Defensive Strategy Selection based on Attack-Defense Game Model in Network Security

Ningbin Zhang*

School of Information Engineering of Xi'an University, Xi'an, 710062, China

Abstract

Security analysis and attack-defense modeling are effective methods to identify the vulnerabilities of information systems for proactive defense. The attack graph model reflects only attack actions and system state changes, without considering the perspective of the defenders. To assess the network information system and comprehensively show attack and defense strategies and their cost, a defense graph model is proposed. Compared with the attack graph, the model makes some improvements. The defense graph will be mapped to the attack and defense game model, in order to provide a basis for active defense policy decision. Moreover, a generation algorithm of defense graph is proposed. A representative example is provided to illustrate our models and demonstrate the high efficiency of the algorithm.

Keywords: network security; active defense; attack-defense game model

(Submitted on August 2, 2018; Revised on September 15, 2018; Accepted on October 11, 2018)

© 2018 Totem Publisher, Inc. All rights reserved.

1. Introduction

Existing computer network information systems are deployed on multiple platforms [1], run numerous application software, and support plentiful linkage patterns. Inevitably, there will be some security vulnerabilities and faults. Network attacks tend to be diversified and integrated [2-3]. Due to limitations on resources and capabilities, network administrators cannot eliminate drawbacks nor defend all attacks. Network information security defenders constantly face a dilemma between information security investment and optimal defense [4]. Achieving balance between information security risk and investment is a problem that must consider defense cost effectiveness, making the most appropriate decisions with limited resources to reach "moderate security". This is a matter of selecting the optimal network security defense measures. The existing security model lacks description of the dynamic gaming between attack and defense, and it cannot accurately reflect the dynamic interaction and status evolution between the attacker and defender in the system [5-6].

Here, we talk about the complication of selecting the best defense strategies for network security. We formally define the problem of choosing the best defensive strategies for network security, which are described with mathematical functions [7-8]. Then, the construction and solving method of the selection function are provided. The Markov decision process has been successfully applied to search the optimal strategy by single intelligent agent under multiple states. Because of that, we can combine the matrix type offensive and defensive game model and Markov decision process to get a random attack-defense game model that can be used to search dynamically the optimal attack-defense strategy by such a few rational intelligent agents under many offensive and defensive states. Random gaming [9-10] can be regarded as a state machine making game system shift from one status to the other with combined efforts of all players. Likewise, the network system can be regarded as a state machine, which makes the system change its status with co-action of offensive and defensive on target conflicts. The objective of the attacker is to destroy the security attribute of the network system. The defender prevents the attacker from impairing secure attributes. System state changes are not certain and involve moving from one state to another in a probability manner. Hence, it is reasonable to depict the network offence and defense conflict problem with the random game model. In the static offense and defense game model, two sides search the best offensive and

* Corresponding author.
E-mail address: ningbinzhangnbz@sina.com
defensive strategy with the static model in single state circumstances, with no consideration of the dynamic state evolution or transition of offense and defense status. In this case, we propose the random offensive and defensive game model, which portrays the dynamic variations of network security offense and defense conflict and can solve the problem of selecting the best prevention strategy. The network attack and defense sides are modeled as a two-person non-cooperative attack and defense random game model [11]. It describes the formalized definition and constituting elements of the model. The attacker’s privilege state on network entity components is used as an element of the offense and defense random game model, the dynamic changes of the network attack and defense states are modeled, attack behaviors are predicted, and the best defense strategy is finally determined. The best defense strategy selection algorithm based on the random offense and defense game model is presented. Through discussion of network instances, we demonstrate that the model and algorithm both work effectively on attack strategy prediction and optimal active defense.

2. Formalized Description of the Optimal Defense Strategy Selection

In network security management, the defender is perplexed by the defense strategy selection problem. What is the optimal defense strategy? A defensive strategy can reduce attack risk and loss, but, meanwhile, the defense cost is increased. How can one weigh them and achieve the optimal defense strategy? The selection of strategy not only considers the cost but also the network asset criticality and the potential attacks. For a single attack, the defense decision needs choose a strategy that realizes the minimum defense cost; for multi-step and multiple attacks, some defending strategy is workable for one attack action but not for others. On that regard, we need consider the effectiveness of the defense strategy for specific attacks, the operation cost, and negative influences. Besides, the happening probability of every attack strategy is unknown. How to guarantee that defensive tactics are optimal and the expected integrated defending cost is the lowest is a complicated issue.

Based on the above analysis, we can define the optimal defense strategy selection problem as one function: $f_{selection} = (C, A, D, G) \rightarrow D'$, where each element is defined as follows:

$C$: entity component collection of the protected network information system; entity component $c \in C$ can be host, router, firewall; each entity component is composed of part or more of software, hardware, data, and service, e.g. web server that runs HTTP service.

$A$: information aggregation of possible attack, happening attack and on the way. For network entity component $c \in C$, $c$ has vulnerability that may be utilized by attacker; it is required to recognize possible attacks, occurrent attacks, and incoming attacks $a \in A$ in order to protect $C$.

$D$: collection of defending strategies taken by the defensive system, e.g. attacks against Ftp Buffer overflow vulnerability; defending strategy $d = (close Ftp service)$, $d \in D$.

$G$: collection of offensive and defensive game models, such as the matrix type offensive and defensive game model and the random attack and defense game model ADSG (introduced in next part); choose different game models according to specific network offensive and defensive situation.

$D'$: collection of optimal defending tactics taken by the defense system, $D' \subseteq D$.

$f_{selection}$ maps from the network security situation $(C, A, D, G)$ to the optimal defense strategy $D'$. For any $i, j$, if $(C_i, A_i, D_i, G_i) \rightarrow D'_i$, $(C_j, A_j, D_j, G_j) \rightarrow D'_j$ and $(C_i, A_i, D_i, G_i) = (C_j, A_j, D_j, G_j)$, then $D'_i = D'_j$. Given network information system entity component collection $C$, determine attack information aggregation $A$ through vulnerability analysis and the invasion detection mechanism; analyze $A$ and $C$ and determine the defending strategy collection $D$; choose a suitable attack and defense game model $G$ as per network attack-defense and requirements; finally, with relative information about $A$, $C$, and $D$, construct the offense and defense game model $G$.

3. Offense and Defense Random Game Model

In this part, we introduce the matrix type offensive and defensive game model and Markov decision-making process. The Markov decision process has been successfully used to search the optimal strategy by a single intelligent agent under multiple states. By combining the matrix type offense and defense game model and Markov decision-making process, we can use the random offense and defense game model dynamically to find the best attack-defense strategy by many rational attack-defense intelligent agents in multiple offense and defense states.
3.1. Matrix Type Attack-Defense Game

The matrix type Attack-Defense Game (ADG) is a three tuple ADG = (N, S, U), where:

1) \( N = (P_1, P_2, \ldots, P_n) \) is a set of players in the game of attack-defense. Participants are the main body of decision making and policy makers.

2) \( S = (S_1, S_2, \ldots, S_n) \) is a set of strategies for the attack-defense. \( \forall i \in n, S_i \neq \emptyset \). \( S_i = (S'_1, S'_2, \ldots, S'_m) \) is the strategy set of offense and defense \( P_i \).

3) \( U = (U_1, U_2, \ldots, U_n) \) is a collection of the revenue function of the attack-defense. \( \forall i \in n, U_i \) is the function of the offensive and defensive \( P_i \).

3.2. Markov Decision-Making Process

The Markov decision-making process is a dynamically optimized method built in the Markov process. It has the basic thinking: transfer the state change of the system to a Markov process to deal with; for every state in the Markov process, the decision-maker can take different actions according to various states and decision actions; the decision-maker can gain certain revenue, which can be negative, meaning it suffers a loss. The Markov decision process aims to find a strategy through which a proper decision action is taken in different states to make the ultimate benefit maximized or minimized. The Markov decision process (MDP) [12] is a tetrad \((S, A, T, R)\): \( S \) \( \times \) \( A \) \( \times \) \( S \) \( \rightarrow \) \([0,1]\) is a state transition function; \( A \) is system behavior collection; \( T\) is the state transition probability function of the attack-defense random game state set. \( R: S \times A \rightarrow R \) is a revenue function. Mark \( R(s, a, s') \) as the profit value gained by system shifting states to \( s' \) with the use of action \( a \), and mark \( T(s,a,s') \) as the probability of the system moving states to \( s' \) with the use of action \( a \).

3.3. Attack-Defense Random Game Model

We extend the single state of matrix type attack-defense to multiple states and the single intelligent agent in the Markov decision-making process to many. By combining the two, we establish an attack-defense random game model, defined as follows:

**Definition** The attack-defense random game model (ADRG) is a seven tuple:

\[ ADRG = (N, S, A, D, P, U_1, U_n) \]

where \( N = \{ \text{Attacker, Defender} \} \) is collection of players joining the offense and defense game. If the number of attacker is \( \geq 2 \), it means distributed collaborative attack; if the number of defending system is \( \geq 2 \), it means collaborative protection by several defending systems. Here, we study the situation were \( n = 2 \) and there is one attacker and one defender. Merge a couple of attackers and defenders, and they can be seen as a single attacker and defender.

\[ S = (S_1, S_2, \ldots, S_n) \] is an attack-defense random game state set.

\[ A = (a_1, a_2, \ldots, a_m) \] is an attacker action set. An attacker in the game state \( S_i \) attacks action set \( A_i \subset A \).

\[ D = (d_1, d_2, \ldots, d_n) \] is a set of defensive actions. The defender in the game state \( S_i \) protects action set \( D_i \subset D \).

\[ P: S \times A \times D \times S \rightarrow [0,1] \] is the state transition probability function of the attack-defense random game.

\[ U_k : S \times A \times D \times S \rightarrow R, k = a, d \] is a set of utility function.

The benefit relationship between the attacker and defender includes zero sum and non-zero sum. Choose the zero sum or non-zero sum game model based on different network environments and attack-defense situations. Over the course of the network attack-defense game, the relationship between the attacker and defender decides that either party will not notify the other of any strategy decision or they reach agreement. The relationship is always non-cooperative and antagonistic.
Therefore, the above model is a non-cooperative attack-defense. The Markov decision-making process is a single intelligent agent’s multi-state model. The game model is a single-state model of multiple intelligent agents. The matrix attack defense game model is a single state model of a multi-agent system. The random attack and defense game model can be seen as the integration and expansion of the two models; it is a multi-agent and multi-state model. The relationship between the three is shown in Figure 1.

![Figure 1. Relations of the ADG, MDP, and ADSG](image)

### 3.4. Attack-Defense Random Game State

We look at the network security state as attack-defense. The network security state describes the network entity components’ hardware and software resource attributes, connectivity, and the user’s or attacker’s ability to access the whole network. Security state changes are caused by attack-defense. The random game state can be represented by a directed graph \( G = (S, E) \), where \( S \) is the graph’s point set, each point represents a game state, and \( E \) is collection of edges, meaning the transition relation of attack-defense. Figure 1 illustrates the game state and the transition relation by citing examples of state graphs that contain three game states \( S = (S_1, S_2, S_3) \). In Figure 2, the state can mutually transit, but in some specific network environments, not all states can mutually transit. In it, \( p_{ij}(a_i, d_j) \) marking between different states means the transitional possibility of the game state changing from state \( i \) to state \( j \) under the action of the attack-defense strategy pair \( (a_i, d_j) \).

![Figure 2. Example of ADRG's state](image)

### 4. Defense Strategy Selection Algorithm based on Attack-Defense Random Game Model

Given \( (C, A, D, G) \), where \( G = ADRG = (N, S, A, D, P, U_a, U_d) \). Because there are many states in the game of attack-defense, the Shapley iterative method can be used to solve the value \( v = (v_1, v_2, \ldots, v_n) \) of offensive and defensive random game and its optimal attack-defense strategy. The defense strategy selection algorithm based on the attack-defense random game model is shown in Algorithm 1.
Algorithm 1 Defense strategy selection algorithm based on attack-defense random game model

Input: \((C, A, D, G, \delta)\)

Output: Optimal attack-defense strategy \(\pi^*, \pi'^* = D'\)

1. By \(C, A, D\) to build a random game of attack-defense \(G = ADG\)
2. Arbitrary initial vector \(v^i = (v^i(1), v^i(2), \ldots, v^i(K))\)
3. Repeat
   4. For every game state \(S \in S_i\) do
      5. For all \(s'_i\) do
         6. With \(v_i\) instead of \(s_i\)
         7. End for
      8. Calculation \(v_i^{\pi*} = Val(a_i^v + \sum_{l=1}^{K} p_i^v(a_i, d_i) v'_i)\)
      9. End for
   10. For every game state \(S \in S_i\) do
      11. \(v_i \leftarrow Val(S_i)\)
      12. End for
   13. Until \(|v_i^{\pi*} - v_i| < \delta, \forall S \in S_i\)
   14. For every game state \(S \in S_i\) do
   15. \((\pi^*_i, \pi'^*_i) = Solv(S_i)\)
   16. End for
   17. Return \(\pi^* = (\pi^*_1), \pi'^* = (\pi'^*_1)\)

5. Experimental Analysis and Results

5.1. Network Topology Structure

Assuming that there is a typical network topology, the attack host is located in the external network, as shown in Figure 3. The protected network information system entity component set is represented by \(C = \{\text{Attacker Host, Smtp Server, Ftp Server, Data Server}\}\).

![Figure 3. Topology of example network]

The firewall separates the target network from the external network. The firewall rules and the connection information are shown in Table 1. The target system vulnerability information is shown in Table 2.

Table 1. Connectivity in example network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Smtp Server</td>
<td>Ftp, Smtp</td>
<td>Allow</td>
</tr>
<tr>
<td>All</td>
<td>Ftp Server</td>
<td>Ftp, Ssh</td>
<td>Allow</td>
</tr>
<tr>
<td>Smtp Server</td>
<td>Database</td>
<td>Oracle</td>
<td>Allow</td>
</tr>
<tr>
<td>Ftp Server</td>
<td>Data Server</td>
<td>Oracle</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Table 2. Vulnerability in servers

<table>
<thead>
<tr>
<th>Host</th>
<th>Vulnerability</th>
<th>CVE ID</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smtp server</td>
<td>Ftp .rhost</td>
<td>2011-0547</td>
<td>User privilege</td>
</tr>
<tr>
<td>Ftp server</td>
<td>Ftp .rhost</td>
<td>2011-0547</td>
<td>User privilege</td>
</tr>
<tr>
<td>Data server</td>
<td>Oracle TNS Listener</td>
<td>2012-0965</td>
<td>User privilege</td>
</tr>
</tbody>
</table>
5.2. Description of Attack-Defense Random Game State

The attacker’s offense and control of the network are manifested in the control of network entity components, i.e. the acquisition of privilege by the attacker for entity components. We express the network security state as the ability of the attacker to access each network entity component, i.e. privilege. Attack actions lead to changes in the network security state, i.e. the state change of the attacker’s privilege for each component. Generally, we can define the attacker’s privilege state collection per actual network system environment. Here, the attacker’s privilege state includes: no privilege, remote access privilege, local user privilege, and root privilege, which from low to high is no privilege < remote access privilege < local user privilege < root privilege.

Assume the attacker has root privilege to invade the host and launch an attack but cannot simultaneously implement multiple attack actions, and acquiring root privilege of the data server is the goal. According to firewall rules, in the Smtp Server and Ftp Server, the attacker has the lowest remote access privilege and is unable to access the data server. However, vulnerability exists in various components, and the attacker can utilize associated weaknesses to make multi-step attacks and elevate privilege to get root privilege of the data server, as described hereunder: in state $S_1$, the attacker uses them as a springboard to employ Oracle TNS Listener’s weak point to get the data server’s root privilege and reach state $S_5$. Besides, the attacker can use Ftp Server’s weakness Sshd Buffer overflow to make attacks and get privilege of the Ftp Server to reach state $S_4$; then, with the connection to the data server, the attacker utilizes Oracle TNS Listener’s loophole to get root privilege of the data server to reach state $S_5$. The directed graph $G = (S, E)$ is shown for the attack-defense random game model in Figure 4. The game state is represented by $S = (S_1, S_2, S_3, S_4, S_5)$, and each state is described as shown in Table 3.

![Figure 4. Attack-defense random game state graph](image)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>Root privilege on Attacker Host</td>
</tr>
<tr>
<td>$S_2$</td>
<td>User privilege on Ftp Server</td>
</tr>
<tr>
<td>$S_3$</td>
<td>User privilege on Smtp Server</td>
</tr>
<tr>
<td>$S_4$</td>
<td>User privilege on Ftp Server</td>
</tr>
<tr>
<td>$S_5$</td>
<td>Root privilege on Data Server</td>
</tr>
</tbody>
</table>

5.3. Attack and Defense Random Game State Transition

In the state directed graph $G = (S, E)$, the edge set $E$ is used to describe the relationship between the state of attack and defense and stochastic game.

Here, the state transition probability $p_{ij}(a_m)$ is expressed as the attacker’s $a_m$ success rate of attacking. The value is
related to the attack complexity, network environment, and other factors, according to the expert knowledge and historical attack data combined with the above assumptions. Table 4 gives specific values.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Category</th>
<th>Success probability</th>
<th>AL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_1$</td>
<td>Ftp .rhost attack on Ftp Sever</td>
<td>User</td>
<td>0.8</td>
<td>7</td>
</tr>
<tr>
<td>$a_2$</td>
<td>Ftp .rhost attack on Smtp Server</td>
<td>User</td>
<td>0.8</td>
<td>8</td>
</tr>
<tr>
<td>$a_3$</td>
<td>Sshd Buffer overflow</td>
<td>User</td>
<td>0.7</td>
<td>5</td>
</tr>
<tr>
<td>$a_4$</td>
<td>Oracle TNS Listener</td>
<td>Root</td>
<td>0.7</td>
<td>10</td>
</tr>
<tr>
<td>$a_5$</td>
<td>No action</td>
<td>Other</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### 5.4. Attack Action Set

Analysis of the attacker’s weaknesses is used to obtain the various states of the attacker action set $A_1 = \{a_1, a_2, a_3, a_4, a_5\}$, $A_2 = \{a_1, a_3\}$, $A_3 = \{a_1\}$, $A_4 = \{a_4, a_5\}$, $A_5 = \emptyset$.

The attack action set is represented by $A = \bigcup_{i=1}^{5} A_i = \{a_1, a_2, a_3, a_4, a_5\}$. The specific description of the attacker’s action is shown in Table 4. At the same time, the attack type, attack success probability, and fatal degree are given. Analyze server vulnerabilities and possible attacks and their associations, and then select defense action sets available for each state from the defense policy library.

$$D_1 = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8\}, \quad D_2 = \{d_2, d_4, d_6\}, \quad D_3 = \{d_2, d_4, d_6\}, \quad D_4 = \{d_2, d_4, d_6\}, \quad D_5 = \emptyset$$

The defensive action set is represented by $D = \bigcup_{i=1}^{5} D_i = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8\}$. Specific defense actions and their operating costs and negative price information are shown in Table 5.

### 5.5. Offensive and Defensive Cost Benefit Calculation

The attack and defense action set is determined, and then the gains and losses are calculated. The zero and non-cooperative attack and defense game model is used to calculate the attack proceeds. Taking into account the actual significance of offensive and defensive gains, attack gains are positive. Because the attack is against a server, it may be harmful to the confidentiality, integrity, and availability of the server. According to the actual circumstances of the network environment, the Ftp Server and Smtp Server security attribute costs 20 and the data server security attribute costs 30. Here, we do not consider the attacker’s attack cost AR or the defense residual cost Rcost. Ocost can query the defense action library, and the specific values are shown in Table 5.

If Ncost is very small, it can be ignored and set to 0. Otherwise, the negative effect of the defensive action can be
equivalent to a DOS attack on the server, which cannot provide normal service. Thus, \( N_{\text{cost}} \) converts to DOS attack, resulting in a system loss to the server. In order to simplify the analysis, specify when a defensive action \( d \) attacks a \( e(a,d) = 1 \). Otherwise, \( e(a,d) = 0 \).

5.6. Optimal Defense Strategy Selection

With Algorithm 1, we can determine the state value of each attack-defense random game and the best attack-defense strategy. The value of each matrix type game model \( S_i \) is calculated by the Gambit method. Finally, the optimal attack-defense strategy is

\[
\pi^* = (\pi_1^*, \pi_2^*, \pi_3^*, \pi_4^*), \quad \pi^{**} = (\pi_1^{**}, \pi_2^{**}, \pi_3^{**}, \pi_4^{**}).
\]

In game state \( S_1 \), attacker takes the best offensive strategy: choose attack action \( a_1 \) in the probability 0.3, choose attack action \( a_2 \) in the probability 0.27, and choose action \( a_3 \) in the probability 0.43. In this state from the perspective of the attacker, attack action \( a_1, a_2, a_3 \) works basically the same to the whole attack process, and there is no significant difference between cost and gain. Therefore, the attacker selects it in the probability of 0.3, which is highly possible to take action \( a_1 \). For the defender, the best defending tactics are: choose defensive action \( d_1 \) in the probability 0.39, \( d_4 \) in 0.47, and \( d_6 \) in 0.14. In the game state \( S_2, S_3, S_4 \), both use the pure strategy, which conforms to the actual attack-defense situation. For the attacker, in game state \( S_2, S_3, S_4 \), there are only two options: attack or non-attack. Only when the attack action is taken can the attacker achieve its purpose. Therefore, the attacker makes an attack in the probability of 1. For the defender, also in the state mentioned above, \( d_6 \) can yield the biggest revenue; therefore, the defender selects it in the probability of 1. The expected return value of each game state is shown in Table 6.

<table>
<thead>
<tr>
<th>Game state</th>
<th>( S_1 )</th>
<th>( S_2 )</th>
<th>( S_3 )</th>
<th>( S_4 )</th>
<th>( S_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payoff of Attacker</td>
<td>364.5</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>40</td>
</tr>
<tr>
<td>Payoff of Defender</td>
<td>-364.5</td>
<td>-64</td>
<td>-64</td>
<td>-64</td>
<td>-40</td>
</tr>
</tbody>
</table>

Figure 5, Figure 6 and Figure 7 describe the attack and defense strategy of the two sides in the game state \( S_1 \) probability change process. Gradually convergence tends to stable strategy to achieve the offensive and defensive Nash equilibrium.

According to significances of Nash equilibrium in game theory, only the defender sticks to its own Nash equilibrium strategy. The system may be impaired to the minimum extent during the attack.

The Nash strategy is obtained through the analysis method of attack-defense. The random game model provides solutions to defenders for active defense by selecting the optimal defending tactics. In actual applications, security preventive measures can be taken based on the network environment, security requirements, and investment for security. If security prevention investment resources are limited, the Nash equilibrium strategy is an option. Moreover, properly increase defending investments to prevent all attack strategies and reinforce network information system security.

This paper presents a model of network survivability strategy selection based on fuzzy matrix game and analyzes and verifies it. Xiao used the game theory to analyze the Nash equilibrium and the optimal strategy of both the defender and the attacker. The method is simple, and the cost and income analysis are rough. Richard proposed a model based on game theory for intrusion intention, goal, and strategy. A description framework based on game theory is studied. The cost and benefit analysis of the method is simple, and it cannot accurately describe the behavior of both parties. Further validation is needed to evaluate the accuracy of intrusion intention and target and strategy reasoning.

Compared with the related work, the optimal defense strategy selection model and method based on the random game model have the following characteristics:

1) Combined with the matrix game model and Markov decision process, it is extended to many people as a multi-state dynamic attack defense model.

2) The attacker’s privilege status on the network entity component is used for the random game model. The dynamic
change of network attack and defense state is modeled, and the attack behavior and optimal defense strategy are predicted.

3) Not only is the cost effectiveness of the defense strategy considered, but also the attack strategy and its benefits are included in the stochastic game model. A detailed quantitative analysis is made that is applied to the random game model.

6. Conclusion

In view of the complexity of network security optimal defense strategy selection, the formal definition of network security is the most selection of optimal defense strategy. In this paper, the static matrix model and the Markov decision process are extended, and the formal definition of a random game model is presented. The model can describe the dynamic change of
network security attack and defense, in order to find the best offensive and defensive strategy for both offensive and defensive states. The experimental results show that the proposed model and algorithm are effective in attack strategy prediction and optimal active defense.

References


Ningbin Zhang received her M.S. degree in Engineering from Xi’an University. She is currently a lecturer in the School of Information Engineering at Xi’an University. Her research interests include database techniques and electronic commerce.