International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.69-78
http://dx.doi.org/10.14257/ijsia.2015.9.7.06

Network Attack Defense Awareness based on Dynamic Game

[1]Man Li and [2]Jinjing Cao

[1,2]Shandong Huayu University of Technology,
Dezhou, ShanDong 253034, china
[1]xdclm@126.com, [2]Lancaoer19831230@163.com

Abstract

By defining attack-defense action sequence and utility function of both sides, combine with dynamic Bayes game theory to analyze the confrontation and interdependence between the two agents' strategies. Dynamic Bayes attack-defense game model can describe each possible strategy in every stage. This paper proposes the construction method of game extensive form by utilizing attack-defense confrontation model, and presents the equilibrium strategy solution algorithm.

Keywords: *Network Security, Attack Model, Attack and Defense Strategy, Game Theory*

1. Introduction

Static game can't reflect the temporal sequence of acts by the attack side and the defense side [1-2]. When the attack behavior happens, the defendant can't change its defensive strategy in the real time by only counting on what's observed. So the model is not workable if used to study the dynamic confrontational situations in the generating process of attack and defense behaviors [3-4]. The scope of its application is limited. To overcome the aforesaid shortcomings, we propose the use of multistage gaming strategy based on incomplete information to describe situations between both sides. The new model is more universal than the former one [5-6].

On that basis, we develop a dynamic gaming method of incomplete information based on attack defense model to probe into the whole countervailing course of attack and defense in network systems and the choice of strategy [7-8]. After the acting sequence of both sides and the method for quantifying strategy effectiveness are defined, the constructing algorithm of attack-defense game's extensive form is developed; and also the generation method of perfect Bayesian equilibrium is discussed. In the end, by citing examples, it introduces the new method and proves its correctness. The defendant can get the best active defending strategy set and the best passive defending strategy set in each phase while considering fully its own strategy and the attacker's [9-10] . The proposed method shows completely the situation and tendency of strategy confrontation at each of both the attack and defense stages [11]. That helps the defendant in finding out the optimal counter strategy accurately and timely before and after the attacking behavior happens, solving the problem with strategy preferential selection in the changing situations of network attack and defense [12-13].

2. Dynamic Attack and Defense Game Model based on Incomplete Information

In real life, network attack and defense is usually a multistage process of strategy confrontation. At each stage, *i.e.* in every possible security situation, either the attack side or the defensive side would forecast any possible acts taken by the other side in the

ISSN: 1738-9976 IJSIA

next phase, by according to network information they collect and observed historical conducts of the counterparty, as for them to decide the best strategy in the next period.

The following example illustrates multi-stage dependence phenomenon of attack defense strategy.

Some attackers decided to attack the internal LAN hosts to obtain the Root permissions, the attacker can use the buffer overflow attack and weak password attack in two ways. Assumptions regarding the host vulnerability of buffer overflow attack has an existing mode of attack, the attack cost is much lower than the latter, in the previous analysis of the attacker will use the former, but if the installation of intrusion detection system to detect the entrance of the LAN attacker, then the attacker will choose weak passwords to obtain permission to attack the host, because the IDS is able to detect this kind of attack, and shielding the attacker's IP, at this time the attacker spent a certain attack cost, but income is 0, and the IP is shielded "punishment" back to the attacker to bring negative effect.

If used weak password attack, although attack cost is higher, but the other attacker can achieve its purpose and positive returns, the attacker will take a weak password attack in the strategy of balance, the attacker can access to the host on the Root permissions and implant malicious code, if the attack defense confrontation process has not ended, the defender also has two kinds of strategies to resist an attack:

(1)Scanning system, clear the virus program and delete the doubtful account;

(2)Re-install the system, and change the system all the account password. When the defensive side to take the first way, defense cost is low but the internal system still remained partial backdoor programs cannot be deleted, the attacker can continue to use this backdoor attack, or use other account again obtain permission, defending party finally still will suffer heavy losses. If adopt second ways although defense cost is high, but can completely remove the attacker's threat, this time the attacker will pay no income attack cost. Based on the above consideration, the confrontation process description of the case is shown in Figure 1.

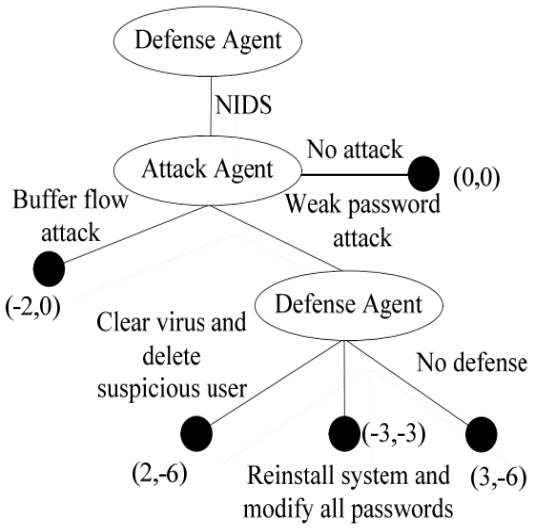

Figure 1. Instruction of Attack and Defense Strategies

2.1. Analysis of the Type of Attack-defense Game

Firstly, in the attack-defense game, the defendant knows not completely the information which is acquired by the other side. This is called incomplete information game.

Secondly, there is “before” and “after” for acts taken by the attack Agent and the defense Agent. As mentioned before, the defending party installs IDS system in the

beginning; then the attacker launches attacks. After being attacked, the defender takes passive defense measures. There is before and after for their acts of choice. And there are consecutively interrelated time phases. The attack Agent dynamically adjusts its attack strategies like attacking way, data packet sending rate, randomness of forged IP etc. as per the detected defensive actions taken by the counter Agent. The defendant side can make strategies like changing firewall filtering rules, setting host security strategy, upgrading the system and anti-virus software etc. to react to possible attack behaviors by the other side. Obviously the attack-defense game is changeable and involves multiple stages.

Thirdly, with network tools (such as detector, scanner) or trial attacking method, the attack side can perceive the defending strategy taken by the defensive party in the last period. At the same time, the defending side can learn instantly of aggressive behaviors of the attacker by virtue of security mechanism like network and host IDS, anti-virus software, monitoring devices. Hence the whole attack-defense procedure is noticeable to both sides.

Thus, the network attack-defense process is a dynamic game based on incomplete information. The incompleteness of information in the game can be interpreted as the incomplete knowledge about the counterparty's type. Such a game can be transferred through the Harsanyi transformation method to the complete but not perfect information dynamic game.

2.2. Definition of Elements in the Attack-defense Gaming Model

Here we need to investigate the best passive defending strategy in one attack situation and also the active defending strategy before the attack is launched. For the sequential arrangement of attack-defense acts, we start our work with the defendant, from the defensive strategy field sets to choose applicable active defending measures, such as restoring devices' loopholes, backup of data and files, installing IDS security detection system. Then, the intruder launches attacks. The sequence of their behaviors is temporally described as follows: the defendant selects defensive tactics from the active strategy sets before the attack happens; then the attacker chooses one attacking way from the available strategy sets as to initiate the attack. To some specified attacking way, the defending side selects some passive protective strategy to respond. Such response includes special type defense and observed type defense. The special defensive strategy refers to those with stoppage effect. Different strategies have different preventive. Some strategies can prevent utterly, *e.g.* re-configuring firewall making the attacker impossible to use any more the original IP for attack except finding another way. Some strategies can prevent partially, *e.g.* close service for 10minutes or removal of one suspicious user's progress. Such attacking approaches can delay or impede the attacker's behaviors, but it's not possible to prevent the attacker from using other methods to do the same thing. The observed type defense means once some dubious actions are perceived, log information is recorded or no any defending action is taken before further observation of the attacker's next intention; till this moment, it's possible to launch subsequent attacks in the original path. Under the two circumstances, the game is over:

(1) Defending measures taken by the defendant Agent at every stage can block utterly all attacks by the attacker from every path;

(2) The attacker realizes its attack goal. In other cases, both sides alternately make decisions.

The sequence of multistage game between the attack and the defending side is portrayed in Figure 2. There, x_j^k stands for the jst decision point of the defendant Agent or the attack Agent in the kst period of the game; $a_{a/d}^i$ is the strategy taken by either Agent in one period of the game. N is a natural, $p_1, p_2, ..., p_n$ denotes the

$\theta_1, \theta_2, ..., \theta_n$ probability of natural selection of various types. (U_a, U_d) said that the gain utility at the end of the process.

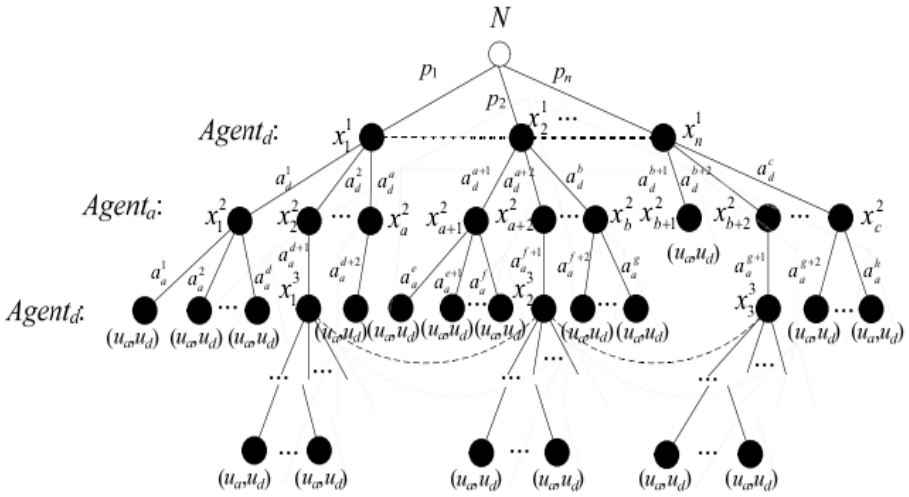

Figure 2. Game Extended of Attack Defense Confrontation

2.3 Network Attack-defense Model

The descriptive method for attack-defense confrontation still uses the idea of extended time Petri net which is based on objects. To represent the contention of attack and defensive strategies, the model shows not only the tactics taken by the attacker and the set of defending strategies taken by the defendant regarding one attack behavior, as well as costs paid for and benefits earned from carrying out such strategies, laying foundation for analyzing the game. The model can be defined as follows:

Definition1: A-DCM is defined as a 10 tuple:

$$\mathbf{A-DCM} = (O, P, T, \lambda, Tok, OA, S, O(p_i), I(t_i), O(t_i))$$

A-DCM can help to establish the dynamic game expansion shape, it describes various factors in game theory model

2.4. Analysis of Dynamic Game in the Attack-defense Model

Before performing gaming analysis in the attack-defense confrontation model, it's required to transform the attack path to the descriptive pattern of game's extensive form as indicated in Figure 2. It clearly defines the temporal sequence of attack and defensive acts and the sets of possible tactics taken at every stage. By simulation, we can analyze actions taken by both the attack Agent and the defense Agent in each phase, helping the defendant in making prompt and right judgment and adopting the best countering solution when attack actions are approaching. The extensive form of the game is defined hereunder:

Definition2: Expand of attack defense confrontation game as

$$\text{A-DCGEF} = \{I, \Theta_a, seq, A, X, pre(x), succ(x), action(x), k(x), a(x), h(x), p, u\}$$

Through the game factors information continuously extracted from the attack defense confrontation in the Petri net model. According to the order of attack and defense actions to simulate all possible attack scenarios, the attack defense confrontation model is converted into the game extended shape. Attack defense confrontation game extended the following construction algorithm.

Algorithm: A-DCGEF ()

Input: A-DCM, I, Θ_a, seq, ρ

Output: A-DCGEF
Description:

(1) Initialization. Create node set X, Information collection $H=\{H_N, H_a, H_d\}$, Action set $a(x)$.

(2) Create node x_1^1, x_2^1, $pre(x_1^1)=x_0^0$, $pre(x_2^1)=x_0^0$

(3) $a(x_1^1)=a(x_2^1)=\{a_d^1, a_d^2, ..., a_d^n\}$

(4)for (Corresponding to each defensive action a_d^i)

(5) Create node x_i^2, x_{n+i}^2

(6) $h_{++num} \leftarrow x_i^2, x_{n+i}^2$

(7) while(node_queue$\neq \varnothing$)

(8) {Remove a node x_j^2 from the end of the node_queue

(9) while($\forall t_i \in O(O_0, po)$ in A-DCM

(10) if(t_i stimulate in the defensive $action(x_j^2)$)

(11) flag=0

(12) while(node_queue$\neq \varnothing$)

(13) {queue node_queue belongs to the same set of information entry into h_{++num}}

(14) remove a node x_j^k from the tail of node_queue

(15) Search $action(x_j^k)$ to corresponding t_i in A-DCM

Through the above algorithm can get defensive and offensive action alternate game tree structure, the structure of each node with the termination of both sides of the utility value together form the dynamic game model.

3. Experiment Design and Discussion

To describe and validate the analysis method used in the attack-defense model, we create the attack-defense scenario as seen in the following:

The network topology in the experiment is shown in Figure 3. The attacker Eve is located in the external network. Protective devices like firewall and IDS exist between the exterior and local network. The firewall allows the external hosts to access only the host in DMZ area, rather than direct visit to the internal local network. In the isolation area DMZ, there are two hosts responsible for providing services to outer net users. IP2 is an IIS Web server, with IIS ASP remote buffer overflow vulnerabilities (BID: 18858). IP3 is an SSH server running RedHat Linux, providing FTP services. Its OpenSSH buffer zone manages and manipulates remote overflow vulnerabilities including AS3 (BID: 8628). IP2 has trust relation to IP3. The inner net includes one PC and one DB server. DB server is Oracle database type, with Windows operating system. There is Oracle TNS Listener remote buffer overflow leak (BID: 4845). PC installs Windows operating system, with RPC overflow and deformed SMB packet remote data destroy loopholes (BID: 8152). WWW service in Web server allows data reading and writing to DB server, which has trust relationship with SSH server.

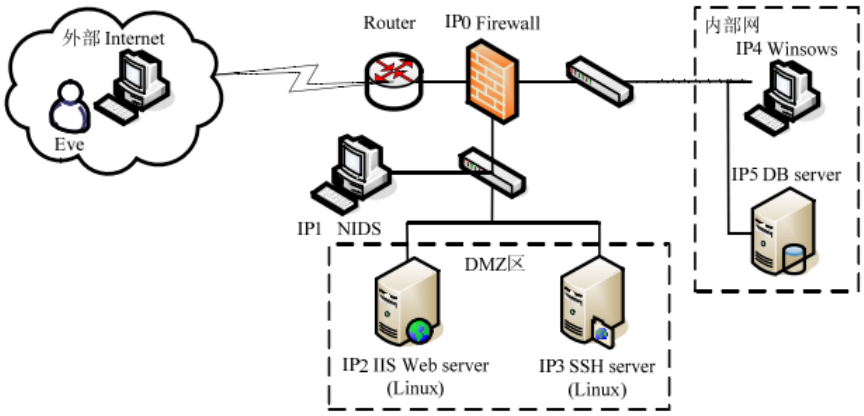

Figure 3. Diagram of the Experimental Network Topology

Assume the attacker Eve attempts to acquire from DB server in the internal net the classified information or Root authority. Based on the above information, we can build a network attack-defense model, which depicts attacking relationship of the attacker to various vulnerabilities in the network device and every accessible path to the attack targets.

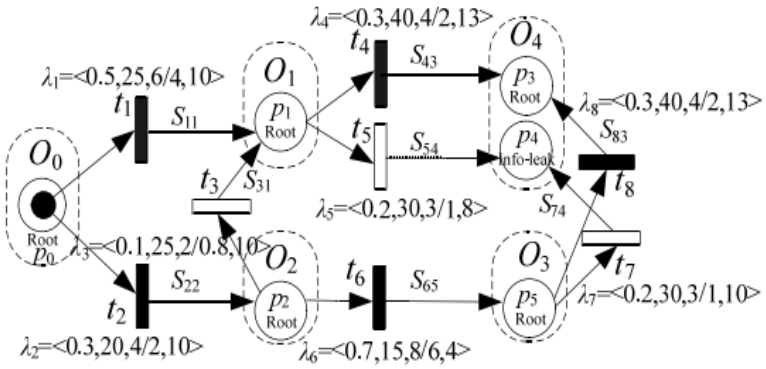

Figure 4. Attack Defense Confrontation Model of Test Network

In Figure 4, target O_i corresponds to network host IP $(i+1)$. The defensive (both active and passive) strategies of dynamic attacking actions.

With A-DCGEF () algorithm, we transform the attack-defense model as indicated in Figure 4 to the extensive form of attack-defense game as in Figure 5. Then we get attack-defense effectiveness (Q=10) on terminal nodes under each combined strategy. In Figure 5, the attack corresponding to the attack t_i in Fig. 4. As the attack ability of the low-level attacker L is limited, both attack t1 and t6 of which the complexity ≥0.5 can't be triggered. So it attacks firstly IP3 for Root permission. After obtaining the power of management and control over Web server with its trust relationship to the server, the attacker acquires confidential information from the inner net database by:

(1) Monitoring locally WWW service password for DB server to read and write information illegally;

(2) Utilizing directly Oracle TNS Listener overflow vulnerability to attack DB server for Root permission to thus create its own account under its full control. The sophisticated attacker H is not restricted by the complexity. It can take more extensive attack strategies than L. That's why the right branch of the game tree is more gigantic than the left.

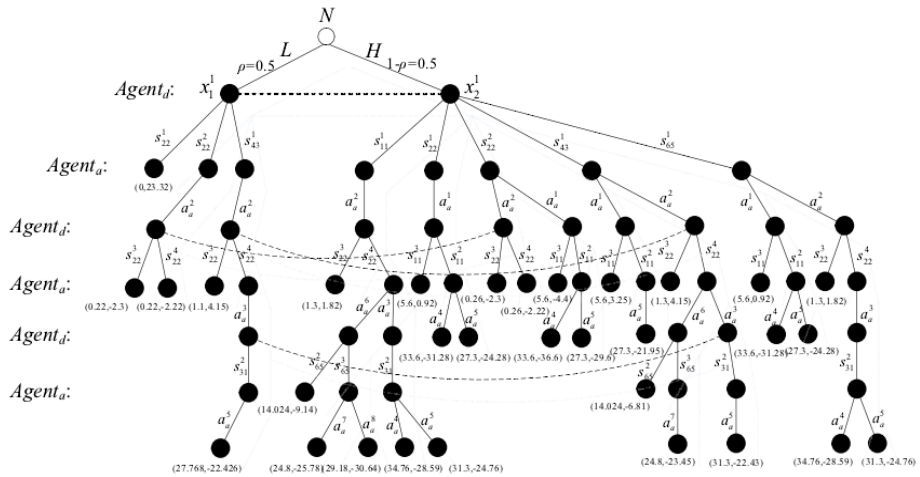

Figure 5. Game Extended of Test Network

Suppose the natural priori probability for the attacker L and H: $p(L) = p(H) = 0.5$. In practice, the probability can be reached through experience or statistical data in some time frame. At the start of the game, the defendant chose active defending actions from the set of active defending strategies in Table 1. In the experiment environment, to ensure normal operation of network communication and service, the access configuration of firewall and the trust relationship of accessing among hosts are not alterable unless in emergencies. So $Agent_d$ active defending measures are only focused on the selection of restoring loopholes of each node. The selection of each measure will have impacts on the attacker's strategy. We see from the branches under L, the recovery of SSH related bugs (s_{22}^1) will make low-level attackers unable to launch attacks. Though s_{22}^2 can't prevent them from utilizing the leak, through authority separation mechanism, attackers are confined to the restricted chroot environment, minimizing the impacts. At the moment, the attacker can counter against IP3, but it's impossible for it to execute subsequent attacks as the acquired permission can't make use of the trust and access relationship. For the goal, the attacker spent a lot as to attack the loop 8682, but it didn't achieve the purpose. It is called negative utility. After taking active countermeasures, the defendant rectified its prior belief in the type of the attacker by referring to the attacker's performance and got the posterior belief. Calculated by Bayes principle, after the latter made the attack, the defendant Agent's posterior belief in the attacking Agent changed to:

$$\tilde{p}_d(L \mid a_a^1) = \frac{p_d(L \mid h_t) \cdot p_d(a_a^1 \mid L)}{p_d(L \mid h_t) \cdot p_d(a_a^1 \mid L) + p_d(H \mid h_t) \cdot p_d(a_a^1 \mid H)}$$

$$\tilde{p}_d(H \mid a_a^1) = \frac{p_d(H \mid h_t) \cdot p_d(a_a^1 \mid H)}{p_d(L \mid h_t) \cdot p_d(a_a^1 \mid L) + p_d(H \mid h_t) \cdot p_d(a_a^1 \mid H)}$$

$$\tilde{p}_d(L \mid a_a^2) = \frac{p_d(L \mid h_t) \cdot p_d(a_a^2 \mid L)}{p_d(L \mid h_t) \cdot p_d(a_a^2 \mid L) + p_d(H \mid h_t) \cdot p_d(a_a^2 \mid H)}$$

$$\tilde{p}_d(H \mid a_a^2) = \frac{p_d(H \mid h_t) \cdot p_d(a_a^2 \mid H)}{p_d(L \mid h_t) \cdot p_d(a_a^2 \mid L) + p_d(H \mid h_t) \cdot p_d(a_a^2 \mid H)}$$

Due to the low level of the attacker cannot use t_1, which adopted attack action a_a^1 .So, $p_d(a_a^1 \mid L) = 0$ .Then $\tilde{p}_d(L \mid a_a^1) = 0, \tilde{p}_d(H \mid a_a^1) = 1$. Get $p_d(a_a^i \mid \theta_{attack})$ according to the historical data statistics. It shown in table1

Table 1. $p_d(a_a^i \mid \theta_{attack})$ **Value Table**

$p_d(a_a^i \mid \theta_{attack})$	a_a^1	a_a^2	a_a^3	a_a^4	a_a^5	a_a^6	a_a^7	a_a^8
L	0	0.74	0.81	0.37	0.62	0	0.62	0.37
H	0.67	0.58	0.77	0.44	0.53	0.57	0.53	0.44

If the attacker takes action a_a^1 , it's certain it's high-level; if the attacker takes measure a_a^2 , the posterior probability $\tilde{p}_d(L \mid a_a^2) = 0.55, \tilde{p}_d(H \mid a_a^2) = 0.44$ can be reached of the attacker's type. When the defendant Agent finds the attacker choosing a_a^5 in the following attack, the former will correct its belief in the type of the attacker's attacks, we regard the belief formed in the last stage as prior information. $\tilde{p}_d(L \mid a_a^2) = \dfrac{0.55.p_d(a_a^5 \mid L)}{0.55.p_d(a_a^5 \mid L) + 0.44\,p_d(a_a^5 \mid H)}$ .We can learn that when the attacker adopts continuously less complicated attacking modes, the possibility of the attacker being low-level becomes increasingly higher.

When the attack behavior has not taken place, the defendant's choice of s_{22}^1 is the optimal active defensive strategy. For the moment, it's impossible for the low-level attacker to counter back and the sophisticated attacker can choose only a_a^1. When the defending side detects attack a_a^1, it can execute passive defensive strategy s_{11}^3 to intercept the attacker's IP for protecting network system. From the analysis of merely the right branch of game's extensive form, we note that for the sophisticated attacker, the active defending strategy's utility reaches $u_d(s_{43}^1) > u(s_{11}^1) > u_d(s_{22}^1)$. That is because restoring loopholes in DB server can help effectively avoiding remote attacks by the attacker and simultaneously getting Root permission, potential damages by such attacks being reduced to the minimum. When the defendant takes s_{11}^1, the attacker can only choose to attack SSH server (a_a^2). Comparatively, when the defendant takes s_{22}^1 and the attacker hits IIS server (a_a^1), a_a^2 is detected more likely than a_a^1 , more probably to take the passive defense. Therefore, s_{11}^1 is more secure than s_{22}^1 . But if the defendant doesn't know the attacking type, the active defensive strategy expected utility is $Eu_d(s_{22}^1) > Eu_d(s_{43}^1) > Eu_d(s_{11}^1)$. That is because implementing s_{22}^1 can block off all attacking paths of the low-level attackers, decreasing greatly the possibility of network system being attacked. If the attack a_a^1 occurs, it's affirmative that the attacker is sophisticated.

4 Conclusion

In view of the lack of modeling and analysis in active defense technology. This paper presents Network Attack Defense Awareness based on dynamic game of incomplete information. This method can describe the attack may occur in network system. In order to predict the optimal path of attack defense, and to advance the development of active and passive defense measures provide study basis effectively.

References

[1] H. Chen, "Research on cloud security attack and defense strategies and security technology evaluation based on game theory", Yunnan University of Finance and Economics, (**2014).**
[2] Z. Wang, H. Jo, Z. Li and Y. Zhao, "Secret strategy research of incomplete information dynamic game model based on science and technology", System engineering theory and practice, vol. 12, (**2013**), pp. 3182-3189.
[3] J. Zhu, B. Song and Q. Huang, "Evolution game model of network security attack and defense based on system dynamics", Journal of China Institute of communications, vol. 1, (**2014**), pp. 54-61.
[4] X. Chen, M. Zhao and G. Xu, "Fuzzy dynamic game of UAV air combat based on Multi Strategy", EO and control, vol. 6, (**2014**), pp. 19-23.
[5] W. Wu, X. Meng, Z. Ma and X. Liang, "Three side dynamic game network can choose the survivability strategy", Journal of Applied Science, vol. 4, (**2014**), pp. 365-371.
[6] X. Wang, H. Yanyan and J. Wang, "Analysis of computer network defense strategy", The command information systems and technology, vol. 5, (**2014**), pp. 13-19.
[7] W. Wang, Y. Xie and Y. Li, "Research on organizational error information dynamic game model of incomplete information transfer mechanism", Based on information theory and practice, vol. 11, (**2014**), pp. 76-80.
[8] S. Shen, "Research on some key problems security in wireless sensor networks based on game theory", Donghua University, (**2013).**
[9] W. Han, Y. Chai and X. Wang, "Study on the strategies of enterprise information security based on game theory", Computer Engineering, vol. 9, (**2013**), pp. 162-166.
[10] X. Dong and L. Wang, "Incomplete information dynamic game analysis on competition in the banking industry", Hunan social science, vol. 4, (**2012**), pp. 137-140.
[11] L. Yu and Z. Jiang, "Research on Crisis Management Based on dynamic game of incomplete information", Shanghai management science, vol. 5, (**2012**), pp. 87-90.
[12] Y. Lou, R. Song and Y. Ma, "Attack defense game model based on RBF neural network", The application of computer and software, vol. 1, (**2011**), pp. 99-101.
[13] W. Lin, H. Wang, J. Liu, R. Deng, A. Li, Q. Wu and Y. Jia, "Research on active defense technology in network security based on non-cooperative dynamic game theory", Journal of computer research and development, vol. 2, (**2011**), pp. 306-316.

Author

Man Li, She is an Associate Professor in Shandong Huayu University of Technology. She is in the research of computer application technology

Jinjing Ca, She is a Lecturer in Shandong Huayu University of Technology. She is in the research of computer application technology