International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.89-98
http://dx.doi.org/10.14257/ijsia.2015.9.7.08

Dynamic Awareness Method for Network Threats based on Rough Vulnerability Relation Model

Jieyun Xu and Hongzhen Xu

East China Institute of Technology
Jiangxi 330013, china
jyxu@ecit.cn

Abstract

In order to solve the redundancy question in complex network which is caused by similar attack method and similar node object in attack model, the node domain and transition domain of Petri Net are divided into equivalence classes, and then the construction method of rough vulnerability relation model is given. By defining similar degree of path, search for all of the characteristic attack path which can attain attack object by use of ant algorithm, and calculate the maximal threat of object node which is brought by characteristic strategy. In order to ensure threat prediction suit for attack scene, dynamic perception method of network threat is proposed, which relies on Intrusion Detection Systems (IDS) warning to amend threat value constantly.

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

1. Introduction

With constant updates of attack technologies, aggrandizing network scale and more complicated structure, the real-time awareness of network threat situations becomes a critical issue to be solved by network administrators[1-2]. But in the face of many nodes (such as user computer, server, security system, network devices) in the complicated network system, vulnerabilities in such nodes, and the intricate connection and access relationship among them, administrators can't figure anything out about how to remove redundant information and extract necessary information and to make timely and comprehensive evaluations of threats by according to the dynamic changes of attack situations [3-4]. So the dynamic threat assessment in the complex network system is an important and very new research topic in today's network security field. It faces great difficulties and moves slowly [5-6].

For the attack strategy generation based on incomplete information, [7] suggested the use of rough attack graph to depict uncertainties for what strategies taken by the attacker. The max-flow analysis algorithm of network risks was developed according to the classification of attack modes [8]. But the rough attack graph's generation method and the related analysis were dependent on the definition and knowledge of the attacker's abilities. In practical analysis, it will meet big challenges, because in the active defending phase, i.e. before the attack happens, the attacker's situation is almost nothing to the defendant. The attacker's power and preference are both uncertain information. So the method is limited in the scope of application [9-10].

Based on the above discussion, we develop a new method which is suitable for attack modeling and threat analysis in the complex network system. At first, a vulnerability correlation model is built for the object-based Petri net. The model describes all attack relations among network hosts. By introducing rough set theory, attack modes with the same attack effect in Petri net and network nodes in the same level in the attack relationship are put to a similar equivalent class [11]. The purpose of classifying is to resolve conflicts between overall grasp of attack trends and scale limitation of paths

ISSN: 1738-9976 IJSIA

through the attainment of only a few feature attack paths to search the whole attack strategy space. Again following the concept of threat degree in the last part, we apply the improved ant colony algorithm to find in the Petri net domain the feature paths to attack targets. Each feature path stands for one class of attack strategy and has the biggest threat degree that it propagates in the class. To make the calculation of threat degree adaptable to the dynamic changes in the network attack situations, we combine the active and before-doing threat analysis with "learn-after-doing" IDS security alarm mechanism. On the basis of preliminary forecast, we rectify in the real time the threat degree of each node by virtue of network monitoring information, to thus build a dynamic network threat awareness method [12].

2. Creation of Rough Vulnerability Correlation Model

2.1. Definition of Petri Net based on Rough Objects

In reality, when several vulnerabilities in one node can reach the same attack purpose, different attackers show different preferences for vulnerabilities to be attacked, specifically, attackers decide to choose which vulnerability as breakthrough point as per their familiarity with various attack modes and the attack power. So all predications made by the defending side is of roughness, e.g. evaluating one or more paths which have the biggest threat degree. They are deterministic judgments made based on incomplete information, which can't be completely held by only the attacker's subjective consciousness and experience. They are imperfect.

Professor Tong He and Kaiquan Shi introduced rough set theory to the traditional graph model. Arcs/sides among nodes are used as dividing object in the domain space. After attributes assigned to those arcs/sides, they are categorized to different equivalent classes $[e]_R$ based on the equivalent relation R, discriminating the type of arcs/sides with the same endpoints. On the basis of ideas of rough graph, the paper brings in rough set theory to Petri net modeling to define a new Petri net model. Rough Petri net has descriptive capability to the incomplete information. It represents the in-distinguish ability among attack behaviors in the same node and that among nodes having similar function, position and attack relationship in the domain network. We define it like:

Definition 2.1 the change of space. Given $U = (t_1, t_2, ...t_U)$ to change the domain, t_i is change of Petri network, said an attack behavior. R is the U attribute set, it can form equivalence relation in U. $U / R = \{T_1, T_2, T_3, ..., T_v\}$ said that all the equivalence classes according to the R partition

Definition 2.2 Node space. Given U $U^{'} = \{O_0, O_1, ...O_{|U^{'}|}\}$ is the node domain. O_i is node object of Petri net. $R^{'}$ is attribute set in $U^{'}$. It can form equivalence relation in $U^{'}.U^{'} / R^{'} = \{Obj_1, Obj_2, Obj_3, ..., Obj_c\}$ shows all valence class of $R^{'}$

2.2 The Division of the Domain Class Space on Petri

According to definitions 2.1 and 2.2, the node object space and the change of space on Petri net divided equivalence class, formed a class space.

Generation algorithm change class space:

Algorithm：Classpace_generation

Input： $U = (t_1, t_2, ...t_U)$, R

Output： $U / R = \{T_1, T_2, T_3, ..., T_v\}$

(1) Initialization. Create set $U / R = \varnothing$ attVal={{Access},{User},{Root, Controlled},{DoS}, {Info-leak}}

(2) for(i=2;i≤ m;i++)
(3) { flag=0
(4) for(j=1;j≤ class_num; j++)
(5) {if $(I(t_i).Obj == I(T_i).Obj \&\& O(t_i) == O(T_i))$
(6) { $T_j = Obj == I(T_j).Obj \&\& O(t_i) == O(T_j))$
(7) {$T_j = T_j \cup t_i$; flag=1;break;}}
(8) if(flag==0)
(9) Create a new class $T_{++class\_num} \in U / R; T_{class\_num} = \{t_i\}$ }
(10) Output U / R

The above algorithm, when state of former transition belongs to the same node object, as after state is on the same fragile state of same node, they are classified as a class.

Compared to generation mode of change class, generation space of node class is complex, first traversal attack relationship of nodes in the Petri network domain to generate conditions- equivalence class space. Then attribute nodes are divided according to the each class space. In order to dynamically adjust the threat degree, this algorithm will have node object of the same attack consequences classified as a class. The following is generation algorithm of node space:

Algorithm：Obj_generation

Input：The domain Petri network ROPN, $U' = \{O_0, O_1, ...O_{|U'|}\}$ is the node domain, R'

Output：$U' / R' = \{Obj_1, Obj_2, Obj_3, ..., Obj_c\}$

(1) Initialization. Create set $U' / R' = \varnothing; Obj\_AR_1 = \{O_1\}$
(2) class_num=0
(3) for(i=1;i≤N;i++){
(4) for(j=1;j≤5; j++) {
(5) for $O_i pj$,Create a new class of $\mathrm{Obj\_AR}_{class\_num+1}$
(6) for $(O_a ph \in InputPlace(O_i pj))$
(7) $\mathrm{Obj\_AR}_{class\_num+1} \leftarrow O_a ph$
(8) for(l=1;l≤class_num; l++)
(9) {flag=0
(10) If $\mathrm{Obj\_AR}_{class\_num+1}$ and Obj_AR_1 are the same elements
(11) $Obj\_AR_1 = Obj\_AR_1 \cup \mathrm{Obj\_AR}_{class\_num+1}$
(12) flag=1; break}}
(13) if(flag==0) ; class_num++
(14) }}

3 Dynamic Analysis of Network Threats based on the Rough Vulnerability Correlation Model

Definition3: The P elements of $g = \{g_1[k].g_2[k], ..., g_n[k]\}$ and ROPN are corresponding. $g_i[k](i = 1, 2, ..., n)$ is a data structure array. Where, token record of $g_i[l] = (route = p_0, t_1, p_1, t_2, ..., t_k, p_l; C_{total;} AT)$, rout and C_{total} are the same.

Definition 4: Path similarity (Rout_Sim). Path similarity is similarity of the rout path sequence in tokens. By the equivalence node to reflect in the path. Set sequence of path $rout_i$ and path $rout_j$ are seq_i and seq_j, there are:

$$Rout\_sim(rout_i, rout_j) = \begin{cases} 1 - \dfrac{bit\_sum(seq_i \oplus seq_j)}{length} \\ 0 \end{cases} \quad (1)$$

The similar path is determined through the following steps:

Set seq_1 and seq_2 the library sequence of path $rout_1$ and $rout_2$. When making fuzzy operations, we start comparison from the rightest end (i.e. target library) of path sequence. If the position of the target is same, the position is 0. Then we judge if the second position in the right is same. If yes, the position is 0; otherwise, with attacking the target library as condition, we need to find from the condition equivalent class $U^{'} / R$ of node objects if the two libraries have equivalent relationship. If they belong to the same equivalent class as far as the target library is concerned, the position is 0.5; or it's 1. Continue comparison in the left. With the second-position library as condition, we judge the equivalent relationship between two libraries in the third place. If the second library is 0, do like before. If the second library is 1 or 0.5, it indicates the library in the second position is unlike. Set $O_i pa$ and $O_j pb$, which are used as the precondition. We continue determining if equivalent relationship exists in $U^{'} / R$ between two libraries in the third position. To $O_i pa$ and $O_j pb$, two libraries in the third position belong to the same class, the position is 0.5; otherwise 1.

When several transitions strike for one token, the token selects to-be-initiated transition according to the probability, which is decided by the changing attack complexity and pheromone concentration.

$$P_{tj}^k = \begin{cases} \dfrac{\tau_j^\alpha \lambda_j^\beta}{\sum_{s \in allowed_k} \tau_s^\alpha \lambda_s^\beta}, allowed_k \neq \varnothing \\ 0, oterwise \end{cases} \quad (2)$$

The generative algorithm for k-feature attack strategy is defined below:

Algorithm: k-AttStr

Input: ROPN, target library

Output: k-max threat feature strategy $g_i[k]$ of each target library

Step 1: initialize α, β, similarity threshold value ε etc; pheromone in every transition t initialized to τ_0; put x ants (i.e. tok) in the initial library $O_o p_0$;

Step 2: when there're toks in the library, relative transition is triggered; when several transitions fight for them, a random number Rd [0,1] is produced; if Rd>0.5, stimulate the transition by equation (2); otherwise, choose the path by $P_{tj}^k = 1/b$;

Step 3: when the transition is activated, assume the tok_h moving to the library p_i; update entries of tok as $rout += t_j p_i$, $C_{total} += \lambda_j$; compare k of C value in $g_i[k]$ and C_{total} value in tok_h, as $g_i^{new}[k] = k\_\max C_{total}(tok_h, g_i^{old}[k])$,where $k\_\max C_{total}()$ means choosing k entries with C_{total} value from bracketed tok entries and save in $g_i[k]$;

Step 4: determine if the tok arrives at the library. In the following cases, the tok stops walking: a. arriving at the target library; b. no transition can be stimulated. c. $Num\_obj > Max\_obj$ in tok.

Step 5: perform global update of new pheromones in each transition;

Step 6: decide if all toks complete iterations; if yes, k paths in $g_i[k]$ in the target library is k feature paths with the biggest threat degree to reach the library. They show every possible attack strategy taken by the attacker.

4 Experiment Design and Discussion

In order to illustrate the establishment and analysis of dynamic network threat perception model, establish the following test network environment, it is shown in Figure 1.

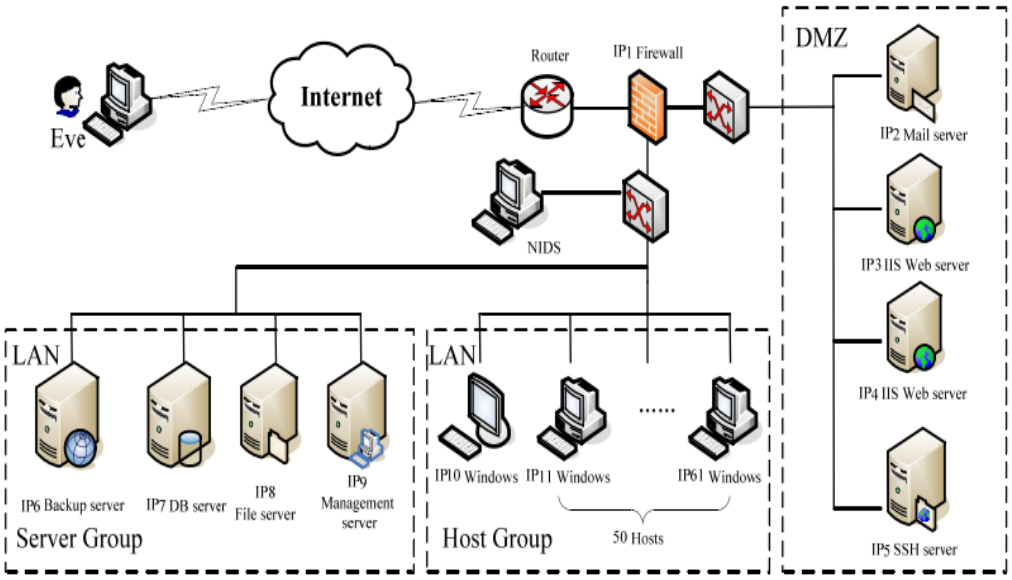

Figure 1. The Network Topology Map

The whole web has 61 host devices, of which 5 hosts running in the DMZ area to provide services to users in the inner and outer net. Two Web servers run simultaneously and are of load balancing configuration. The internal local network includes two parts: server cluster and user cluster. The former consists of backup server, database server, file server and administrator server. The database server stores enterprise private data. Backup server copies important files in IP7 and IP 8 and updates them synchronously. When both database and backup servers break down, they can be automatically shifted as to provide promptly the relevant services. The administration server is responsible for security monitoring tasks. It drives related function modules to generate MD5 abstracts of key data files and regularly monitor and compare abstracts. If application servers in DMZ area and intranet server clusters are attacked, it will send alarms to the administrator and generate relative report. In the user cluster, there are 50 ordinary client computers and one management computer (IP10). With the help of firewall configuration software installed in the management computer and server management software, network administrators can configure firewall and control resource management, performance maintenance and monitoring configuration of each application server system. IP10 will assess punctually the current threat degree of network as per the alarm information sent by NIDS and IP9 and take defending strategies.

Firewall configuration information is in Table 1:

Table 1. Security Policy Configuration of the Firewall

The source address	The source port	The destination address	The destination port
Extranet	Arbitrarily	LAN	Arbitrarily
Extranet	Arbitrarily	DMZ	Arbitrarily

LAN	Arbitrarily	Extranet and DMZ	Arbitrarily
IP3,IP4	80	IP7	1521
IP3,IP4,IP5	Arbitrarily	IP8	Arbitrarily
IP3,IP4	Arbitrarily	LAN	Arbitrarily
IP2	Arbitrarily	LAN	Arbitrarily

In the above configuration, WWW servers in IP3, IP4 can read data from and write data to the database server IP7 in the intranet. The FTP service runs in all IP3, IP4 and IP5. They can provide publishable files to outer visitors by accessing File server in LAN. Apart from the firewall, the server in the intranet server cluster prevents outer IP from accessing and allows the access by only business network devices. Using scanning tools like Nessus, OVAL can help get open services by all hosts and existent loopholes in the network.

The network information and harms caused by attacking various vulnerabilities are shown in Table 2.

Table 2. The Existing Loopholes and Access Relation on Each Node

hid	service	leak-id	leak description	Result
IP1	/	12918	RedHat Linux telnet Overflow	Root
IP3 IP4	WWW FTP	8668 4855	Wu-Ftpd SockPrintf() IIS Buffer Overflow	Root Root/DOS
IP5	FTP SSH	8628 9904 13454 36901	OpenSSH Buffer Overflow SITE Command Remote Buffer Overflow FTP Server Remote Buffer Overflow Weak Password	Root User User Root
IP6	ORACLE	39441	Oracle 11gR2 Remote command execution overflow	Info-leak
IP8		31874	Windows Server Service remote Rpc overflow	Root/DOS
IP10		8152	SMB Bao remote data destruction loopholes	Root
IP11-IP61		31067 31874	Microsoft office remote Code execution vulnerability Windows Server Service remote Rpc overflow	Root Root

With currently collected network information and access correlation among hosts, the universal attack Petri net model is produced. The model displays the attack relationship among any nodes. As seen in Figure 2, hollow transition means legal access behaviors among nodes; solid transition is illegal attack behaviors. The picture keeps only legal access behaviors which can result in object-related privilege promotion or information leakage for the direct utilization of such behaviors by the attacker. Such behaviors is part of the attack process. Other access relations as the precondition of attack are omitted. O_0 is object of the attacker; other O_i corresponds to $\mathrm{IP_i}$ in Figure 2; user computers IP12-IP60 have similar structure and attack relationship with O_{11} and O_{61}.

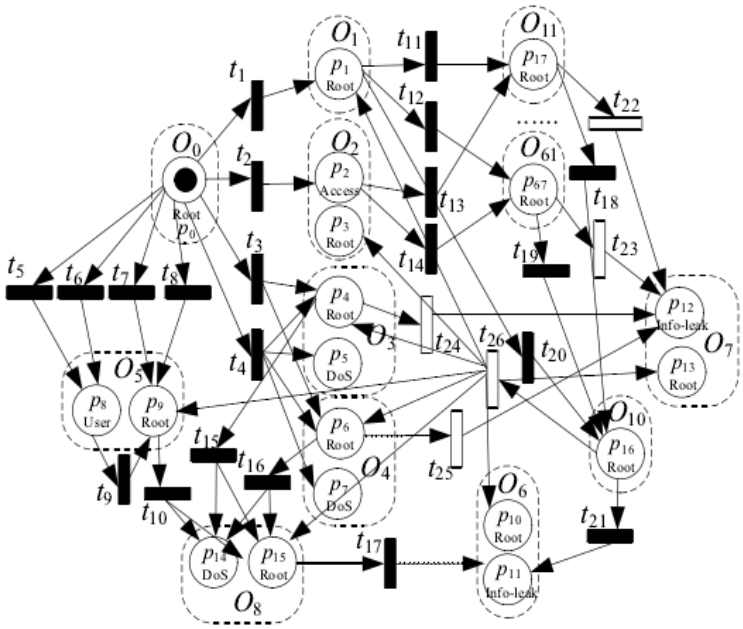

Figure 2. The Domain Petri Network Attack

In the domain Petri net. By Classpace_generation of generation algorithm and Obj_generation algorithm obtained the following equivalence partitioning.

U/R={{t_1}, {t_2}, {t_3, t_4}, {t_5, t_6}, {t_7, t_8}, {t_9}, {t_{10}}, {t_{11}}, {t_{12}}, {t_{13}}, {t_{14}}, {t_{15}}, {t_{16}}, {t_{17}}, {t_{18}}, {t_{19}}, {t_{20}}, {t_{21}}, {t_{22}}, {t_{23}}, {t_{24}}, {t_{25}}, {t_{26}}};

U'/R'={{$O_6.p_{11}$: $O_8.p_{15}$}, {$O_6.p_{11}$: $O_{10}.p_{16}$}, {$O_7.p_{12}$: $O_{11}.p_{17}$,$O_{12}.p_{18}$…,$O_{61}.p_{57}$}, {$O_7.p_{12}$: $O_3.p_4$,$O_4.p_6$}, {$O_8.p_{14}$,$O_8.p_{15}$: $O_5.p_9$,$O_3.p_4$,$O_4.p_6$}, {$O_{10}.p_{16}$: $O_{11}.p_{17}$,$O_{12}.p_{18}$…,$O_{61}.p_{57}$}, {$O_{10}.p_{16}$: $O_1.p_1$}, {$O_{11}.p_{17}$,$O_{12}.p_{18}$…,$O_{61}.p_{57}$: $O_1.p_1$}, {$O_{11}.p_{17}$,$O_{12}.p_{18}$…,$O_{61}.p_{57}$: $O_2.p_2$}, {$O_1.p_1$,$O_2.p_3$,$O_3.p_4$,$O_4.p_6$,$O_5.p_9$,$O_6.p_{10}$,$O_7.p_{13}$,$O_8.p_{15}$: $O_{10}.p_{16}$}};

Changes of t_5, t_6 said respectively the holes attack of 9904, 13454 on the SSH server. They can be exploited directly, and access to the Root permissions. In the attack effect, two kinds of attack methods are equivalent. At the same time, t_7 t_8 said the attacker can obtain attack IP5 Root privileges by buffer overflow and weak password, two kinds of attack methods also have the indiscernibility

Set database server IP7 and backup server IP6 are key protection object in LAN, to obtain illegal access of the sensitive data and Root permissions, the enterprise will be caused heavy losses. IP6.Info-leak, IP6.Root, IP7.Info-leak and IP7.Root are attack target. The domain Petri network and the generated together are as k- feature attack strategy mining algorithm input. The following is values of the parameters in k-AttStr algorithm:

Each iteration puts into 20 toks in the initial database $O_0.p_o$, as $k=4, t_0=8, \alpha=0.5, \beta=0.7, \varepsilon=0.76, Max\_obj=4, \xi=2, Q=30, \eta=0.2, p=0.3$, set the index weight value of attack threat: $\omega=0.4, w_1=w_2=0.5, a_1=a_2=0.5, P_c=P_i=P_a=1/3, P_{pr}=P_{cr=0.5}$.

The Tok completed about 7 search, 4 object library records are:

$g_{10}[0]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{20}, $O_{10}.p_{16}$, t_{26}, $O_6.p_{10}$; C_{total}=1.2; AT=0.5774);

$g_{10}[1]$=($rout$=$O_0.p_0$, t_2, $O_2.p_2$, t_{13}, $O_{11}.p_{17}$, t_{18}, $O_{10}.p_{16}$, t_{26}, $O_6.p_{10}$; C_{total}=1.3; AT=0.564);

$g_{10}[2]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{11}, $O_{11}.p_{17}$, t_{18}, $O_{10}.p_{16}$, t_{26}, $O_6.p_{10}$; C_{total}=1.9; AT=0.4963);

$g_{11}[0]$=($rout$=$O_0.p_0$, t_2, $O_2.p_2$, t_{13}, $O_{11}.p_{17}$, t_{18}, $O_{10}.p_{16}$, t_{21}, $O_6.p_{11}$; C_{total}=2; AT=0.393);

$g_{11}[1]$=($rout$=$O_0.p_0$, t_4, $O_3.p_4$, t_{15}, $O_8.p_{15}$, t_{17}, $O_6.p_{11}$; C_{total}=1.7; AT=0.4227);

$g_{11}[2]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{20}, $O_{10}.p_{16}$, t_{21}, $O_6.p_{11}$; C_{total}=1.9; AT=0.40235);

$g_{12}[0]$=($rout$=$O_0.p_0$, t_2, $O_2.p_2$, t_{13}, $O_{11}.p_{17}$, t_{22}, $O_7.p_{12}$; C_{total}=0.6; AT=0.5794);

$g_{12}[1]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{11}, $O_{11}.p_{17}$, t_{22}, $O_7.p_{12}$; C_{total}=1.2; AT=0.4834);

$g_{12}[2]$=($rout$=$O_0.p_0$, t_4, $O_3.p_4$, t_{24}, $O_7.p_{12}$; C_{total}=0.3; AT=0.6394);

$g_{13}[0]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{20}, $O_{10}.p_{16}$, t_{26}, $O_7.p_{13}$; C_{total}=1.2; AT=0.5774);

$g_{13}[1]$=($rout$=$O_0.p_0$, t_2, $O_2.p_2$, t_{13}, $O_{11}.p_{17}$, t_{18}, $O_{10}.p_{16}$, t_{26}, $O_7.p_{13}$; C_{total}=1.3; AT=0.564);

$g_{13}[2]$=($rout$=$O_0.p_0$, t_1, $O_1.p_1$, t_{11}, $O_{11}.p_{17}$, t_{18}, $O_{10}.p_{16}$, t_{26}, $O_7.p_{13}$; C_{total}=1.9; AT=0.4963);

The above 12 groups of records are the characteristic attack paths the initial library $O_0.p_o$ to target library $O_6.p_{10}, O_6.p_{11}, O_7.p_{12}, O_7.p_{13}$ .3 paths reflect the variety characteristics of the attacker's strategy in each target library, it can cover the entire attack strategy space, and they are maximum path of threat attack degree in all kinds of strategies.

The above 12 records is a subset in the Petri net, forming a rough Petri net in equivalence classes and the node object equivalence class space

5 Conclusion

It proposed a new dynamic evaluation method for network threats. With IDS alarming information to rectify constantly the previous prediction, the network threat assessment is more practical. Meanwhile for complicated network system, it defined different security monitoring ranges. The rough Petri net was applied to reduce the generated number of attack paths. The adjustment and assessment of threat degree proved more flexible and practicable. The model reacts quickly to the external environment.

References

[1] J. Zhang, “Research on Key Technologies of network security situation assessment”, The National Defense University of science and technology, (**2013).**
[2] D. Ma, “Research on Key Technologies of network threat detection and situation prediction”, The University of national defense science and technology, (**2013).**
[3] C. Chen, “Research on technology of network security situation assessment based on knowledge acquisition and fusion rule”, The PLA Information Engineering University, (**2013).**
[4] D. Zhang, “Research on the credibility of network system based on autonomic computing and self-optimization method”, Henan University of Science and Technology, (**2013).**
[5] P. Liu, Y. Meng and Y. Wu, “Perception and prediction of large-scale network security situation”, Computer security, vol. 3, (**2013**), pp. 28-35.
[6] P. Ni and Z. Wu, “Research on analysis method of network vulnerability”, Computer technology and development, vol. 4, (**2013**), pp. 126-130.
[7] G. Huang and Y. Li, “Evaluation model based on rough graph network risk”, Computer applications, vol. 30, no. 1, (**2010**), pp. 190-195.
[8] X. Liu, H. Wang and H. Lv, “Ann the illumination”, Network security situation awareness based on fusion of quantization, Journal of Jilin University (Engineering and Technology Edition, vol. 6, (**2013**), pp. 1650-1657.

[9] R. Chen, "The complex network threat modeling and detection technology research", The University of national defense science and technology, (**2013)**
[10] C. Wang, B. Zhang and G. Huang, "The attack strategy of mining and risk assessment model of attack based on full network", Computer engineering and applications, vol. 4, (**2012**), pp. 1-4.
[11] J. Ma, Y. Wang, J. Sun and S. Chen, "Study on the method of network security evaluation based on attack graph", Application Research of computers, vol. 3, (**2012**), pp. 1100-1103
[12] Y. Zhang, X. Tan, X. Cui and H. Xi, "Method of network security situation awareness based on Markov game model", Journal of software, vol. 3, (**2011**), pp. 495-508.

Author

Jieyun Xu, She received her B.S degree in computer Science from East China Institute of Technology, and received her M.S degree in computer Science from East China Institute of Technology. She is a lecturer in East China Institute of Technology. Her research interests include Computer science and technology.

Hongzhen Xu, He was born in china in 1976, and received his PHD degree in computers Software and theory from TongJi University. Currently, he is a professor in East China Institute of Technology. His research interests include software engineering, trustworthy software and computer network