International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.109-118
http://dx.doi.org/10.14257/ijsia.2015.9.1.12

Analysis Method based on Rough Attack-defense Bayes Game Model

Kai Zhang

School of Computer Sciences, Neijiang Normal University
NeiJiang 641100, China
Zk903@126.com

Abstract

In order to solve the strategic interdependence question during the attack and defense process in a complex network, the dissertation proposes an analysis method based on rough attack-defense Bayes game model. After defining the inner structure of attacking agent and defense agent, the dissertation extends traditional object Petri Net and introduces rough set theory into node domain and transition domain, then propose the network attack-defense confrontation model. By dividing domain attack strategy set into equivalence classes, the extraction method of characteristic attack strategy set is given. Then the rough game model and utility function of attack and defense agents are defined, accordingly, the solution of Bayes equilibrium strategy and maximal attack and defense strategy set are proposed. The analysis method can reduce the scale of strategic space of the game model, and suitable for researching on complex network attack and defense action.

Keywords: *Attack and Defense Strategy, Object Petri net, Rough Set, Game Theory*

1. Introduction

To find out the network security state must first clear what subjects exists in the network, security on the main play different roles in different network systems [1-2], such as access and communication of legal users although the consumption of certain cyber source (bandwidth, CPU, memory, etc.), but will not lead to deadly effect on the network service and communication function, the user data confidentiality; malicious attackers through a variety of means of attack attempt to interfere with network security, illegal access to confidential information, destroy the host and network function [3], their behavior is a network security system is the biggest threat; Network defense is to protect the network function in normal operation, the main protection of user data security transmission and storage, they monitor network information, network security situation analysis, prediction of network attacker behavior, and to have occurred and the impending attacks take safety protection measures, to save and protect cyber source. This can be seen. In any network attack scenarios are subject to the three main categories, including the attacker and defender is two characters have a major influence on network security [4-5].

Security trends and attacker and defender network this group confrontation forces are closely related, rational and two party in taking full analysis of other possible strategies adopted and return strategy, in order to determine the various strategy combinations, position and ultimately benefit the in network security situation of confrontation, and choose their own optimal strategy to predict each other may adopt strategy. As you can see, this is a defensive strategy of mutual influence, mutual dependence. Game theory is the study of various participants "battle of wits" forms and consequences (*i.e.*, between people in the interests of mutual restriction rational behavior strategies and corresponding results when an economic theory). In this paper, the theory is introduced into the network attack and defense research,

ISSN: 1738-9976 IJSIA

analysis of attacker and defender conflict in interests according to each other's behavior to reflect their best.

The game analysis of network attack and defense is still in the front stage, foreign scholars such as Lye [6], Burke [7], Liu [8] and others through the stochastic game, incomplete information game model to intrusion intention, goal and strategy of reasoning, the home also has a few papers [9-10] game theory was applied in the field of network security, and made great contributions to the development of this field. But the study is essential for the intrusion response system for the game analysis, belong to the post safety analysis method.

Jiang Wei and [11] proposed the analytical method of game based on active defense, the method must be based on the two party to attack each other strategies and utility explicitly informed, as a game of perfect information, cannot describe the differences between attacker strategy sets and utility under different attack ability. At the same time, the construction of defense map and its corresponding strategy analysis methods cannot adapt to the complex network demand, in complex network system, the attack path. Mold is huge, the attack path up to many hundreds in one of only 20 hosts within the LAN. If the attack path all added to the strategy of attack is not realistic to focus on the game analysis, so the application area of this model is limited [12-13].

Following consideration of the above problems, this chapter presents a confrontation based on network attack and defense model (Attack-Defense Confrontation Model, A-DCM) analysis of rough Bias game method, research of complex network system defense strategy confrontation situation. The attack and defense two parties as agent, they can make appropriate to reflect on their own environment, puts forward the design structure of the two intelligent body, and on the basis of its internal analysis and modeling and strategy gives the corresponding study method. This method can help defense under incomplete information to obtain the biggest defense strategy set and optimal active defense strategy set.

2. Generation of Offensive and Defensive Strategy based on Model of Network Attack Defense Confrontation

2.1. Define the Model of Network Attack and Defense Confrontation

In the network game, generating attack strategy and defense strategy are one of the keys. The extended a network attack defense confrontation model object Petri net, still use objects to describe a host node, interface of database objects to describe the host vulnerability state, based on this idea, in order to reflect the defense strategy of confrontation situation, for each attack change, define the corresponding defense strategy, and will attack and defense costs, the implementation of action income, attack complexity and defensive stop rate and other factors into the model.

Many functions and node attack relationship similar to the existence of a complex network, the same node also tend to have more similar vulnerabilities. The similarity between nodes and vulnerability of indiscernibility, an attacker can accord to their preferences were randomly selected, the defender to make accurate judgments. At the same time they cause redundancy in the analysis of network attack and defense strategy, the strategy space attacker with the exponential growth of the redundant information. In order to solve the above problem, the node object domain and transformation domain in attack path in the net on the division of equivalence classes, similar attacks and similar nodes into a class, building space mining help characteristic attack paths.

Because the characteristic attack paths with roughness in space, this chapter still rough set theory into object Petri net modeling, a definition of network attack defense confrontation model based on object Petri net rough extension, its definition is as follows:

Definition 1: REOPN of the rough extension object Petri net is defined as one 9 tuple:

$$REOPN=(O, P, T, \lambda, Tok, OA, S, R, R')$$

2.2. The Attack Strategy Set and Rough

Definition 2: equivalence partitioning on domain attack strategy sets.

Set Domain attack strategy set is $DASS=\{s_a^1, s_a^2, ..., s_a^n\}$, In a similar division relation R / R'.

$[s_a^i]_{R/R'} = \{s_a^j \mid s_a^i.Num\_obj = s_a^j.Num\_obj$ and $\forall t_h \in s_a^i, t_h \in s_a^j$

Definition 3: characteristic attack strategy set rough

In equivalence class space domain attack strategy set DASS, when CASS can be induced into equivalence classes and attack strategy, then CASS is R / R' precision attack strategy set. Otherwise, CASS is R / R' rough attack strategy set, then CASS can be too accurate strategy set $\underline{CASS}$ and $\overline{CASS}$ to approximate representation

3. Analysis of Game Theory based on Attack Defense Confrontation Model

3.1 The Definition of Attack Defense Game Model and the Largest Defense Strategy Set

Used rough extended object oriented Petri net modeling of attack defense confrontation situation can be set low level attack strategies attacker and a high level of the attacker and the corresponding defense strategy set respectively, these strategies with rough set, is proposed based on the concept of rough game, a game model of rough Bias and two party strategy of confrontation situation analysis. It is shown in Figure 1

Definition 4: rough attack defense game model (RA-DGM) is one 5 tuple:

$$RA\text{-}DGM=\{I, \Theta, p, S, U\}$$

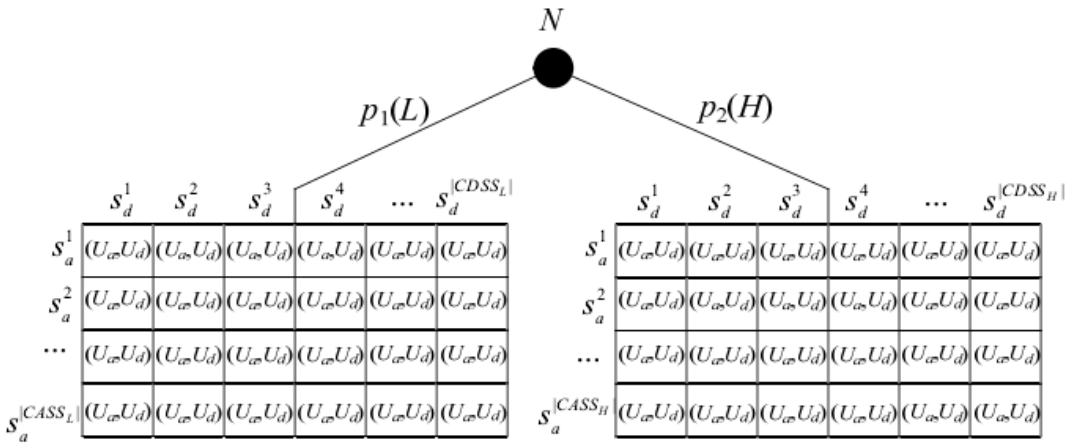

Figure 1. Static Bayes Game Strategies of Network Attack and Defense

Definition 5: maximum attack strategy set and maximum defense strategy set. Let the strategy set of attack defense game model set is

$$BNEStrategy=\{EquSolve_1, EquSolve_2,..., EquSolve_n\}$$

Definition 5 shows that equilibrium attack strategy sets the upper approximation for attackers to all possible optimal attack strategy, namely the maximum attack strategy set. In these attacks, to find out the change to belong to the same and balanced defense strategy set attack changes the focus of these changes, the defense strategy and balanced defense strategy belongs to the same type of strategy for the defense of all possible optimal defense strategy, namely the maximum defense strategy set.

3.2. The Utility Matrix Generation Algorithm of Offensive and Defensive Utility Matrix

Algorithm: $Umatrix\_generation(A\text{-}DCM, DASS_{L/H}, CASS_{L/H}, CDSS_{L/H})$

Input: $A\text{-}DCM, DASS_{L/H}, CASS_{L/H}, CDSS_{L/H}$

Output: $utility_{L/H}$, $utility_L$ and $utility_H$ were low level and high level attacker type utility matrix strategy, $utility_L$ corresponding strategy set is the CASSL, CDSSL, $utility_H$ corresponds to the set is strategies for CASSH, CDSSH, the two generation method is same

Description:

1 Initialization parameter in utility calculation:

$$P_t, P_r, P_k, P_c, P_i, P_a, P_{pr}, P_{cr}, P_{t'}, P_{r'}, \gamma_c, \gamma_i, \gamma_a, Q$$

2 The utility to create three-dimensional array $utility[x][y][2]$ to store $Agent_a$ and $Agent_d$ strategy of confrontation,

3 For $(i=0;i<x;i++)$

4 For $(j=0;j<y;j++)$

5 Calculated all contain $s_d^j(\delta_{ab}, \delta_{cd}, ...)$ strategy number $rblock\_num$ labeled transition attack in DASS

6 $rblock\_rate=rblock\_num/|DASS_{L/H}|$

7 If s_d^j had no defense effect on the s_a^i

8 $\{utility[i][j][0] = -\sum_{t_v \in s_a^i} AC(t_v) + \sum_{t_v \in s_a^i} AI(t_v) - rblock\_rate \times Q$

9 $utility[i][j][1] = -\sum_{t_v \in s_a^i} SD(t_v) - DC(s_d^j) + rblock\_rate \times Q\}$

10 Else

11 Search $s_d^j(\delta_{ab}, \delta_{cd}, ...)$ mark

12 $cur\_tran=th; sumAC=0; sumSD=0$

13 $while(pre(cur\_tran)!=Null)$

14 $\{cur\_tran=pre(cur\_tran); sumAC+=AC(cur\_tran); sumSD+=SD(cur\_tran)\}$

15 Delete all contain $s_d^j(\delta_{ab}, \delta_{cd}, ...)$ labeled transition attack strategy in DASS

16 $cur\_tran=th; sumAI=0$

17 $while(pre(cur\_tran)!=Null)$

18 $\{cur\_tran=pre(cur\_tran)$

19 flag=0;

20 if(cur_tran $\in s_a^k$) flag=1;break }

21 if(flag==1)

22 {while(pre(cur_tran)!=Null)

23 sumAI+=AI(cur_tran)}

24 sum_AC=0; sum_AI=0; sum_SD=0

25 while(all $t_v \in s_a^i$)

26 utility[i][j][0]=s_d^j.r×(-sumAC+sumAI-rblcok_rate×Q) +(1-s_d^j.r)
×(-sum_AC+sum_AI)

4. Experiment Design and Discussion

In order to illustrate the analysis of network attack defense game method, this paper establishes environmental test network. It is shown in Figure 2. The 57 network device, wherein the DMZ region 3 servers running, provides the service for the internal, external users: two Web servers running at the same time and configure load balancing, a SSH server. The internal LAN is divided into two parts: a server cluster and the user cluster. Server cluster has one backup server, database server and file server. Database server IP6 storage enterprise internal private data, backup server IP5 backup files on the IP6. IP6 has a trust relationship on IP5. Firewall enable external host can only access the DMZ regions of the host, cannot directly access the internal LAN; While the DMZ region in IP2, IP3 WWW services to the network database server IP7 to read and write data, does not have access to the LAN in the equipment; IP4 can access any host Host in Group. Supposing that hackers in Internet, intranet to access confidential business information on the IP6.

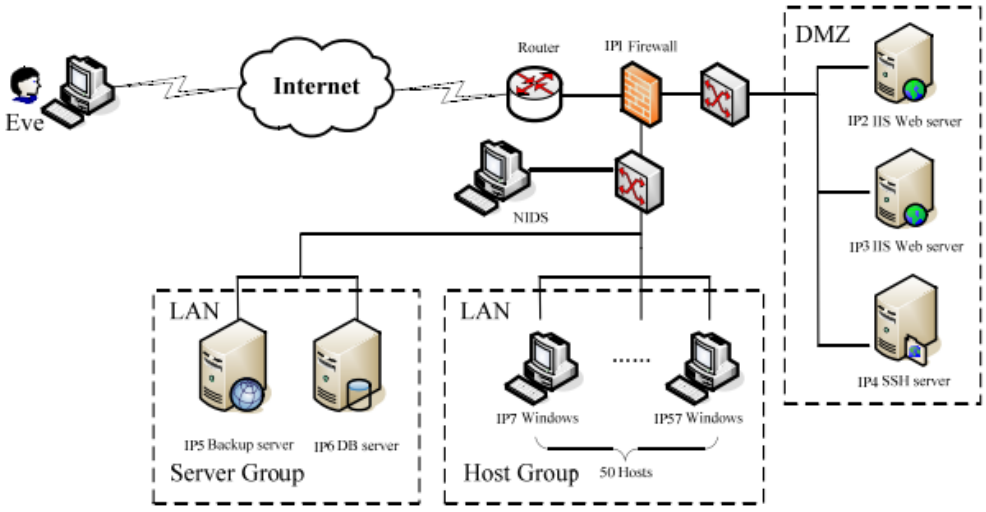

Figure 2. Test Network Topology

Scanning tools such as Nessus, use the OVAL, we can get the host an open service platform and loopholes, the network information and the vulnerability of the harm is shown in Table 1.

Table 1. Each Node on the Vulnerability and Access Relations

hid	service		leak-id	leak description	Result
IP1	/		12918	RedHat Linux telnet Overflow	Root
IP2 IP3	WWW FTP		8668 4855	Wu-Ftpd SockPrintf() IIS Buffer Overflow	Root Root/DOS
IP4	FTP SSH		8628	OpenSSH Buffer Overflow Weak Password	Root Root
IP5	ORACLE		38115	Oracle 11gR2 Remote command execution overflow	Root
IP7-IP57			31874	Windows Server Service remote Rpc overflow	Root

According to the relationship between the current access to collect network information as well as the host, generation of attack defense confrontation model, as shown in Figure 3.

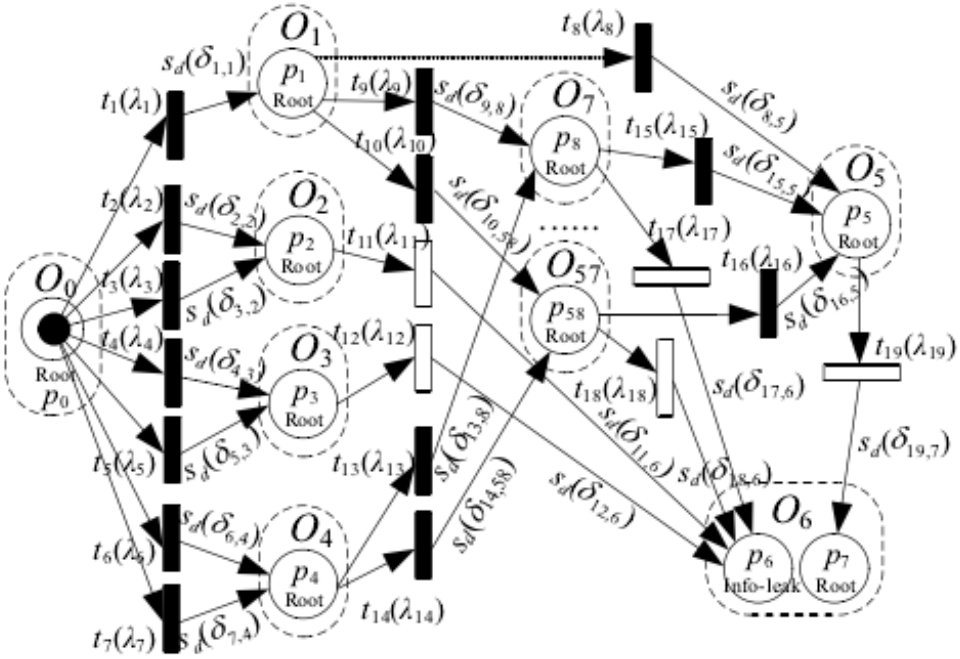

Figure 3. Attack Defense Confrontation Model based on Object Petri Net Rough Extension

The model reflects the defense relationship and node objects exist and changes on the domain of equivalence relation between two arbitrary nodes. Hollow transition diagrams that legitimate access behavior of node objects. Solid change said attacks illegal. O_0 showed the attacker object, O_i is corresponding IP_i in Figure3, user $IP8-IP56$, O_7, O_{56} and attack relationship are the same.

Where:

$\lambda_1 = <30,0.3,4/2,25>, \lambda_2 = \lambda_4 = <25,0.3,4/2,20>, \lambda_3 = \lambda_5 = <25,0.1,1/1,20>$

$\lambda_6 = <20,0.3,4/2,15>, \lambda_7 = <20,0.5,5,15>, \lambda_8 = \lambda_{15} = \lambda_{16} = \ldots = <35,0.7,10,25>$

$\lambda_9 = \lambda_{10} = \lambda_{13} = \lambda_{14} = \ldots = <15,0.3,4/2,10>, \lambda_{11} = \lambda_{12} = \lambda_{17} = \lambda_{18} = <30,0.2,3/1,25>$

$\lambda_{19} = <40,0.1,1/1,35>$

Table 2. Describes the Defense Strategy

Name	The corresponding defensive strategy number
Install the 12918 flaw patch	$s_d^1(\delta_{1,1}) = <30,30,3,1>$
Install the 8668 flaw patch	$s_d^2(\delta_{2,2}) = s_d^3(\delta_{4,3}) = <25,25,3,1>$
Install the 4855 flaw patch	$s_d^4(\delta_{3,2}) = s_d^5(\delta_{5,3}) = <25,25,3,1>$
Install the 8628 flaw patch	$s_d^6(\delta_{6,4}) = <20,20,3,1>$
Install the 31874 flaw patch	$s_d^7(\delta_{9,8}, \delta_{13,8}) = s_d^8(\delta_{10,58}, \delta_{14,58}) = \ldots <15,15,3,1>$
Modify the SSH login password	$s_d^9(\delta_{7,4}) = <20,20,3,0.8>$
Blocking the access port	$s_d^{10}(\delta_{11,6}) = s_d^{11}(\delta_{12,6}) = <30,30,20,1>$ $s_d^{12}(\delta_{17,6}) = s_d^{13}(\delta_{18,6}) = <30,30,10,1>$
To change the host trust relationships	$s_d^{14}(\delta_{19,7}) = <40,40,5,1>$

Classification of node objects in Figure3 domain and change domain are as follows:

$O / R' = \{O_1, \{O_2, O_3\}, O_4, \{O_7, O_8, \ldots, O_{57}\}, O_5, O_6\}$

$T / R = \{t_1, \{t_2, t_3, t_4, t_5\}, t_6, t_7, \{t_9, t_{10}, t_{13}, t_{14}, \ldots\},$

$\{t_{11}, t_{12}, t_{17}, t_{18}, \ldots\}, \{t_8, t_{15}, t_{16}, \ldots\}, t_{19}\}$

According to 2.2 formation characteristics of attack / defense strategy set:

$CASS_L = \{ s_a^1 = O_0.p_0, t_1, O_1.p_1, t_9, O_7.p_8, t_{17}, O_6.p_6;\ s_a^2 = O_0.p_0, t_2, O_2.p_2, t_{11}, O_6.p_6;$

$s_a^3 = O_0.p_0, t_6, O_4.p_4, t_{13}, O_7.p_8, t_{17}, O_6.p_6; \}$

$CASS_H = \{ s_a^1 = O_0.p_0, t_1, O_1.p_1, t_9, O_7.p_8, t_{17}, O_6.p_6;\ s_a^2 = O_0.p_0, t_2, O_2.p_2, t_{11}, O_6.p_6;$

$s_a^3 = O_0.p_0, t_6, O_4.p_4, t_{13}, O_7.p_8, t_{17}, O_6.p_6;$

$s_a^4 = O_0.p_0, t_1, O_1.p_1, t_8, O_5.p_5, t_{19}, O_6.p_7;$

$$s_a^5 = O_0.p_0,\ t_1,\ O_1.p_1,\ t_9,\ O_7.p_8,\ t_{15},\ O_5.p_5,\ t_{19},\ O_6.p_7;$$

$$s_a^6 = O_0.p_0,\ t_6,\ O_4.p_4,\ t_{13},\ O_7.p_8,\ t_{15},\ O_5.p_5,\ t_{19},\ O_6.p_7;$$

$$s_a^7 = O_0.p_0,\ t_7,\ O_4.p_4,\ t_{13},\ O_7.p_8,\ t_{15},\ O_5.p_5,\ t_{19},\ O_6.p_7;$$

$$s_a^8 = O_0.p_0,\ t_7,\ O_4.p_4,\ t_{13},\ O_7.p_8,\ t_{17},\ O_6.p_6;\ \}$$

$$CDSS = \{\ s_d^1(\delta_{1,1}),\ s_d^2(\delta_{2,2}),\ s_d^6(\delta_{6,4}),\ s_d^7(\delta_{9,8},\delta_{13,8}),\ s_d^{10}(\delta_{11,6}),\ s_d^{12}(\delta_{17,6}),\ s_d^9(\delta_{7,4}),$$

$$s_d^{14}(\delta_{19,7})\ \}$$

Let $Q=10, p_1(L)=0.7, p_2(H)=0.3$ by Umatrix_generation can be obtained Offensive and defensive utility matrix

$utility_L =$

	s_d^1	s_d^2	s_d^6	s_d^7	s_d^{10}	s_d^{12}	s_d^9	s_d^{14}
s_a^1	(−4.8,31.8)	(48.9,−77.9)	(44.2,−73.2)	(21,−18)	(48.8,−94.8)	(16.8,−22.8)	(49,-78)	(49,-80)
s_a^2	(33.2,−53.2)	(−0.1,22.1)	(33.2,−53.2)	(37.8,−57.8)	(−4.2,−14.8)	(37.8,−64.8)	(38,-58)	(38,-60)
s_a^3	(34.2,−63.2)	(38.9,−67.9)	(−4.8,21.8)	(10.8,−7.8)	(38.8,−84.8)	(6.8,−14.8)	(39,-68)	(39,-70)

$utility_H =$

	s_d^1	s_d^2	s_d^6	s_d^7	s_d^{10}	s_d^{12}	s_d^9	s_d^{14}
s_a^1	(−3.28,30.28)	(55,−78)	(51.75,−74.75)	(22.8,−17.8)	(55,−95)	(30.9,−24.9)	(51.75,−74.75)	(50.1,−75.1)
s_a^2	(38.72,-54.72)	(-0.03,22)	(38.75,-54.75)	(41.8,-57.8)	(-2.07,-14.9)	(41.9,-64.9)	(38.75,-54.75)	(37.1,-55.1)
s_a^3	(41.72,-64.72)	(45,-68)	(-3.25,20.25)	(12.8,-7.8)	(45,-85)	(20.9,-14.9)	(41.75,-64.75)	(40.1,-65.1)
s_a^4	(−3.28,30.28)	(49,−108)	(45.75,−104.75)	(48.8,−107.8)	(49,−125)	(48.9,−114.9)	(45.75,−104.75)	(8.1,−25.1)
s_a^5	(−3.28,30.28)	(80,−123)	(76.75,−119.75)	(22.8,−17.8)	(80,−140)	(79.9,−129.9)	(76.75,−119.75)	(26.1,−40.1)
s_a^6	(66.72,−109.72)	(70,−113)	(−3.25,20.25)	(12.8,−7.8)	(70,−130)	(69.9,−119.9)	(66.75.−109.75)	(16.1,−30.1)
s_a^7	(63.72,−109.72)	(67,−113)	(63.75,−109.75)	(9.8,−7.8)	(67,−130)	(66.9,−119.9)	(10.8,−6.4)	(13.1,−30.1)
s_a^8	(38.72,−64.72)	(42,−68)	(38.75,−64.75)	(9.8,−7.8)	(42,−85)	(17.9,−14.9)	(5.8,2.6)	(37.1,−65.1)

In this paper, there is not any pure strategy equilibrium solution, this game is a finite game. There must be a mixed strategy equilibrium. Bias equilibrium can be obtained by BNEStrategy_generation algorithm and the network game solution. Low levels of the attacker respectively with probability (0.422, 0.237, 0.339) to select the attack strategy (s_a^1, s_a^2, s_a^3), high level of an attacker with probability (0.431, 0.35, 0.217) to select (s_a^7, s_a^1, s_a^3) is the best choice of attack strategy. In all kinds of high and low level attack strategies under section, the defender with the probability 0.362 to select $s_d^7(\delta_{9,8}, \delta_{13,8})$, with probability 0.346 to select $s_d^1(\delta_{1,1})$ $s_d^1(\delta_{1,1})$ .With probability 0.291 to select $s_d^6(\delta_{6,4})$ is optimal defense strategy. The optimal strategy of roughness in both offensive and defensive strategies in the domain of equivalence classes, according to definition5, set the maximum attack strategy can get the experimental network and the maximum defense strategy sets are as follows:

$$maxASS=\{\{O_0.p_0,t_1,O_1.p_1,t_9,O_7.p_8,t_{17},O_6.p_6;\ \ldots\ ;O_0.p_0,t_1,O_1.p_1,t_{10},O_{57}.p_{58},t_{18},O_6.p_6;\},$$
$$\{O_0.p_0,t_2,O_2.p_2,t_{11},O_6.p_6;\ O_0.p_0,t_3,O_2.p_2,t_{11},O_6.p_6;\ O_0.p_0,t_4,O_3.p_3,t_{12},O_6.p_6;$$
$$O_0.p_0,t_5,O_3.p_3,t_{12},O_6.p_6;\}$$
$$\{O_0.p_0,t_6,O_4.p_4,t_{13},O_7.p_8,t_{17},O_6.p_6;\ldots;O_0.p_0,t_6,O_4.p_4,t_{14},O_{57}.p_{58},t_{18},O_6.p_6;\}$$
$$\{O_0.p_0,t_7,O_4.p_4,t_{13},O_7.p_8,t_{15},O_5.p_5,t_{19},O_6.p_7;\ldots;O_0.p_0,t_7,O_4.p_4,t_{14},O_{57}.p_{58},t_{16},$$
$$O_5.p_5,t_{19},O_6.p_7;\}\}$$

The following types of strategies to reflect these four groups of maximum attack strategy set respectively:

Attacker → firewall →LAN ordinary user →The LAN database server

Attacker →Web server →the LAN database server

Attacker →FTP server →LAN ordinary user →The LAN database server

Attacker →FTP server →LAN ordinary user →backup server →The LAN database server

$$maxDSS=\{s_d^1(\delta_{1,1}),s_d^6(\delta_{6,4}),\{s_d^7(\delta_{9,8},\delta_{13,8}),s_d^8(\delta_{10,58},\delta_{14,58}),\ldots\}\}$$

The largest defense strategy reflects the defender should consider to repair the firewall, FTP server and the existence of the user holes in LAN machine

From the above analysis we can see, the high level tend to use more attack the high complexity of the attack, this is because they prevent rate is low (such as the defender to modify your password and cannot guarantee that will not be high level again, and the attacker cracked) some vulnerabilities have not issued security patch (such as 38115), more easy to avoid defense stop.

At the same time, high / low level of preference to choose the attacker node important degree and high correlation attack, in order to get benefit more and more alternative strategies. Because the access to the DB server through a network user clusters to steal enterprise data dominated in the strategy space, high cost and limited defense negative host access, thus early repair leaks on the user machine is the best strategy ($s_a^7, s_a^8, \ldots$), the attack path can effectively prevent the 98.3%.

A firewall node important degree and by changing the filter settings can directly attack intranet any host and backup server, so $s_d^1(\delta_{1,1})$ has a high probability of selection

Because FTP has access to the user through the cluster, FTP can attack the arbitrary choice of a user machine as a springboard, so it is more than Web server has more attacking options and attack is more harmful, should consider the defense strategy $s_d^6(\delta_{6,4})$

5. Conclusion

This paper not only studies the behavior and strategy, but considering the attacker and defender strategy of mutual restriction and dependence. Proposed a new defense model structure - attack defense confrontation model based on object Petri net rough extension, based on rough set theory and the traditional Bias game combination, equivalence partitioning in the attack and defense strategy space, by extracting the features from each equivalence class attack strategies to remove the redundant information in complex networks, reduction the strategy space scale, so that the application of game theory in the study of network attack and defense is more widely.

References

[1] S. Zhang, W. Liu and J. Wei, "Evaluation method for network risk quantification based on game theory model", Journal of Information Engineering University, vol. 2, (**2014)**, pp. 156-162.
[2] S. Wang, G. Yin, H. m. Zhan and J. Liu, "The analysis of Bias game entities in the software system of network configuration", Computer Engineering, vol. 02, (**2014)**, pp. 52-57.
[3] G. Liu, H. Zhang and Q. Li, "Optimal defense network security decision method based on game theory model", Journal of Nanjing University of Science and Technology, vol. 01, (**2014)**, pp. 12-21.
[4] F. Yu, K. Chan, X. Wu and Y. song, "Select the network attack and defense strategies based on stochastic game model", Journal of Beijing University of Posts and Telecommunications, vol. S1, (**2014)**, pp. 35-39.
[5] K. Chan, X. Wu, Y. Fu and Y. song, "Network security evaluation of stochastic game and network based on entropy", Journal of Beijing University of Posts and Telecommunications, vol. S1, (**2014**), pp. 92-96.
[6] K. W. Lye and J. Wing, "Game strategies in network security", School of Computer Science, Carnegie Mellon University, Pittsburgh, Technical Report: CMU-CS-02-136, (**2002)**.
[7] D. Burke, "Towards a game theory model of information warfare", Airforce Institute of Technology, Technical Report: AFIT/GSS/LAL/99D-1, (**1999)**.
[8] P. Liu and W. Zang, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", Proceedings of the 10th ACM Computer and Communications Security Conference (CCS'03). Washington, DC, (**2003),** pp. 179-189.
[9] stone, L. Yin and X. Li, "The intrusion dynamics based on game theory", Research and development of computer, vol. 45, no. 5, (**2008)**, pp. 747-757.
[10] Shi, S. Guo and Y. Lu, "An intrusion response method based on attack graph", Journal of software, vol. 19, no. 10, (**2008**), pp. 2746-2752.
[11] J. Wei, B. Fang and T. Zhihong, "Attack defense game model of network security evaluation and optimal active defense based on", Chinese Journal of computers, vol. 32, no. 4, (**2009**), pp. 817-825.
[12] S. Zhang, J. Li and X. Chen, "Dynamic game theory of distributed denial of service attack defense based approach", Journal of Shanghai Jiao Tong University, vol. 42, no. 2, (**2008)**, pp. 198-201.
[13] Y. Guo and J. Ma, "Game theory of adaptive network intrusion detection and response based on the framework", Systems engineering and electronics, vol. 27, no. 5, (**2005)**, pp. 914-917.

Author

Kai Zhang, he is currently an associate professor in school of computer sciences of Neijiang Normal University. His research interests include information technology.

