Research Article

Optimal Network Defense Strategy Selection Method Based on Evolutionary Network Game

Xiaohu Liu,1,2 Hengwei Zhang,1,2 Yuchen Zhang,1,2 and Lulu Shao1

1State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
2Henan Key Laboratory of Information Security, Zhengzhou 450001, China

Correspondence should be addressed to Hengwei Zhang; wby_zzmy_henan@163.com

Received 24 February 2020; Revised 9 October 2020; Accepted 17 October 2020; Published 28 October 2020

Copyright © 2020 Xiaohu Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The basic hypothesis of evolutionary game theory is that the players in the game possess limited rationality. The interactive behavior of players can be described by a learning mechanism that has theoretical advantages in modeling the network security problem in a real society. The current network security evolutionary game model generally adopts a replicator dynamic learning mechanism and assumes that the interaction between players in the group conforms to the characteristics of uniform mixed distribution. However, in an actual network attack and defense scenario, the players in the game have limited learning capability and can only interact with others within a limited range. To address this, we improved the learning mechanism based on the network topology, established the learning object set based on the learning range of the players, used the Fermi function to calculate the transition probability to the learning object strategy, and employed random noise to describe the degree of irrational influence in the learning process. On this basis, we built an attack and defense evolutionary network game model, analyzed the evolutionary process of attack and defense strategy, solved the evolution equilibrium, and designed a defense strategy selection algorithm. The effectiveness of the model and method is verified by conducting simulation experiments for the transition probability of the players and the evolutionary process of the defense group strategy.

1. Introduction

Today, the trends in network attack and defense exhibit an increasingly sharp conflict, increasingly complex confrontation scenarios, and rapid development of technical methods, and as the attacks on networks become increasingly automatic and intelligent, they are also becoming increasingly sustained and dynamic. Static defense strategies based on specific rules and attack signature matching can no longer effectively cope with frequent and multiple attacks on the network. Network security is dynamic rather than static, and therefore the defense strategy should evolve dynamically with the advancement of the attack and defense process, and the return should be maximized for the given constraints of people, time, the changing situation, resources, capabilities, and preferences [1]. Network security is relative rather than absolute, and a key factor in an effective defense measure is to minimize the expected security loss for different attack scenarios and defense strategies.

In a traditional network defense decision-making process, most of the comparison and analysis are from the perspective of the defender. The optimal defense strategy is obtained collectively, with little consideration given to the effects of the attacker’s strategy and with insufficient understanding of the antagonistic relationship between the attacker and the defender of the network [2]. In fact, the essence of cybersecurity is confrontation, and the attack and defense strategies are mutually constrained and mutually influential. The selection of a defense strategy should be studied from the perspective of attack and defender confrontation. Game theory is a theoretical tool for studying the interdependence and competition among decision-making subjects. In the real world, game theory matches up well with network attack and defense in terms of the essential characteristics of target opposition, strategy dependence, and noncooperative relationship. It has been applied by some researchers to network attack and defense behavior analysis.
and strategy selection [3–8]. In the modeling and analysis of network attack and defense based on classical game theory, there are four possible categories according to the game information set and action sequence: complete information static game, complete information dynamic game, incomplete information static game, and incomplete information dynamic game. Classical game theory generally assumes that the players in the game are completely rational, have unlimited information processing and computing power, and will not make mistakes or be influenced by others in the decision-making process. However, in the real world, this assumption is difficult to sustain, particularly because both the attack and defense players have limited rather than complete rationality. This would weaken the theoretical value and the guiding effect of the classical game model. It is therefore necessary to construct an effective game model and analysis method for the attack and defense sides that takes into account the characteristics of limited rationality.

Drawing on the idea of biological evolution, ecologists Maynard Smith and Price proposed in 1973 the concept of evolutionary stable equilibrium. In 1978, Taylor and Jonker discovered the relationship between evolutionary equilibrium and replicator dynamics, which yielded evolutionary game theory [9]. They studied the dynamic evolution of the group, overcame the restriction of complete rationality, and made game equilibrium the result of gradual optimization in the learning process of the player. This has led to a more accurate description of the evolutionary process of the group strategy. In the evolutionary game process, which is driven by the learning mechanism and the difference of game return, the dominant strategy will gradually spread among the players before finally forming the Evolutionary Stable Strategy (ESS). Some researchers have proposed a defense strategy modeling analysis method based on evolutionary game to explore the evolution of both strategies in the process of attacker and defender confrontation, as in [10–15]. Learning mechanism is the core of the evolutionary game model, and it is also the essential feature that distinguishes it from the classical game model. At present, the replicator dynamic learning mechanism is widely used in the field of network security research. The basic principle is that the player achieves evolution by constantly imitating high-return strategies. For example, an attack-defense evolutionary game model was established and an evolutionary stable equilibrium algorithm was proposed in [16] using the replicator dynamic learning mechanism to describe the rate of change of the number of players in the group who choose a specific strategy. The work in [17] focused on the advanced persistent threat (APT) attack and defense problem in cloud storage environments and established an APT attack and defense evolutionary game model using a replicative dynamic learning mechanism. The evolutionary process of the attack and defense strategies in the continuous confrontation process was also analyzed. Reference [18] took aim at the security problems faced by intelligent networks and proposed a network attack and defense framework based on an evolutionary game model using a replicative dynamic learning mechanism and also investigated how to maximize defense return with limited node resources. The network security and defense issues for the Internet of Things were investigated in [19], a multistage evolutionary game model was established, the replicator dynamic learning mechanism was used to describe the evolutionary behavior of attack and defense, and the optimal defense strategy was obtained through dynamic analysis of the evolution process. In [20], the replicator dynamic learning mechanism was improved by introducing an excitation coefficient, by perfecting the replicator dynamic rate calculation method, and by proposing an evolutionary game strategy selection method based on improved replicator dynamics. In [21], a Bayesian evolutionary game model of attack and defense was established. The influence of irrationality in the player’s strategy selection process was modeled by choosing an intensity factor, thereby improving the replicator dynamic learning mechanism. However, the above models all assumed that the players could interact through uniform mixture and complete contact; that is, each player was fully capable of learning and could learn from any individual in the group. Because this assumption did not conform to the reality of network attack and defense, it has jeopardized the guiding value of the model.

This paper offers three main contributions. (1) It improved the learning mechanism in the network attack and defense evolution game based on topological structure of the network, established the learning object set according to the learning ability of the players, and overcame the assumption that players in the group mix and interact uniformly in accordance with the objective reality that players in the attack and defense group have limited learning capability. (2) It calculated the strategy transfer probability of players to the learning object using the Fermi function, depicted the influence of irrationality in the learning process using random noise, and reflected the process of transitioning toward a dominant strategy and successive optimization of the players in the attack-defense confrontation. (3) It analyzed the specific process of solving for equilibrium in the evolutionary network game, designed a defense strategy selection algorithm, and provided an optimal defense strategy selection method.

2. Evolutionary Network Game Process Analysis and Learning Mechanism Design

2.1. Analysis of Evolutionary Network Game Process. Network security is a dynamic process in which the attack and defense players interact with and influence each other. The state of the network is determined jointly by the strategy of both the attack and the defense. As members of the groups, the attackers and defenders usually do not exist in isolation, but are related to each other in some form of social relationship, forming an attack group and a defense group within a certain network topology. In the process of the continuous dynamic game between the attack and defense groups, driven by the learning mechanism and influenced by the difference of game return, the players in the game continuously learn from other players in the group, continually lowering the probability of choosing a strategy of low return and increasing the probability of choosing a
strategy of high return. This causes the dominant strategy to gradually spread in the group until reaching equilibrium.

In actual network attack and defense, due to restrictions such as resources, capabilities, and preferences, the interaction range and learning ability of the players are usually limited; they can usually only learn from a few players nearby. To address this shortcoming, we set out in this paper to improve the learning mechanism based on network topology, in which we regard the individual players as nodes in a social network. The connections between the players are treated as network connections. On this basis, we adopted an evolutionary network game on which to model the attack and defense scenarios, to design the defense strategy selection algorithm, and to analyze the dynamic evolutionary process of attack and defense strategies that spread and stabilize in group confrontations.

**Definition 1** (learning object node). A learning object node is where a player in the game can interact with and transfer the strategy according to a specific probability within the scope of that player’s learning capability. Collectively, the learning object nodes constitute a player’s learning object set. In a social network, the average distance between players is 6 [22]. In this paper, the learning range of a player in the game is defined as 3, and the learning object set are the nodes whose distance from the player’s node network is less than or equal to 3.

The learning behavior of players’ nodes in the game can lead to adjustment and optimization of the strategy, which will lead to evolution of the state of the network’s attack and defense system. The evolution of the system state will change the attack and defense returns, which will further affect the learning behavior of the players. Under normal circumstances, because the players are less than fully rational, the system cannot achieve a stable equilibrium state through just one learning behavior, but instead promotes continuous learning and gradual evolution with time until the group strategy converges to the evolutionary stable strategy. The evolutionary dynamics process is shown in Figure 1.

### 2.2. Evolutionary Learning Mechanism Design

Learning is the intrinsic motivation of group evolution. In the current studies of network attack and defense game research, the replicator dynamic learning mechanism is the most widely used, and its core is the replicator dynamic equation [23]. This equation is used to calculate the rate of change over time \( \dot{x}_i \) of the probability \( x_i(t) \) that a particular strategy \( i \) is selected in a population:

\[
\dot{x}_i = x_i(t) (u_i(t) - \bar{u}(t)),
\]

(1)

where \( x_i(t) \) indicates the probability that the group selects strategy \( i \) at time \( t \); \( u_i(t) \) indicates the return that the player selects strategy \( i \) at time \( t \); and \( \bar{u}(t) = \sum_{i=1}^{I} x_i u_i(t) \) indicates the average return that the player in the group selects different strategies.

Because the replicator dynamic learning mechanism assumes that there is no difference in the probability of interactive learning between individuals, it is particularly suitable for population evolution with uniform mixed interaction characteristics. However, whether it is an attack group or a defense group, the learning ability and resources of the players are always limited, and it is impossible to make indiscriminate interactions with all the players in the group.

Further, the decisions of the players have certain random and irrational characteristics. Therefore, there are some limitations in describing the evolution process of attack and defense groups using the replicator dynamic learning mechanism.

In the analysis given in Section 2.1, when a player is assumed to only interact with the learning object node and to transfer its strategy to the superior strategy with a certain probability after comparing the returns, the learning process is consistent with the idea of "pairing comparison" of the Fermi function. Therefore, the replicator dynamic learning mechanism can be improved on the basis of the learning object set. Assuming that player node \( y \) is the learning object node of player node \( x \), then the probability \( W(s_x \leftarrow s_y) \) that node \( x \) strategy is transferred to node \( y \) strategy can be obtained from Fermi function:

\[
W(s_x \leftarrow s_y) = \frac{1}{1 + e^{(U_x - U_y)/\lambda}},
\]

(2)

where \( U_x \) and \( U_y \) represent the returns of node \( x \) and node \( y \), respectively, and \( \lambda \) is a random noise coefficient, with \( \lambda > 0 \).

In the evolutionary network game of network attack and defense, players tend to choose high-yield strategies. The players’ preference and sensitivity to the profit margin is an important manifestation of its irrational characteristics. In this paper, random noise coefficient is used to describe it. The random noise coefficient mainly describes the scene where the player’s irrational characteristics are mainly
affected by his preference and sensitivity to the difference of returns.

In the actual network attack and defense scenario, different values of random noise coefficient can be set according to the irrational characteristics of players. The bigger the \( \lambda \) is, the stronger the irrationality of the player is. When \( \lambda \rightarrow +\infty \), \( W(s_x \rightarrow s_y) \rightarrow 0.5 \), and it indicates that node \( x \) strategy is transferred to node \( y \) strategy in a completely random manner. When \( \lambda \rightarrow 0 \), it means that the evolutionary network game has evolved into a completely rational game, and there is no learning mechanism.

If \( U_x = U_y \), then \( W(s_x \rightarrow s_y) = 0.5 \), and it indicates that node \( x \) selects the node \( y \) strategy with a probability of 0.5. If \( U_x > U_y \), then \( W(s_x \rightarrow s_y) < 0.5 \), and \( W(s_x \rightarrow s_y) \) gradually approaches 0 as \( |U_x - U_y| \) increases, indicating that the probability that node \( x \) adopts the node \( y \) strategy diminishes. If \( U_x < U_y \), then \( W(s_x \rightarrow s_y) > 0.5 \) and gradually approaches 1 as \( |U_x - U_y| \) increases, indicating that the probability that node \( x \) adopts the node \( y \) strategy is becoming greater.

The transition probability \( W(s_x \rightarrow s_y) \) for the player node strategy to transition to the learning object node is closely related to the return and is affected by the degree of irrationality. It is consistent with the evolution process of gradual upgrade from a low-return strategy to a high-return strategy in the attack and defense confrontation, and it can depict the evolution mechanism of group strategy.

3. Construction of Evolutionary Network Game Model

From the macro time scale level, the long-term sustained learning behavior of the player node will lead to topological changes in the group network. However, from the micro time scale level, the topological structure of the group network can be regarded as static. Micro time scale is a time scale level, the topological structure of the group network changes in the group network. However, from the micro time scale level, the topological structure of the group network will not change.

Definition 2. The evolutionary network game model is represented by five elements: \( ENGM = (N, S, P, \lambda, U) \).

1. \( N = (N_A, N_D) \) is the player space of the game, \( N_A \) and \( N_D \) represent the attack group and the defense group, respectively, in the evolutionary network game, and both groups contain multiple player nodes.

2. \( S = (S_A, S_D) \) is the strategic space, where \( S_A \) and \( S_D \) represent the attack strategy and the defense strategy, respectively. Each player in the attack and defense group has multiple optional strategies. \( (S_{A1}, S_{A2}, \ldots, S_{Am}) \) represents a set of attack strategies, and \( (S_{D1}, S_{D2}, \ldots, S_{Dk}, \ldots S_{An}) \) represents a set of defense strategies with \( m, n \in N \) and \( m, n \geq 2 \).

3. \( P = (P_A, P_D) \) is the persuasion space. \( P_A \) indicates the attacker’s persuasion, which is used to describe the probability that a player in the attack group chooses different strategies. \( P_D \) is the defender’s persuasion, which is used to describe the probability that a player in the defense group chooses different strategies. The persuasion space corresponds to the strategy space, the attacker persuasion set is \( (P_{A1}, P_{A2}, \ldots, P_{Am}, \ldots P_{An}) \) with \( \sum P_{Am} = 1 \), and the defense group persuasion set is \( (P_{D1}, P_{D2}, \ldots, P_{Dk}, \ldots P_{An}) \) with \( \sum P_{Di} = 1 \).

4. \( \lambda \) is the random noise figure, indicating the degree of irrationality of the player, corresponding to \( \lambda \) in the Fermi function. In the process of evolutionary game, the higher the irrationality of the players, the stronger the randomness of the strategy selection. It is difficult to determine the irrationality of a particular individual, and it can only be determined that it belongs to a different range. Therefore, in this paper, from the perspective of groups, \( \lambda \) describes the average irrationality of players in a group.

5. \( U = (U_A, U_D) \) is the return space. \( U_A \) and \( U_D \) represent the attacker’s return and the defender’s return, respectively. In the evolutionary network game model, the returns are influenced by both the attack strategies and the defense strategies and appear in the form of a combination of returns. For example, \( U = (U_{A1}, U_{Dk}) \) indicates the attacker’s return \( U_{A1} \) and the defender’s return \( U_{Dk} \) when the attacker adopts strategy \( S_{A1} \) and the defender adopts strategy \( S_{Dk} \).

The evolutionary network game tree defined above is shown in Figure 2.

4. Solution of Evolutionary Network Game Equilibrium and Design of Defense Strategy Selection Algorithm

4.1. Evolutionary Network Game Equilibrium Solution. Before solving for the evolutionary network game equilibrium, it is necessary to first provide the strategy options for the player node. To facilitate theoretical derivation and analysis, we simplify the number of attack and defense strategies without jeopardizing generality. The strategy options open to the player nodes in the attack group are the enhanced attack strategies, designated as \( S_A = (S_{A1}, S_{A2}) \). Strategy options open to the player nodes in the defense group are the enhanced defense strategy and the common defense strategy, designated as \( S_D = (S_{D1}, S_{D2}) \).

4.1.1. Calculation of Returns. The basis for quantitative calculation and game analysis is the quantification of the player node return. For the player node to implement network attack and defense operations according to the antagonistic strategy, it takes labor, material resources,
calculation, and other costs, but at the same time it also produces corresponding security return with economic ramifications. For the defender, the choices of a defense strategy must strike a balance between cost and return in order to achieve a global optimum. Table 1 shows the symbols relevant to the definitions and the descriptions. For detailed calculation methods, see [19].

\[ AR = f(DL). \]  

The loss that was avoided due to defense strategy is counted as a defense reward \( AR \), represented by the defense loss \( DL \), in a positive value. In order to quantify and calculate the attack and defense return on the same scale, it is set that there is a functional relationship between the attack reward \( AR \) and the defense loss \( DL \), which is recorded as follows:

\[ U_A = AR - AC, \]  
\[ U_D = DL - DC. \]

Considering the two aspects of cost and return, the return of the attack and defense player nodes may be expressed by equations (4) and (5), respectively.

**Definition 3** (strategy density). Strategy density is the ratio of the number of player nodes in a group that selects a particular strategy to the total number of player nodes in the group. From the individual perspective, the player node selects a particular strategy according to its persuasion. From the group perspective, a large number of players selecting a strategy counts as the strategy density. Hence, the evolutionary state of the group is related to the change in strategy density over time.

According to the definition, let the strategy density for player nodes selecting strategy \( S_{D1} \) be \( p \):

\[ p = \frac{n}{N}, \]  
where \( n \) is the number of player nodes that select strategy \( S_{D1} \), and \( N \) is the total number of player nodes in the defense group. According to the mean field approximation theory, any defense player node will select a strategy according to the strategy density. Therefore, the persuasion for selecting strategy \( S_{D1} \) is \( p \), and the persuasion for selecting strategy \( S_{D2} \) is \( 1-p \).

Similarly, we assume that the strategy density for an attack player node to select strategy \( S_{A1} \) is \( q \):

\[ q = \frac{m}{M}, \]  
where \( m \) is the number of player nodes that select strategy \( S_{A1} \), and \( M \) is the total number of player nodes in the attack group. According to the mean field approximation theory, any player node in the attack group would select strategies according to the strategy density. Hence, the persuasion for selecting strategy \( S_{A1} \) is \( q \) and the persuasion for selecting strategy \( S_{A2} \) is \( 1-q \).

The return of the player node in the game is determined jointly by the attack and defense strategies. The player node in the attack group and the player node in the defense group each has two types of optional strategies. The attack and defense game tree is shown in Figure 3.

For the player node in the defense group, the expected return for selecting strategy \( S_{D1} \) is \( U_d = qU_{D1} + (1-q)U_{D2} \). For the player node in the attack group, the expected return for selecting strategy \( S_{A1} \) is \( U_a = pU_{A1} + (1-p)U_{A3} \).

**Definition 4** (trend node). The trend node is a virtual node that represents the overall trend and direction of the evolution of the attack and defense groups. The return of the trend node is the expected return under different strategic density combinations of the attack and defense groups, and it changes dynamically with the evolution of the group strategy.

The return of trend node \( \overrightarrow{a} \) in the attack group is

\[ U_{\overrightarrow{a}} = pqU_{A1} + p(1-q)U_{A2} + (1-p)qU_{A3} + (1-q)(1-p)U_{A4}. \]

The return of trend node \( \overrightarrow{d} \) in the defense group is

\[ U_{\overrightarrow{d}} = pqU_{D1} + p(1-q)U_{D2} + (1-p)qU_{D3} + (1-p)(1-q)U_{D4}. \]
4.1.2. Equilibrium Solution. The learning behavior of the player node leads to dynamic changes in the group strategy density with time, and its dynamic rate of change may be used to characterize the evolution state of the group. By taking time derivatives of the strategy density $p$ of $SD_1$ and strategy density $q$ of $SA_1$, we define an evolution equation of the attack and defense groups and form the simultaneous equations shown in the following equation:

$$\begin{align*}
\frac{dp}{dt} &= p(1-p)[W(d\leftarrow d) - W(d\rightarrow d)] = p(1-p)\left[\frac{1}{1+e^{(U_d-U_d)/\lambda}} - \frac{1}{1+e^{(U_d-U_d)/\lambda}}\right], \\
\frac{dq}{dt} &= q(1-q)[W(a\leftarrow a) - W(a\rightarrow a)] = q(1-q)\left[\frac{1}{1+e^{(U_a-U_a)/\lambda}} - \frac{1}{1+e^{(U_a-U_a)/\lambda}}\right].
\end{align*}$$

(10)

In order to solve the equations, we introduce an auxiliary function tanh:

$$\tanh\left(\frac{U_x-U_{\rightarrow x}}{2\lambda}\right) = \frac{1}{1+e^{(U_x-U_{\rightarrow x})/\lambda}} - \frac{1}{1+e^{(U_{\rightarrow x}-U_x)/\lambda}}$$

(11)

Let $z = (U_x-U_{\rightarrow x})/2\lambda$, then equation (11) can be converted to

$$\begin{align*}
\frac{dp}{dt} &= p(1-p)[W(d\leftarrow d) - W(d\rightarrow d)] = -p(1-p)\tanh\left(\frac{U_d-U_{\rightarrow d}}{2\lambda}\right), \\
\frac{dq}{dt} &= q(1-q)[W(a\leftarrow a) - W(a\rightarrow a)] = -q(1-q)\tanh\left(\frac{U_a-U_{\rightarrow a}}{2\lambda}\right).
\end{align*}$$

(13)

When the rate of change of strategy density in the attack and defense group is zero, the game process reaches a state of evolutionary equilibrium [24]. At this point, the equations satisfy the following condition:

---

**Table 1: Symbols and description.**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Measurement method</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Attack cost</td>
<td>Resources required by the attacker to implement the attack strategy</td>
</tr>
<tr>
<td>AR</td>
<td>Attack reward</td>
<td>The reward of the attacker from the implementation of the attack strategy</td>
</tr>
<tr>
<td>DC</td>
<td>Defense cost</td>
<td>Resources required by the defender to implement a defense strategy</td>
</tr>
<tr>
<td>DL</td>
<td>Defense loss</td>
<td>Damage suffered by the defender due to the attack by the attacker</td>
</tr>
</tbody>
</table>

---

**Figure 3: Attack and defense game tree.**
Calculations show that there are five sets of solutions for equation (14), and there may be five corresponding evolutionary equilibrium points.

(1) $F_1 = \begin{bmatrix} p = 0 \\ q = 0 \end{bmatrix}$, indicating that the player node in the defense group selects pure strategy $S_{D2}$, the player node in the attack group selects pure strategy $S_{A2}$.

(2) $F_2 = \begin{bmatrix} p = 0 \\ q = 1 \end{bmatrix}$, indicating that all the player nodes in the defense group adopt pure strategy $S_{D2}$, the player node in the attack group adopts pure strategy $S_{A1}$.

(3) $F_3 = \begin{bmatrix} p = 1 \\ q = 0 \end{bmatrix}$, indicating that all player nodes in the defense group select pure strategy $S_{D1}$, the attack group adopts pure strategy $S_{A2}$.

(4) $F_4 = \begin{bmatrix} p = 1 \\ q = 1 \end{bmatrix}$, indicating that all player nodes of the defense group select pure strategy $S_{D1}$, the attack group adopts pure strategy $S_{A1}$.

(5) $F_5 = \begin{bmatrix} \tanh((U_d - U_{d^-})/2a) = 0 \\ \tanh((U_a - U_{a^-})/2a) = 0 \end{bmatrix}$, indicating that the strategy transition probabilities $W_{d \rightarrow d}$ and $W_{a \rightarrow a}$ from player node in the attack and defense group to the trend node are equal to the strategy transition probabilities $W_{d \rightarrow a}$ and $W_{a \rightarrow d}$ from the trend node to the player node and that the group evolution enters a dynamic equilibrium state. Solve for $F_5$ with MATLAB R2018A and obtain $p = (U_{A4} - U_{A3})/(U_{A1} - U_{A2} - U_{A3} + U_{A4})$ and $q = (U_{D4} - U_{D2})/(U_{D1} - U_{D2} - U_{D3} + U_{D4})$, designated as $p^*$ and $q^*$, respectively.

According to the evolutionary game theory, $F_1$, $F_2$, $F_3$, and $F_4$ are saddle points, and $F_5$ is a central point. The evolutionary network game model is based on a strategy of evolutionary stability. By combining the initial states of different attack and defense groups, this method can be used to predict the possible attack strategy used by the attacker and to guide the defender in selecting the defense strategy.

4.2. Design of Defense Strategy Selection Algorithm. Based on the evolutionary network game equilibrium solution discussed in Section 4.1, a defense strategy selection algorithm is designed, as shown in Table 2.

If the number of optional strategies of the attacker is $m$, and the number of optional strategies of the defender is $n$. The time complexity of the algorithm mainly focuses on the revenue comparison of different attack and defense strategies. The time complexity of the defense strategy selection algorithm is $O((m + n)^2)$. The space complexity of the algorithm mainly focuses on the storage of the profit value and the intermediate results of equilibrium solution. The space complexity of the defense strategy selection algorithm is $O(mn)$. The comparison shows that the time complexity and space complexity of the algorithm are in the same order of magnitude as those in the related literature [20, 21].

The analysis shows that the more the number of attack and defense strategies, the higher the time complexity and space complexity of defense decision algorithm. Therefore, in practical application, the attack and defense strategies can be classified to reduce the number of attack and defense strategies and improve the algorithm solving speed.

4.3. Comparison of Research Results. In this section, we analyze and compare the results of this paper with those of other relevant studies in terms of five aspects: learning range, learning mechanism, random interference, detailed process, and application scenarios of the solution process. The comparison results are shown in Table 3.

Of the five aspects, the range of learning mainly examines whether the interactive objects in the model are all the players or the learning object set. The learning mechanism reflects the mechanism used by the model to describe the learning behavior of the players in the game. The random interference mainly examines whether the model takes into account the irrationality of the players in the game. The ESS solution process primarily investigates the degree of detail of the evolutionary equilibrium solution process. The more detailed the solution process, the greater the guiding effect on the practice. The application scenario is mainly distinguished according to the application object of the model. Most of the studies do not consider the topology of the group network and assume that the players in the group can interact with the whole group in a uniform and mixed manner. The learning and emulating behaviors of players are described using the replicator dynamic learning mechanism without considering the limitations on player learning ability. As a result, the influence of random interference in the selection process of the players is not taken into account. Moreover, since the ESS solution is relatively simple, it can only provide limited practical guidance for selecting a defense strategy. The comparison shows that the security game model based on the evolutionary game network is more in line with the actual network attack and defense and can provide valuable practical guidance.

5. Analysis of Simulation Experiments and Results

In order to confirm the validity of the model and method, we conducted simulation experiments on the strategy transition probability of the players and the evolution process of the defense group strategy. The simulation experiment of the strategy transfer probability of the players was used to verify whether the learning mechanism in the model conforms to the reality of network attack and defense and to analyze the relationship between the strategy transfer probability $W$ and the random noise coefficient $\lambda$ of the player. The simulation experiment on the defense group strategy evolution process was used to study the relationship between the dynamic change in the group strategy and the strategy density of the
attack and defense groups. The analysis provides an understanding of the behavior of dynamic evolution, diffusion, and stability of the defense group strategy for different initial conditions.

5.1. Simulation Experiment of Player Strategy Transfer Probability. Based on network topology, the evolutionary network game model improves the learning mechanism. The player node uses the Fermi function to calculate the strategy transition probability to the learning object node, and the parameters involved are the player node gain and the random noise coefficient. Therefore, the interval for $U_x$ and $U_y$ of the simulation experiments is set to $(0, 10)$ and the random noise coefficient $\lambda$ of the players is, respectively, 0.1, 0.5, 1, and 5. The strategy transition probability from node $x$ to learning object node $y$ as $U_x$ and $U_y$ changes is plotted in Figure 4 with MATLAB R2018A software for four different values of $\lambda$.

Figure 4 contains four subgraphs of (a), (b), (c), and d, which shows the change in the strategy transition probability $W$ for $\lambda$ values of 0.1, 0.5, 1, and 5 as $U_x$ and $U_y$ change.

By analyzing the common trend of the four subgraphs, we arrived at the following conclusion on the relationship between $W$ and the relative value of the player return: the smaller $U_x$ is than $U_y$, the greater is $W$, and the greater $U_x$ is than $U_y$, the smaller is $W$. The results of the simulation experiments are consistent with the actual evolution law of the network attack and defense confrontation in that the players transition from a low-return strategy to a high-return strategy.

After comparing the trends of the four subgraphs, we arrived at the following conclusion on the relationship between $W$ and the random noise coefficient $\lambda$. The higher the value of $\lambda$, the closer the value of $W$ to 0.5 and the smaller the fluctuation, indicating a higher randomness of the strategic transfer of the player node. The simulation results are consistent with the irrational random selection of the attack and defense cyber confrontation.

In the simulation experiments on the strategic transfer probability of the player node in the game, the learning mechanism was found to be consistent with the actual evolutionary behavior of the network attack and defense, which verified the correctness and effectiveness of the learning mechanism in the evolutionary network game model.

5.2. Simulation Experiments on Defense Group Strategy Evolution Process. Due to the confrontational nature of network attack and defense, the process of strategy evolution of the defense group is affected by both the attack and defense strategies. In order to analyze the strategy evolution of the defense group, we investigated the relationship between the rate of change $dp/dt$ of the defense group strategy density and the defense group strategy density $p$ and the

---

Table 2: Defense strategy selection algorithm.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Algorithm Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initialize $ENGM = (N, S, P, \lambda, U)$;</td>
</tr>
<tr>
<td>2</td>
<td>Initialize strategy space and strategy density of the attack group;</td>
</tr>
<tr>
<td>3</td>
<td>Initialize strategy space and strategy density of the defense group;</td>
</tr>
<tr>
<td>4</td>
<td>Calculate return $U_A$ of attack player node (Equation (8));</td>
</tr>
<tr>
<td>5</td>
<td>Calculate return $U_D$ of defending player node (Equation (9));</td>
</tr>
<tr>
<td>6</td>
<td>Calculate probability of player node strategy transition (Equation (2));</td>
</tr>
<tr>
<td>7</td>
<td>Calculate time evolution of player group strategy density (Equation (10));</td>
</tr>
<tr>
<td>8</td>
<td>Introduce auxiliary function tanh (Equation (12));</td>
</tr>
<tr>
<td>9</td>
<td>Solve equation set for equilibrium point (Equations (13) and (14));</td>
</tr>
<tr>
<td>10</td>
<td>Refine equilibrium point and screen evolutionary stability strategy;</td>
</tr>
<tr>
<td>11</td>
<td>Output optimal defense strategy;</td>
</tr>
<tr>
<td>12</td>
<td>End</td>
</tr>
</tbody>
</table>

Table 3: Comparison analysis of pertinent literatures.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Learning range</th>
<th>Learning mechanism</th>
<th>Random disturbance</th>
<th>ESS solution</th>
<th>Application scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>[16]</td>
<td>All players</td>
<td>Replicator dynamics</td>
<td>No</td>
<td>Detailed</td>
<td>Cyber defense</td>
</tr>
<tr>
<td>[17]</td>
<td>All players</td>
<td>Replicator dynamics</td>
<td>No</td>
<td>Detailed</td>
<td>Cloud storage</td>
</tr>
<tr>
<td>[18]</td>
<td>All players</td>
<td>Replicator dynamics</td>
<td>No</td>
<td>Simple</td>
<td>Smart grid defense</td>
</tr>
<tr>
<td>[19]</td>
<td>All players</td>
<td>Replicator dynamics</td>
<td>No</td>
<td>Simple</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>[20]</td>
<td>All players</td>
<td>Incentive coefficient + replicator dynamics</td>
<td>No</td>
<td>Detailed</td>
<td>Network defense</td>
</tr>
<tr>
<td>[21]</td>
<td>All players</td>
<td>Select intensity factor + replicator dynamics</td>
<td>Yes</td>
<td>Detailed</td>
<td>Network defense</td>
</tr>
<tr>
<td>This paper</td>
<td>Learning object set</td>
<td>Fermi function + replicator dynamics</td>
<td>Yes</td>
<td>Detailed</td>
<td>Network defense</td>
</tr>
</tbody>
</table>
attack group strategy density $q$ and carried out the simulation experiment of the defense group strategy evolution process.

According to experts’ experience and historical data and [19, 20], we assigned values to the attack return and the defense return involved in the attack and defense game tree in Figure 3, as shown in Table 4.

Based on the values of the attack and defense return and the evolutionary network game equilibrium solution $F_2$, we obtained $p^* = 0.7$ and $q^* = 0.6$. In the simulation experiment, the values of $p$ and $q$ were set to the interval of $(0, 1)$, and the change interval was 0.025. A total of 1,600 different combinations of $p$ and $q$ can be simulated. MATLAB R2018A software was used to simulate the rate of change $dp/dt$ of the defense group strategy density with the changes of $p$ and $q$, as shown in Figure 5.

Figure 5 shows a three-dimensional view of $dp/dt$ with respect to $p$ and $q$. For the convenience of observation and analysis, (a) and (b) represent two different side views of the three-dimensional map, respectively. The defense group strategy density $p$ and the attack group strategy density $q$ combined to form the initial state $(p, q)$ of the game model. According to the relationship between $(p, q)$ and $(p^*, q^*)$, the evolution process of the defense group strategy can be divided into four cases:

Case 1. $p < p^*$ and $q < q^*$, then $dp/dt > 0$ at this time. This shows that in the continuous confrontational evolution, the probability of selecting strategy $S_{D2}$ by players in the defense group becomes higher and higher, and the probability of selecting strategy $S_{D1}$ becomes lower and lower, and the process gradually converges to $p = p^*$. At the same time, as $p$ gradually increases, the value of $dp/dt$ gradually increases, indicating that the rate at which $p$ increases becomes faster and faster.

Case 2. $p > p^*$ and $q > q^*$, then $dp/dt > 0$ at this time. This shows that in the continuous confrontational evolution, the probability of selecting strategy $S_{D1}$ by players in the defense group becomes higher and higher, the probability of selecting strategy $S_{D2}$ becomes lower and lower, and the process gradually converges to $p = p^*$. At the same time, as $p$ gradually increases, the value of $dp/dt$ gradually decreases, indicating that the rate at which $p$ increases becomes slower and slower.

Case 3. $p > p^*$ and $q < q^*$, and $dp/dt < 0$ at this time. This shows that in the continuous confrontational evolution, the probability of selecting strategy $S_{D1}$ by players in the defense group becomes lower and lower, the probability of selecting strategy $S_{D2}$ becomes higher and higher, and the process gradually converges to $p = p^*$. At the same time, as $p$ gradually decreases, the value of $dp/dt$ gradually decreases, indicating that the rate at which $p$ decreases becomes slower and slower.

Case 4. $p > p^*$ and $q > q^*$, and $dp/dt < 0$ at this time. This shows that in the continuous confrontational evolution, the probability of selecting strategy $S_{D1}$ by players in the defense group becomes lower and lower, the probability of selecting strategy $S_{D2}$ becomes higher and higher, and the process gradually converges to $p = p^*$. At the same time, as $p$...
gradually decreases, the value of \( \frac{dp}{dt} \) gradually increases, indicating that the rate at which \( p \) decreases becomes faster and faster.

Through the simulation experiments and analysis of the results, we gained an understanding of the evolutionary process of the group strategy of the defense group. The evolutionary process of the defense group strategy is closely related to the game return and is affected by the initial state of the probability density of the attack and defense group strategies. It is therefore necessary to study the selection of defense strategy from the perspective of attack and defense confrontation and to determine the optimal defense strategy through evolutionary network game analysis.

6. Conclusion

Both the network attacker and the network defender are people of limited rationality. In the study of network attack and defense based on game theory, one must overcome the assumption of traditional game theory that people are completely rational. The evolutionary game theory breaks through the constraint that people are completely rational in the game and regards the game equilibrium as the result of the gradual optimization of the players’ learning and evolution in the game. The simulation experiment of the strategy transfer probability of the player in the game verified the effectiveness of the learning mechanism. The simulation experiment of the strategy evolution process of the defense group provided the evolitional behavior of the strategy of the defense group for different attack and defense strategy densities. The model can describe the process of dynamic evolution and more accurately depict the diffusion and equilibrium process in the group confrontation. The modeling and analysis results are closer to the essence of the network attack and defense, can more realistically explain and predict the network attack and defense behavior, and guide the defense practice.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Authors’ Contributions

Xiaohu Liu and Hengwei Zhang contributed equally to this work.

Acknowledgments

This work was supported by the Henan Science and Technology Research Project (Nos. 182102210144 and 192102210293).

References


