Active Defense strategies selection for network mixed malicious action

CHEN Yong-qiang
Dept. of Information Security
Naval Univ. of Engineering
Wuhan, China
chenyongqiang919@163.com

WU Xiao-ping
Dept. of Information Security
Naval Univ. of Engineering
Wuhan, China
wxp8@sohu.com

FU Yu
Dept. of Information Security
Naval Univ. of Engineering
Wuhan, China
fuyu0219@163.com

***Abstract*—In order to deal with the problems that defense measures are not been take into accounted and the return of the unit cost in network security analysis, a active defense strategies selection method for network mixed malicious actions was proposed. Firstly, a network security mixed game model was presented combined with the actual situation that the utility of the players are not equal. Premise in the classification of the mixed confront scenes, the utility function was proposed with the return of the unit cost. Then, the network mixed defense strategy selection algorithm was given and the best strategy for defender was obtained by analyzing the Nash equilibrium of the game model. Finally, a representative example is given to illustrate the efficacy and feasibility of the method on malicious actions prediction and active defense strategy selection.**

Keywords- network security; game; active defense; strategies selection;

I. INTRODUCTION

With the development of the network, the concept of network security has been studied from passive defense to active defense for early prediction. The defense effect depends on the actions of the malicious behavior sponsors to be taken. In order to get the best defense effect with limited resources, it is important to select a reasonable defense strategy.

Mutual influence of the network strategies is a behavioral interactions, game theory can be used to analysis this problem. In [1], the author introduced game theory to heterogeneous complex military systems and describes how to use game theory to analyze network security event. In [2], the author gives a measure of analyze network security event based on game theory, the confrontation between the attacker and the defender was described as a double game problem. In [3]-[4], an active defense method of network security was proposed based on dynamic game theory. In [5], the author proposed the concept of stochastic petri net combined stochastic game with petri net. But the problem of revenue quantify has not considered in all the literatures above. In [6], the inherent harm of malicious behavior was described by criticality and lethality. In [7], the author firstly proposed a cost-sensitive model as the basis of response decision. In [8], a network game model was proposed and confrontation strategies were classified. The literatures above assume that the malicious sponsor can launch independent malicious behavior, but not consider security strategy under mixed malicious actions.

In response to these problems, a network defense strategy for mixed malicious actions was proposed in this paper. Firstly, modeling a network security mixed game model and classifying the game scene, then analyzing the utility function. By solving Non-zero-sum game, the optimal defense strategy is obtained and malicious action is predicted.

II. NETWORK SECURITY GAME MODEL

Network Security mixed Game Model (NSMG) is represented by a four-tuple, $NSMG=\{\{P_a,P_d\},\{A_a,A_d\},\{S_a,S_d\},\{U_a,U_d\}\}$ whose elements are defined below:

(P_a,P_d) is the set of players is assumed to be where P_a represents the malicious behavior sponsors and P_d represents the defenders. A_a is the set of mixed malicious actions. $A_a=\left(A_a^1,A_a^2,\cdots,A_a^m\right)$ where $A_a^k=\left(a_1,a_2,\cdots a_t\right)$ represents the mixed malicious action; a_i represents the independent malicious action; If $\left|A_a^k\right|=1$, the mixed malicious action change to independent malicious action. Similarly, $A_d=\left(A_d^1,A_d^2,\cdots,A_d^n\right)$, $A_d^k=\left(d_1,d_2,\cdots d_t\right)$. S_a is the set of mixed strategy over the action set A_a. $S_a=(s_1,s_2,\cdots,s_m)$ where $s_j=(p_j(A_a^1),p_j(A_a^2),\cdots,p_j(A_a^m))$ $\sum_j p_j\left(A_a^i\right)=1$, $p_j\left(A_a^t\right)$ is the probability of choose A_a^t. Similarly, to the defender, $s_d=(p_d(A_d^1),p_d(A_d^2),\cdots,p_d(A_d^n)),\sum_j p_d\left(A_d^j\right)=1.$

$\boldsymbol{U}_a=\left[u_{ij}^a\right]_{m\times n}$ is the utility matrix of malicious behavior sponsor where u_{ij}^a represents the reward of

malicious behavior sponsor when (A_a, A_d) was taken. Similarly, for the defender, $\boldsymbol{U}_d = \left[u_{ij}^d\right]_{m\times n}$.

III. QUANTIFY THE UTILITY

A. The utility of independent action

In order to quantify the utility of players better, gives the following definition:

Definition 1: Assert Value. The goal of network defense is to ensure the security of network and different network assets has different safety requirements. In this paper, $\overrightarrow{AV} = (r_1, r_2, r_3)$ is the value of network asset on security attribute (CIA) where (r_1, r_2, r_3) represents the value of network asset in confidentiality, integrity and availability respectively.

Definition 2: Malicious behavior type. Faced with different goals, malicious behavior sponsor has different attention of security attributes of network assert. In this paper, $\overrightarrow{W_i} = (w_{i1}, w_{i2}, w_{i3}), 0 \le w_{ij} \le 1, \sum_j w_{ij} = 1$ is the type of malicious action where (w_{i1}, w_{i2}, w_{i3}) represents the attention degree on security attributes respectively.

Definition 3: Defensive rate. It reflects the probability of defense action to prevent the malicious behavior successfully. $\lambda_{ij}, 0 \le \lambda_{ij} \le 1$ is the success probability that defense action d_j to malicious behavior a_i. If defending behavior is ineffective $\lambda_{ij} = 0$, if completely prevent malicious action $\lambda_{ij} = 1$ else $0 \le \lambda_{ij} \le 1$.

There are many different definitions of utility functions. In [8], the utility function is defined as the difference between the benefits and costs. In order to reflect the effect of unit cost, the utility function is defined as (benefit-cost)/ cost in this paper. Suppose the players take independent action (a_i, d_j), the corresponding expression for utility functions is:

$$u_{a_i}(a_i, d_j) = \frac{RG_i \times (1-\lambda_{ij}) - Cost_{a_i}}{Cost_{a_i}} \quad (1)$$

$$RG_i = \overrightarrow{AV_i} \times \overrightarrow{W_i}^{\mathrm{T}} \times AS_i \quad (2)$$

$$Cost_{a_i} = ZC_{a_i} + PN_{a_i} \quad (3)$$

RG is the reward of malicious action; AV_i is the value of the target assert of malicious action a_i; AS_i is the success rate of malicious action a_i; $Cost_{a_i}$ is the cost of independent malicious action a_i which contains resource cost (ZC_{a_i}) and penalty cost (PN_{a_i}) when malicious action was found.

$$u_{d_j}(a_i, d_j) = \frac{RG_i - \left(RG_i \times (1-\lambda_{ij})\right) - Cost_{d_j}}{Cost_{d_j}} \quad (4)$$

$$Cost_{d_j} = PC_{d_j} + NI_{d_j} \quad (5)$$

$Cost_{d_j}$ is the cost of independent defense action d_j which mainly refers to the consumption of resources to perform preventive measures (PC) and the negative influence to the system (NI) ; There are no relationship between negative influence and malicious action, negative influence is only with defense action.

B. The utility of mixed action

Assuming that all the independent actions are independent of each other, the game can be divided into three scenes:

- Scene 1: The scene of independent malicious action a_i and mixed defense action $A_d^k = (d_1, d_2, \cdots d_t)$. The corresponding defensive rate of mixed defense action is $\theta_k = 1 - \prod_j (1-\lambda_{ij})$, the corresponding cost of hybrid defense action is $C_d^k = \sum_j Cost_{d_j}$. The corresponding expression for utility function of player is:

$$u_{a_i}(a_i, A_d^l) = \frac{RG_i \times (1-\theta_k) - Cost_{a_i}}{Cost_{a_i}} \quad (6)$$

$$u_{A_d^l}(a_i, A_d^l) = \frac{RG_i - \left(RG_i \times (1-\theta_k)\right) - C_d^k}{C_d^k} \quad (7)$$

- Scene 2: The scene of mixed malicious action $A_a^k = (a_1, a_2, \cdots a_t)$ and independent defense action d_j. Because of the independence of the malicious action, the game can be divided to several games which two players take independent malicious action a_i and independent defense action d_j respectively. The corresponding expression for utility function is:

$$u_{A_a^k}(A_a^k, d_j) = \sum_{i=1}^{t} u_{a_i}(a_i, d_j) \quad (8)$$

$$u_{d_j}(A_a^k, d_j) = \frac{\sum_i \left(RG_i - \left(RG_i \times (1-\lambda_{ij})\right)\right) - Cost_{d_j}}{Cost_{d_j}} \quad (9)$$

- Scene 3: The scene of mixed malicious action $A_a^k = (a_1, a_2, \cdots a_t)$ and mixed defense action $A_d^l = (d_1, d_2, \cdots d_s)$. It can be understood as the combination of scene 1. The reward of mixed malicious action is the sum of all the reward of independent malicious action a_i to mixed defense action $A_d^l = (d_1, d_2, \cdots d_t)$. The corresponding expression for utility function is:

$$u_{A_a^k}(A_a^k, A_d^l) = \sum_{i=1}^{t} u_{a_i}(a_i, A_d^l) \tag{10}$$

$$u_{A_a^l}(A_a^k, A_d^l) = \sum_{j=1}^{s} u_{d_j}(a_i, A_d^l) \tag{11}$$

Through collecting the information of cost and resource about the players, it can analyze whether the player have enough resource to take some actions, so as to simplify the state space, which is more consistent with the actual situation. Assume that the largest resources players have are S_a, S_d respectively, the cost to take mixed action for both players of the game required to meet formula (9):

$$\begin{aligned} \sum_i Cost_{a_i} &\le S_a \\ \sum_j Cost_{d_j} &\le S_d \end{aligned} \tag{12}$$

Assume that the players of the game take mixed strategy $s_a = (p_a(A_a^1), p_a(A_a^2), \cdots, p_a(A_a^m))$ and $s_d = (p_d(A_d^1), p_a(A_d^2), \cdots, p_a(A_a^n))$ respectively, the corresponding expression for mixed utility function is:

$$\begin{aligned} U_a(s_a, s_d) &= \sum_{i=1}^{m} p_a(A_a^i) \sum_{j=1}^{n} p_d(A_d^j) u_a(A_a^i, A_d^j) \\ U_d(s_a, s_d) &= \sum_{j=1}^{n} p_d(A_d^j) \sum_{i=1}^{m} p_a(A_a^i) u_d(A_a^i, A_d^j) \end{aligned} \tag{13}$$

The cost of both players can be measured by investment of technology, money and time et al, and the reward can be measured from material and psychological. In this paper, cost and reward of players are abstracted as money.

C. Nash Equilibrium

If players of the game take mixed strategy (s_a^*, s_d^*), (s_a^*, s_d^*) is Nash Equilibrium if and only if it satisfies formula (14):

$$\begin{aligned} u_a(s_a^*, s_d^*) &\ge u_a(s_a, s_d^*) \ \ \forall s_a \in S_a \\ u_d(s_a^*, s_d^*) &\ge u_d(s_a^*, s_d) \ \ \forall s_d \in S_d \end{aligned} \tag{14}$$

In [9], the author has proved that any game of finite strategy has one mixed strategy Nash Equilibrium at least. Because of the numbers of actions in $NSMG$ are limited, correspondingly the strategy game is limited. So the $NSMG$ has one mixed strategy Nash Equilibrium at least. When reach the Nash Equilibrium, it can't get more profits from change strategy unilaterally.

IV. Mixed Strategy Game Solution

It has been proved that $NSMG$ has a non-empty set of optimal strategy for each player. Combining reward quantization method, we obtain the optimal defense strategy selection algorithm:

Input: Network Security Game Model $NSMG$

Output: active defense strategy s_a^*, s_d^*

step1. Initialize $NSMG$

step2. Modeling A_a, A_d with independent action of both players

step3. compute the independent utility function $u_{a_i}(a_i, d_j), u_{d_j}(a_i, d_j)$ by (1)-(5)

step4. compute the mixed utility function $u_{a_i}(a_i, d_j), u_{d_j}(a_i, d_j)$ by (6)-(11) and payoff matrix $\boldsymbol{U}_a, \boldsymbol{U}_d$.

step5. The optimal mixed strategy can be obtained by solving the following linear program:

$$\max f(S_a, S_d, \boldsymbol{U}_a, \boldsymbol{U}_d) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_a(A_a^i) p_d(A_d^j) u_a(A_a^i, A_d^j)$$

$$+\sum_{j=1}^{n}\sum_{i=1}^{m} p_d(A_d^j) p_a(A_a^i) u_d(A_a^i, A_d^j) - v_1 - v_2$$

$$\begin{cases} \sum_{j=1}^{n} u_a(s_a^i, s_d^j) p_d^j \le v_1 \quad i = 1, 2, \cdots, m \\ \sum_{i=1}^{m} u_d(s_a^i, s_d^j) p_a^i \le v_2 \quad j = 1, 2, \cdots, n \\ \sum_i Cost_{a_i} \le C_a, \sum_j Cost_{d_j} \le C_d \\ \sum_{i=1}^{m} p_a^i = 1, \sum_{j=1}^{n} p_d^j = 1 \end{cases}$$

Step6. Analysis of the Nash Equilibrium and predict the malicious action which is most likely happen, then determine the active defense strategy.

V. Case Study

Use the following network to illustrate $NSMG$. The topology of the network is show in Fig. 1. The goal of malicious behavior sponsors is to intrude the database server. The database server has opened the service of e-mail and FTP. The rule of firewall is that the host in LAN1 only with root privilege to Ftp service and the host in LAN2 only with

root privilege to e-mail service. The malicious behavior sponsors scan the target network to find vulnerabilities in Database server (CVE-2004-0159\CVE-2004-0148) and hosts (CVE-2002-0836\CVE-2002-0838 in host1; CVE-2002-0083 in host2). Then the malicious behavior sponsors can use the vulnerabilities to get root privilege and intrude the database server further more. The information of the actions of two players is shown in Table I and Table II. The information of opposite action is shown in Table III.

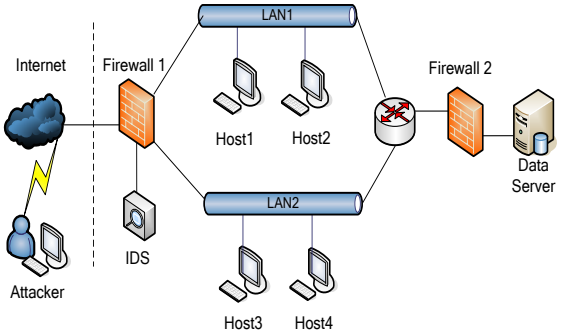

Figure 1. The topology of the network

TABLE I. INFORMATION OF MALICIOUS ACTION

Symbol	Act Action	AS	W	ZC	PN
a1	ApacheChunked-Enc	0.6	(0.3,0.5,0.2)	500	200
a2	Wu-FtpdSockPrintf()	0.8	(0.1,0.6,0.3)	600	200
a3	FTP Bounce	0.5	(0.6,0.2,0.2)	400	200

TABLE II. INFORMATION OF DEFENSE ACTION

Symbol	Defense Action	PC	NI
d1	Patch Ftp. rhost on Smtp Sever	600	200
d2	Close rsh on Smtp Sever	500	200
d3	Close rsh on Ftp Sever	300	300
d4	restart ftpd	400	100

TABLE III. INFORMATION OF OPPOSITE ACTION

Act Action	Defense Action	λ
a1	d1	0.6
	d2	0.4
a2	d2	0.2
	d3	0.7
	d4	0.6
a3	d1	0.3
	d3	0.9
	d4	0.5

In order to simplify the analysis, assume that the assert value of all the hosts is (3000，4000，2000), resource of players are 2000. In the condition of infinite resource, $A_a = (a_1, a_2, a_3, a_4, (a_1, a_2), (a_1, a_3), (a_2, a_3), (a_1, a_2, a_3))$ Co nsidering the constraints of resource to players, some mixed action can't be taken, $A_a = (a_1, a_2, a_3, a_4, (a_1, a_2), (a_1, a_3), (a_2, a_3))$ .Similarly, $A_d = (d_1, d_2, d_3, d_4, d_5, (d_1, d_2), (d_1, d_3), (d_1, d_4), (d_2, d_3), (d_2, d_4), (d_3, d_4), (d_2, d_3, d_4))$. The utility matrixs of two players are shown in Fig. 2 and Fig. 3:

u_a	a_1	a_2	a_3	(a_1,a_2)	(a_1,a_3)	(a_2,a_3)
d_1	0.13	2.3	0.75	2.26	0.88	3.05
d_2	0.69	1.64	1.5	2.33	2.19	3.14
d_3	1.83	–0.01	–0.75	1.82	1.08	–0.76
d_4	1.83	0.32	0.25	2.15	2.08	0.57
(d_1,d_2)	–0.32	1.64	0.75	1.32	0.43	2.39
(d_1,d_3)	0.13	–0.01	–0.83	0.12	–0.7	–0.84
(d_1,d_4)	0.13	0.32	–0.13	0.45	0	0.19
(d_2,d_3)	0.68	–0.21	–0.75	0.47	–0.07	–0.96
(d_2,d_4)	0.68	0.06	0.25	0.74	0.93	0.31
(d_3,d_4)	1.82	–0.6	–0.86	1.76	0.96	–1.46
(d_2,d_3,d_4)	0.68	–0.68	–0.86	0	–0.18	–1.54

Figure 2. The utility matrix of malicious behavior sponsors

u_d	a_1	a_2	a_3	(a_1,a_2)	(a_1,a_3)	(a_2,a_3)
d_1	0.48	–1	–0.44	0.49	1.05	–0.44
d_2	0.13	–0.25	–1	0.89	0.13	–0.25
d_3	–1	2.08	1.25	2.08	1.25	4.33
d_4	–1	2.17	0.5	2.17	0.5	3.67
(d_1,d_2)	0.003	–0.65	–0.7	1.38	1.18	–0.69
(d_1,d_3)	–0.15	0.32	–0.004	2.57	2.25	3.89
(d_1,d_4)	–0.09	0.22	–0.25	2.66	1.55	3.23
(d_2,d_3)	–0.39	0.54	0.04	2.97	1.38	4.08
(d_2,d_4)	–0.34	0.45	–0.38	3.06	0.63	3.42
(d_3,d_4)	–1	1.11	0.30	4.25	1.75	8
(d_2,d_3,d_4)	–0.56	0.33	–0.21	–0.23	1.88	7.75

Figure 3. The utility matrix of defender

If both players take independent action against each other, $s_a = (0.538, 0, 462, 0), s_d = (0.682, 0, 0, 0.312)$. We can see that the most likely action is a_1. If both players take mixed action against each other, $s_a = (0, 0.238, 0, 0.762, 0, 0), s_d = (0, 0, 0, 0.186, 0, 0, 0, 0, 0.814, 0, 0)$. It reflects that malicious behavior sponsor selected mixed action in order to improve the reward of unit cost.

VI. CONCLUSION

In this paper, the network security is abstracted as non-cooperate game model combined with the actual situation of network. In the view of network security attribute, describe utility function with the ratio of reward and cost. The optimal defense strategy selection algorithm is given. The result of the experiment shows that *NSMG* is efficacy in

malicious action prediction and active defense strategy selection.

ACKNOWLEDGMENT

The author would particularly like to thank National Science Foundation for the support for this study. This work was funded by the National Science Foundation. The author would also like to thank Wang Jia-sheng for many useful comments and suggestions.

REFERENCES

[1] Browne R, "C4I defensive infrastructure for survivability against multi-mode attack," Proceedings of the 21st Century Military Communication- Architectures and Technologies for Information Superiority. Los Angeles,CA, 2000, vol. 1, pp: 417-424.

[2] Lye K., Wing J. M, "Game Strategies in network security," Proceedings of the IEEE Computer Security Foundations Workshop, Copenhangen: 2002: 71-86.

[3] LIN Wangqun, Wang Hui, LIU jiahong, Deng Lei, Li Aiping, Wu Quanyuan, et al, "Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory," Journal of Computer Research and Development, vol. 48, pp. 306-316, February 2011.

[4] ZHANG Shaojun, LI Jianhua, CHEN Xiuzhen, Hu Wei, "Method Research for Defending Against Distributed Denial of Service Attacks Based on Dynamic Game Theory," JOURNAL OF SHANGHAI JIAOTONG UNIVERSITY, vol. 42, pp. 198-201, February 2008.

[5] Wang Yuanzhuo, Lin Chuang, Cheng Xueqi, Fang Binxing, "Analysis for Network Attack-Defense Based on Stochastic Game Model," Chinese Journal of Computers. Vol. 33, pp. 1748-1762, September 2010.

[6] Northcutt S, "Networking Intrusion Detection:An Analyst's Handbook," Indianapolis, Indiana, United States: New Riders Publishing, 1999.

[7] Lee Wenke, "Toward cost-sensitive modeling for intrusion detection and response," Journal of Computer Security, vol. 10, pp. 5-22, April 2002.

[8] Jiang Wei, Fang Binxing, Tian Zhihong, Zhang Hongli, "Evaluating network security and optimal active defense based on attack-defense game model," Chinese Journal of Computers, vol. 32, pp. 817-827, April 2009.

[9] M J. Osborne, A Rubinstein, R Aumann, "A Course in Game Theory,2nd ed," The MIT Press, 1994.