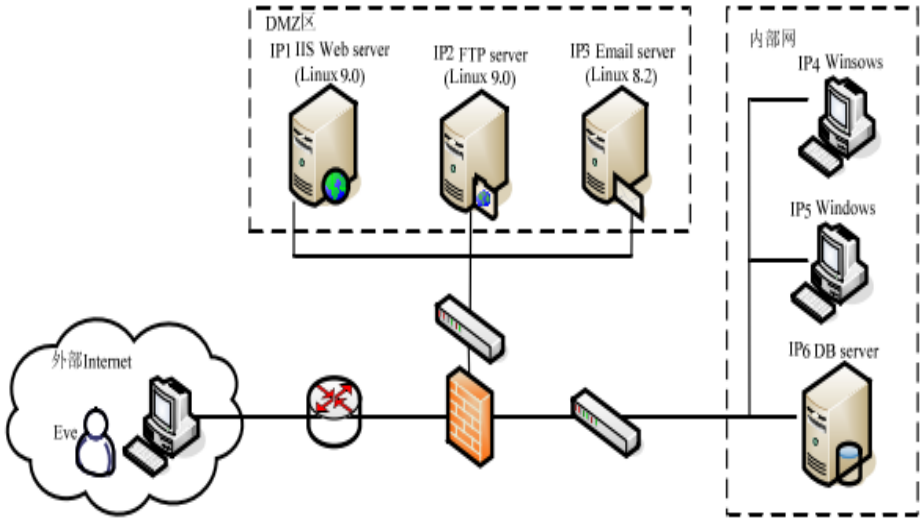

Figure 2. Topology Network

The environment consists of three components: an Internet DMZ network, the isolation zone and the internal LAN. DMZ zone has three servers, network IP6 stored enterprises important data, IP5 is as the control machine. Network administrator is responsible for the DMZ and intranet server resource allocation through it. The firewall is running the Linux operating system workstation, it controls access network between extranet and intranet, the host can access the DMZ zone of the server, you cannot access the internal LAN, between DMZ zone in the host can access each other, internal LAN only IP4 can be DMZ region of Web server and FTP server access, IP5 and IP6 are not visible. Hackers in the network is to launch an attack on the server and the host node DMZ and intranet.

Collect all the host of open service and leak information using leak scanning tools, it is as shown in Table 1, where, leak-id uses the loopholes number of Bugtraq leak database. The information and the relationship of these firewalls are stored in network status information database NSIS.

Table 1. Network Node Leak Information

hid	service	leak-id	leak description	Result
IP1	HTTP FTP	8668 4855	1.Wu-Ftpd SockPrintf() 2.IIS Buffer Overflow	Root Root
1P2	FTP SSH	9904 13454 36901 38479	1. SITE Command Remote Buffer Overflow 2. FTP Server Remote Buffer Overflow 3The Linux kernel pipe.c local privilege escalation vulnerabilities 4Linux Kernel dvb_net_ule() Remote Denial of service vulnerabilities	User User Root DoS
1P3	SMTP	8641	Sendmail Prescan () buffer overflow leak	Root
1P4		31874	Windows Server service remote RPC overflow	Controlled
1P5		18037	Word buffer overflow	Controlled
1P6	ORACLE	4845	Oracle TNS Listener remote buffer overflow	Controlled

According to the network state information base and attack rules, the top layer of Petri network construction algorithm HESPN-Generate can be obtained by adjusting the Petri network, it is as shown in Figure 3, the network establishes 7 objects, 6 test network host object and 1 initial information database objects, attack Transition was generated according to the rules of rough attack, if the attacker can control two hosts to server launch distributed denial of service attack, all hosts attack relations are as follows:

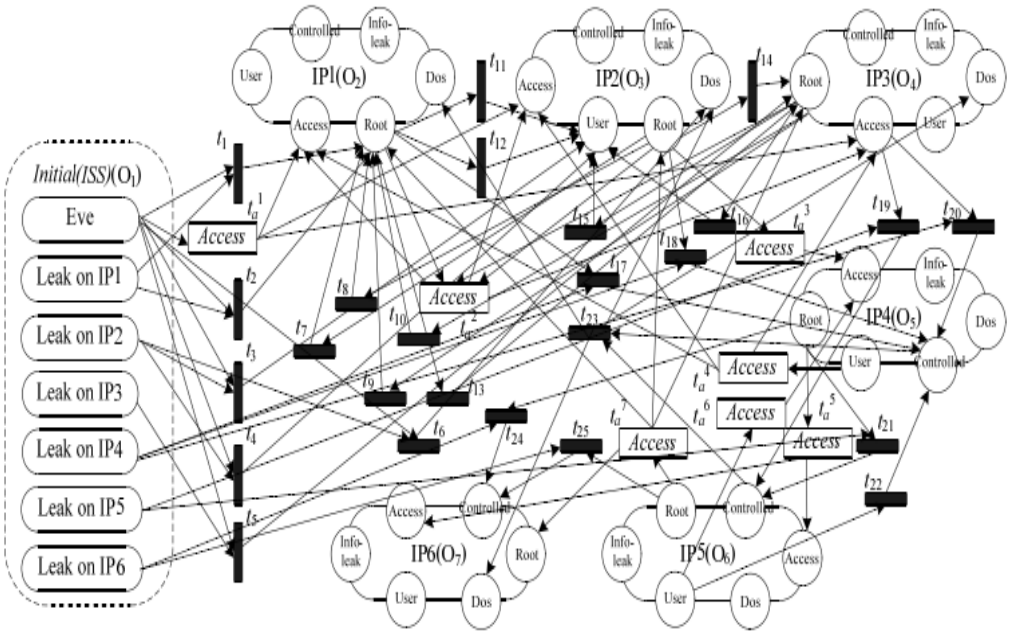

Figure 3. Diagram of Trials Network Top-level Petri Net

The top Petri network shows the DMZ region and the inner nodes access relations and various possible attack relationship, assuming IP2 and IP6 are as an important node in the network, the IP6 confidential information leakage and IP2 denial of service are concerned, according to the rough path mining algorithm, IP2.DoS and IP6.Info-leak are input for attack, attack path that rough set RAP:

Table 2. Rough Path Set RAP

O_{target}	rP_{num}	$path$
O_7	rp_1	<O_1,O_2.Root>,<O_2.Root,O_5.Root>,<O_5.Root,O_7.Controlled>
O_7	rp_2	<O_1,O_3.User>,<O_3.Root,O_5.Root>,<O_5.Root,O_7.Controlled>
O_7	rp_3	<O_1,O_4.Access>, <O_4.Access,O_6.Controlled>, <O_6.Root,O_7.Root>
O_7	rp_4	<O_1,O_4.Access>, <O_4.Access,O_6.Controlled>,<O_6.Root,O_7.Root>
……	……	……

O_3	rp_i	$<O_1,O_4.Access>$ $<O_4.Access,O_5.Controlled>$, $< O_5.Root,O_6.Controlled>$, $<O_5.Controlled \wedge O_6.Controlled,O_3.DoS>$
O_3	rp_{i+1}	$<O_1,O_3.DoS>$
.....	.....	.....

Table 2 lists the 6 paths as an example. $rp_1, rp_2, rp_3, rp_4, rp_i$ is a rough path. Attacker rp_1 is to gain the Root permission and IP4 access. through 4855 leak of Web server, and then use the RPC overflow with elevated privileges to access the database server, attack DB server overflow leak could allow an attacker to execute arbitrary instructions, can visit IP6 confidential information to expand the IP6 object. rp_2 attackers is to gain the user permission through the use of the IP2 loophole, but if you want to get IP4 access must have Root permission, can further improve the privilege to open the object O_3, by attacking the local elevation of privilege leak to achieve $< O_3.User, O_3.Root >$. In the rp_4, when an attacker is to execute arbitrary instructions on IP5 need to develop object, whether can gain full control over IP5 by means of attack, and to access the purpose of IP6 operation,

rp_i is a attack path of refused service on IP2, the attacker access DMZ mail server, it will contain the shock wave virus file by attachment to user of IP4, IP4 after infection with 20s interval detection connected host, further infection 135 port open IP5. IP4 and IP5 carry out the DDoS attack on IP1 in a remote attacker control. rp_{i+1} is a precise path, the attacker is by using the IP2 Remote Denial of service leak directly to a standstill. It can be seen from table2, from the initial base O_1 to attack target, RAP reflects all the relationship of network leak. In this case, the rough path to the target IP6.Info-leak a total is 284, reached the path to IP2.DoS is 41, RAP total is 325 records.

Not involved object and Transition are as "unable" in the rough path set RAP. The target is O_2, object O_7 is not involved in the attack; attack target is O_7, the domain network 6 hosts were involved in the attack. The object of this case are available, transition just tag does not participate in the attack. When the number of the network host is above 50, the steps are effective to delete irrelevant nodes, save storage space and precise way the search space.

In the extended object subnet, RAP rough paths need to be extended objects with O_3, O_5, O_6, O_7. Figure 3 shows the attacker access to certain privileges or capability to perform the remote attacks, continue to use the local host leak attack to gain more rights and illegal operation data file.

Figure 4 (c) is not migration relationship of interface States, the host IP5 does not have the permissions or enhance the attackers attack ability condition. Figure 3 and Figure 4 are combined into network attacking Petri net model.

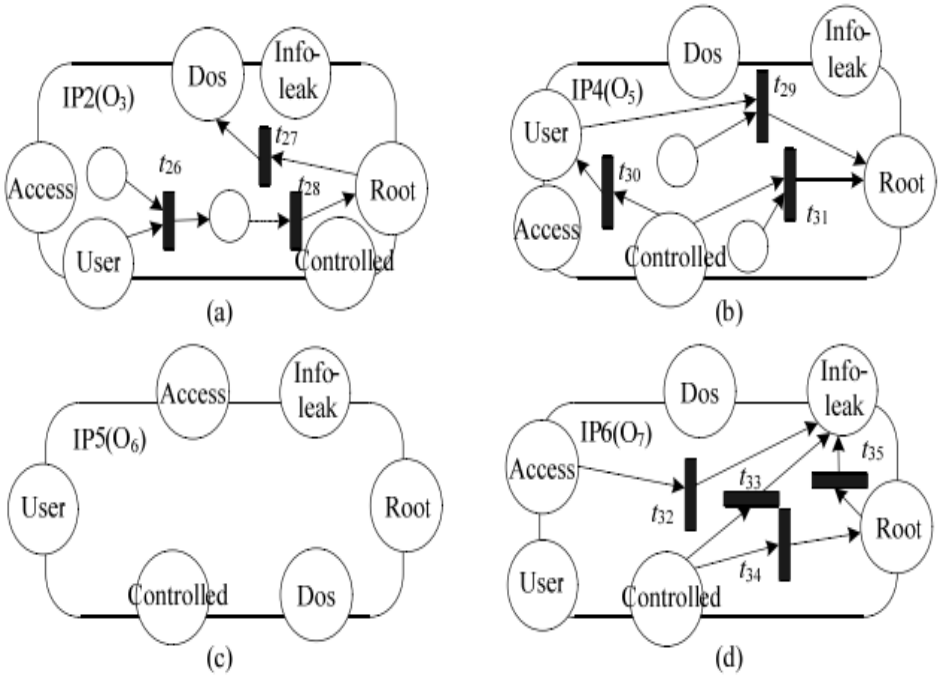

Figure 4. Sub Petri Net of Extended Object

Using the k key fragile path mining method can find out the exact path to the target IP2.DoS and IP6.Info-leak. In the simulation experiment, let k=3, the Transition of attack effectiveness expected value is as shown in the following table3:

The following values of the parameters involved in the algorithm: initial object in O_1 Eve library the token number is 20, the rest of the interface library of the token number is 4, the maximum token number of search $N\max = 200, \tau_0 = 10, Q = 20, \xi = 1, \eta = 0.3, \alpha = 0.5$ $\beta = 0.5$, $p = 0.5$, $p_{\min} = 0.1, \theta = 0.8$. In the path search process, the largest object token allows traversal number Max_obj is 4, the limit value of the ant colony algorithm greatly reduces the searching time, when token search is about 70 time, three key ant road HESPN system at IP6.Info-leak has been basically highlight. After completing 200 iterations, in the IP6.Info-leak, the 3 most excellent token record is:

$\{seq=t_2t_{17}t_{31}t_{24}t_{34}t_{35}; Num\_obj=3; G=0.493\}$,

$\{seq=t_1t_{17}t_{31}t_{24}t_{34}t_{35}; Num\_obj=3; G=0.482\}$, $\{seq=t_a^1t_{20}t_{31}t_{24}t_{34}t_{35}; Num\_obj=3; G=0.474\}$.

Three key paths to IP2.DoS is $\{seq=t_6; Num\_obj=1; G=3.33\}$, $\{seq=t_a^1(t_{19} \wedge t_{20})t_{23}; Num\_obj=4; G=0.56\}$, $\{seq=t_3t_{26}t_{28}t_{27}; Num\_obj=1; G=0.55\}$

Table 3. Transition the Effectiveness Value in HESPN

ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8	ϕ_9	ϕ_{10}	ϕ_{11}	ϕ_{12}
2.08	2.5	1.4	1.37	2.32	3.33	2.08	2.5	2.08	2.5	1.4	1.37
ϕ_{13}	ϕ_{14}	ϕ_{15}	ϕ_{16}	ϕ_{17}	ϕ_{18}	ϕ_{19}	ϕ_{20}	ϕ_{21}	ϕ_{22}	ϕ_{23}	ϕ_{24}
2.32	2.32	1.4	1.37	1.42	1.42	2.18	2.2	1.33	1.42	3.57	1.53
ϕ_{25}	ϕ_{26}	ϕ_{27}	ϕ_{28}	ϕ_{29}	ϕ_{30}	ϕ_{31}	ϕ_{32}	ϕ_{33}	ϕ_{34}	ϕ_{35}	$\phi_a^1 - \phi_a^4$
1.53	1.8	3	2.6	1.6	0.93	2.02	1	3.54	5	5.3	1
$\phi_a^5 - \phi_a^6$	ϕ_a^7										
0.8	10										

According to the formula8-9 by RAP and critical path set can be calculated for each network node risk index ND and LTD leak threat, it is as shown in the Table 4:

Table 4. Every Node of Network Risk and Leak Threat Degree Value

Node	NUR	KP	ND (a=b=0.5)	LTD
$IP1(O_2)$	0.772	0.33	0.55	LTD (8668)=1.112, LTD (4855)=1.104
$IP2(O_3)$	0.84	0.5	0.67	LTD (9904)=0.714, LTD (13454)=0.838 LTD (36901)=0.838, LTD (38479)=1.464
$IP3(O_4)$	0.803	0.33	0.56	LTD (8641)=0.803
$IP4(O_5)$	0.895	0.66	0.78	LTD (31874)=2.021
$IP5(O_6)$	0.572	0.16	0.36	LTD (18037)=0.698
$IP6(O_7)$	0.874	0.5	0.68	LTD (4845)=1.874

In the Table 4, risk degree of host IP4 is the highest. This is because the firewall to allow DMZ server to access the IP4, it has become the only channel DMZ area and the internal LAN, so the attacker is to the outer bound by IP4 on the intranet host attack. At the same time, port 135 is the default open port system, as long as the 135 port and IP4 establish TCP connection can attack the RPC leak, allowing an attacker to execute arbitrary instructions thereon and further access to system control, the IP4 attacker is either on the IP2 issued a denial of service attack and can also attack IP6 illegal access to resources access. So the 31874 hole is easy to attack and high risk, considering the threat degree is the highest. Thus, the attacker will often attack using the relevance and low leak of node. IP2 and IP6 are the target node, easy to understand they have high risk. The attacker through the IP3 mail server sent to a virus file forwarded directly to the network the host node, this attack is low cost and harm, Therefore, through the rough path IP3 path and accurate are than IP1 more nodes, the risk is greater.

5. Conclusion

This paper uses HESPN to achieve modeling for the whole network attack behavior, and puts forward the method of generating the model. Rough attack path mining in the top Petri is to search and attack the target host node and attack relationship, we extend object node to establish to the whole HESPN attack model. On the basis of the ant colony algorithm to further tap the k key vulnerable path, these path of attack effectiveness are the highest, it was

most likely taken by an attacker. By comprehensive consideration the rough path and precise path, presented assessment methods of each node of the risks and vulnerabilities, provide an important basis for decision of network defense.

References

[1] H. Guangqiu, Z. Bin and W. Chunzi, "The network attack model based on extended SPN", Computer Engineering, vol. 22, **(2011)**, pp. 12-18.
[2] W. Chunzi, Z. Bin and H. Guangqiu, "The attack strategy mining and risk assessment model based on attack the whole network", Computer engineering and applications, vol. 4, **(2012)**, pp. 14-18.
[3] H. Guangqiu and W. Jincheng, "The fuzzy Petri net attack model of double branch fuzzy sets based consistency", Computer applications, vol. 02, **(2009)**, pp. 529-534.
[4] W. Yuanzhuo, L. Chuang, C. Xueqi and F. Binxing, "Network attack defense game model based on stochastic analysis method", Chinese Journal of computers,vol. 09, **(2010)**, pp. 1748-1762.
[5] Huangdan, "Encryption based on attribute based trust management combination scheme in wireless sensor networks", Journal of computer applications, vol. 04, **(2014)**, pp. 1047-1050.
[6] L. Qin, "Multi user shared security issues of cloud computing services environment", Central South University, **(2012).**
[7] L. Chang, "Modeling and optimization of the design of multi path transmission", Beijing Jiaotong University, **(2013).**
[8] W. Cong, "Studying the network space embedding model and application", The University of Electronic Science and technology, **(2013).**
[9] L. Xuejiao, "Research and implementation of network security attack model and event correlation technology", Huazhong Normal University, **(2009).**
[10] H. Kegang and D. Jianjie, "The hierarchical structure of Petri network", The computer science and exploration, vol. 2, no. 2, **(2008)**, pp. 123-130.
[11] H. Guangqiu, W. Jincheng and Z. Bin, "Characteristics of the optimal path to Transition SPN sequences with different distributions", Engineering and application of computer, vol. 45, no. 29, **(2009)**, pp. 43-48.

Authors

Yongfu Zhou, he received his master's degree of engineering in Huazhong University of Science and Technology software engineering. He is a lecturer in Heyuan Polytechnic. He is in the research of Computer network and security technology.