IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 10, 2018, accepted May 21, 2018, date of publication May 29, 2018, date of current version June 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2841885

Optimal Network Defense Strategy Selection Based on Incomplete Information Evolutionary Game

HAO HU[1,2], YULING LIU[3], HONGQI ZHANG[1,2], AND RUIXUAN PAN[1,2]

[1]China National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450001, China
[2]The Third College, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China
[3]Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Corresponding author: Yuling Liu (ylliu@tca.iscas.ac.cn)

This work was supported in part by the National Key Research and Development Program of China under Grants 2016YFF0204002 and 2016YFF0204003, in part by the Equipment Pre-Research Foundation During the 13th Five-Year Plan Period under Grant 6140002020115, in part by the CCF-Venus ''Hongyan'' Scientific Research Plan Foundation under Grant 2017003, and in part by the Science and Technology Leading Talent Project of Zhengzhou under Grant 131PLJRC644.

ABSTRACT The issue of selecting the optimal defense strategy in the dynamic adversarial network is difficult. To solve this problem, we start from the realistic bounded rationality of both the attacker and the defender. First, we build the Bayesian attack–defense evolutionary game model combining with incomplete information game scenario. Specifically, we convert the uncertainty of the strategy payoffs of attackers and defenders to the uncertainty of their related types. Meanwhile, both the set of player types and the set of game strategies can be expanded to n in our model. Furthermore, we improve the replicator dynamics equation by adding the selecting intensity factor to depict the noise effect. This reflects the randomness of decision making for players due to their bounded learning capacities. In this way, the static analysis in the traditional game is extended as a dynamic process. On this basis, we summarize the evolutions of different player types with different strategies. Finally, by calculating the evolutionary stable equilibrium, we give the algorithm of selecting optimal defense strategy and depict the evolutionary track of this strategy selected by the defender with time going by. Our method provides decision support for the network proactive defense toward moderate security. Moreover, the dynamic analysis efficiency of defense decision making is improved, and the predicting ability of the defense situation is enhanced. Experimental results verify the scientificity and availability of the proposed model and method.

INDEX TERMS Network attack-defense, incomplete information, bounded rationality, evolutionary game, optimal defense strategy.

I. INTRODUCTION

With the complexity of large-scale network information system, security attacks become more and more diversified. Therefore, it is urgent to analyze and predict the attack-defense behavior of the network, and then implement proactive defense. Game theory is a decision-making theory for studying the direct interaction between decision-making entities. It has the characteristics of objective opposition, non-cooperative and strategic dependence, all of which are in line with the basic characteristics of network attack and defense. Therefore, applying the game theory to model and analyze network attack-defense processes has become a hot research issue in recent years [1].

This paper aims at the security issue of defense strategies selection in the network attack-defense environment. Based on the bounded rationality of both attack-defense players, this paper formulates Bayesian evolutionary game model in the incomplete information scenario. Meanwhile, we expand the capability of player types set and strategies set to any n. We treat the uncertainty of attack-defense strategies as the uncertainty of player's type. Moreover, we expand the static analysis of Nash equilibrium to the dynamic and evolving process. Based on this, we explore the replicated dynamic equations to describe the attack-defense behaviors, summarize the evolutionary processes of different strategies with different player types, and give the optimal defense strategy by

calculating the evolutionary stable equilibrium. Afterwards, we describe the evolutionary track of the final selection of players to provide dynamic decision-making for network proactive defense.

The main contributions of this paper are

1) The evolutionary game model of incomplete information on network security attack-defense is developed. Our model transforms the uncertainty of the game characteristics between both sides of attacker and defender to the uncertainty of each other's type, which is consistent with the fact of incomplete information scenario.

2) The stochastic replicator dynamic equations for decision-making of both sides of attacker and defender are constructed. By bringing in the selecting intensity factor to reflect the noise effect, we improve the replicator dynamic equations to describe the evolutionary track of strategy more accurately.

3) The selection algorithm of optimal defense strategy is designed. It provides support of decision-making for network proactive defense under moderate security. Moreover, the proposed algorithm is more practical, since it allows the defender to consistently update his strategy on his opponent's strategy as the game evolves.

II. RELATED WORKS

In the study of network security using game theory, the accuracy and scientificity of the game model are limited to two key hypothesizes: 1) whether the game information is incomplete for both sides of attacker and defender and 2) whether the game players are bounded rationality.

According to whether the game information is open or not, existing researches can be categorized as the complete information game and the incomplete information game, the information is the knowledge about the game features such as the strategy set and the payoff function of each other in both sides of attack-defense. The complete information game means that each player has the accurate knowledge of other players' knowledge. For example, Jiang *et al.* [2], [3] handled the network attack-defense as the zero-sum game process, in which both players have complete information and take actions at the same time. On this basis, they established non-cooperation static game model and stochastic game model to implement network security evaluation [2] and defensive strategy selection [3] respectively. In practical applications, for example, for the security issue of sensor networks, implementing replicating node attack may increase the attack cost, to analyze the optimal attack strategy, Li *et al.* [4] established a complete information game model between attacker and sensor trust node, further by calculating the Nash equilibrium, the optimal solution is provided. Agah and Das [5] developed the complete information repeated game model between the intrusion detection system and the wireless sensor nodes, and then analyzed the retransmission strategies of the node packets. Considering that smart grid is vulnerable to malicious SQL injection attacks, Esmalifalak *et al.* [6] considered the action times of attack-defense as the basic strategies and established a two-person zero-sum complete information game model by using the increase/decrease on power prices as the payoff function, and verified the proposed model in Electricity Market. Wu *et al.* [7] further used the reinforcement-learning algorithm to solve the Nash equilibrium and achieved the assessment and prediction of the security situation of the grid system. Serra *et al.* [8] used Pareto algorithm to optimize the solving procedure of Nash equilibrium, which reduces the computational complexity. Wang *et al.* [9] combined Petri nets with the stochastic game model for minimizing attack benefit. They established a zero-sum game model under the condition of complete information, and then evaluated the network security quantitatively. To sum up, it is easy to find that the above models all adopt the complete information hypothesis, which is hard to be implemented in realistic attack-defense adversarial network. Since the strategies' payoffs are the private information for the game players, the attack-defense information of the actual network is asymmetric and intimate.

To break the limitation of complete information, Liu *et al.* [10] analyzed the impacts of the changes of strategies on attack-defense performance in the scenario of worm attack. Based on incomplete information conditions and with the Bayesian game model, they considered the cases of three different types of attacker. However, they mainly focused on the Nash equilibrium of pure strategy. From the perspective of dynamic resist and incomplete information, Zhang *et al.* [11] and Liu *et al.* [12] handled the defender as the sender of the signal and the attacker as the receiver of the signal. During the game process, the attacker identifies the type of defender based on the defense signal. Such studies include the single stage [11] and the multi-stage incomplete information attack-defense signal game model [12], which gives the calculating method of optimal defense strategy and enhances the accuracy and dynamics of strategy decision-making. Patcha and Park [13] built a signal game model for individual node of network, and analyzed the optimal response strategy of the intrusion detection system. However, all of the above investigations are based on the hypothesis that both sides of attacker and defender are completely rational and know how to realize the maximization of their payoff. Moreover, they will choose strategies earning maximum payoffs at the same time. In fact, it is hard for the attack-defense behaviors of the network to be completely rational. The environment and personal interests may affect the players. In general, they are bounded rationality agents. Ignoring the precondition of bounded rationality, it may lead to deviation for the modeling and analyzing of attack-defense behaviors and impact the scientific and guidance of the selection method for optimal defense strategy. Therefore, the application of bounded rationality in the game analysis of network security is significant and has practical significance [14].

In recent years, some scholars try to use the evolutionary game model to describe the evolutionary process of network adversarial behaviors. The evolutionary game benefits from the idea of biological evolution. Based on the

bounded rationality of game players, they consider that the game players improve their strategy choices by combining with historical experience. The network gradually evolves to a stable state through the learning and improving mechanism, through which one can effectively improve the reliability and accuracy of the analysis of game behaviors. Liu *et al.* [15] proposed a game-theoretic approach to achieve an energy-efficient cooperative defense scheme. Specifically, to increase security of data in the sensor-cloud, a two-layer gateway-assisted detection and defense decision problem involving multiple intrusion detection systems using an evolutionary game is formulated, which optimizes the detection strategy for lowering energy consumption and reducing alert messages. Zhu *et al.* [16] used the system dynamics to model the evolutionary process of attack-defense game, and developed the economic cost model under the condition of complete information. The proposed model benefits the governance of network security. However, it only abstracts two kinds of attack-defense strategies from a global perspective, namely, attack/no attack and defense increase/not decrease. Therefore, the analysis of generalized game structure is not given. Taking into account that the randomness of attack-defense methods will inevitably lead to the state transition for the game system, in order to analyze the system stable equilibrium in different system states. Huang *et al.* [17] analyzed the optimal defense strategy in different security states with Markov decision process, and used linear programming algorithm to calculate the optimal solution, but Huang *et al.* treated the attack-defense strategies and payoffs as public knowledge, and there is only one type for the attacker/defender respectively. In essence, it still belongs to the category of complete information game. Based on the non-cooperative game theory, Huang *et al.* [18] furthered constructed an attack-defense evolutionary game model and studied the replicator dynamics and evolutionary stable strategy of both sides of attacker and defender. However, the model is still limited to the hypothesis of incomplete information and mainly analyzes the deterministic evolutionary behavior. To analyze the strategy selection of whether or not to adopt the antivirus software to against the malware, Hayel and Zhu [19] established an evolutionary Poisson game framework and designed mechanisms to control software users' behaviors to achieve a system-wide objective. Chen and Yeh [20] investigated the game strategies of how to select some beneficial genetic variations for non-cooperative and cooperative evolutionary game. His research focus on the analysis of how the non-cooperative strategy can be converted to an equivalent multi-objective optimization (MOEA) problem and a MOEA-based searching algorithm was designed to solve the problem. For evaluating the quality of an optimal evolution solution, Liu and Liu [21] explained that the robustness is an important index and studied the robustness of the coevolution rules against attacks for cooperation game. However, the information requirement in the above researches is still limited to the complete information, which requires that individual player always prefers high-payoff strategy during the process of selection. In fact, since different players have different cognize abilities and asymmetric information, the process of strategy improvement will inevitably be lack of far-sight. Therefore, the local short-sighted strategy has its own rationality. It is of great significance to explore non-deterministic strategy evolutionary analysis.

In recent years, the range and application range of evolutionary game research is expanding. Such as the social network modeling, to explore the effect of users' decisions, actions, personal interests, and socio-economic interactions on the scientific problem related with the social network population, Du *et al.* [22] explored the community-structured evolutionary game for privacy protection in social networks, which can promote the spreading of privacy protection behavior throughout the network. The dynamics of information diffusion process over social networks using evolutionary game theoretic framework was formulated by Jiang *et al.* [23], [24], which highlighted the correspondence between the evolutionary game theory and information diffusion. Wang *et al.* [25] gave the analysis of population behavior of social networks by employing the evolutionary game, but did not give a detailed solution of how to calculate the solution of equilibrium. By combing the above researches, we can derive that evolutionary game theory has been successfully applied in some related fields and gained some outstanding achievements, which provide a significant reference for exploring the game law in the field of network security. However, the investigations in the direction of network security are not many, and its research in the network security is still in its infancy.

In terms of information requirements, the current researches only consider the complete information condition. They require players to master adversary's information accurately. However, the information is asymmetric and the complete information reduces the operability of the model. For game type and game structure, existing approaches requires that the attack-defense players have fixed kinds of type, and analyze the simple structure containing two independent strategies. In the future study, we should consider the generalized game structures. In terms of evolutionary behavior, existing researches mainly explore the deterministic strategy, but do not consider nondeterministic strategy caused by the incomplete information. Therefore, studying the stochastic evolutionary strategy is closer to the practical application. In terms of the equilibrium solution, the current researches calculate the equilibrium by forming payoff matrices and focus on how to optimize the calculation process, but do not deeply summarize the dynamic process of strategy evolution. Promising directions lay in the analysis of strategy selection varies with time. In terms of application scenarios, no matter the behavior analysis of social network or the dynamics research of security governance, they in essence base on the strategies selections, so that the researches on the issue of strategy selection is more general.

III. INCOMPLETE INFROMATION ATTACK-DEFENSE EVOLUTIONARY GAME MODEL

In this section, we first give the motivations of this paper, and then construct the attack-defense evolutionary game model under the condition of incomplete information. Finally, we develop the evolutionary equations of strategy selection.

A. MOTIVATION ANALYSIS

Network attack-defense has the characteristics such as non-cooperation, incomplete information and limited rationality, etc. Based on this, the motivations are as follows.

1) Attack-defense incomplete information. In view of the incomplete information game scenario, by borrowing the Hessian transformation [26], the paper converts the uncertainty of attack-defense strategy payoff to the uncertainty of attack-defense player's type. We first assign each player with a unique type related to its strategy and payoff. The type is the private knowledge of the player. It determines the occurrence probability of each type. The probability distribution of the types is a public knowledge that all players can calculate through historical statistics data. From this aim, we convert the probability calculations of player types to that of players' strategies.

2) Attack-defense bounded rationality. During the process of network adversary, different attackers and defenders have different abilities of cognizance, which is influenced by their own interests such as safety knowledge, skill level, experience, etc. Therefore, the selections of strategies affected by various uncertain factors lead to the bounded rational repeated game. With time going by, the payoff differences between different strategies populations will change. By studying and modifying the strategy selection of other populations, under the driving of this evolutionary mechanism, low-payoff populations continue to follow the strategies of high-payoff populations in order to improve their own strategy. Starting from the sets of attack-defense strategies, this paper develops the evolutionary game model to explore the tracks of the attack-defense strategy dynamic evolutions.

B. INCOMPLETE INFORMATION ATTACK-DEFENSE EVOLUTIONARY GAME MODEL

Based on the analysis in Section III-A, we give the definition of the evolutionary game model of network attack-defense by referring to the basic two-player game model [27], [28], which includes five basic elements: attack-defense players set, player types set, probability distribution set of player types, attack-defense strategies set and payoff function set.

Definition 1: Attack-defense Incomplete Information Evolutionary Game Model AIEGM can be formalized as a 5-tuple $\text{AIEGM} = (N, T, E, S, U)$.

1) $N = (N_A, N_D)$ is the set of population of game players, where N_D is the population of defenders, and N_A is the population of attackers.

2) $T = (T_A, T_D)$ is the space of attack-defense types of players, $T_A = \{t_1, t_2, \cdots, t_\lambda\}$ is the type space of the attacker population, where $\lambda \in N^+$ and $\lambda \geq 2$, λ is the total number of attacker types. $T_D = \{t\}$ is the type of the defender.

3) $E = (E_A, E_D)$ is the probability distribution of the type of the players, $E_A = \{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_\lambda\}$ is the probability distribution set of the attacker type space $\{t_1, t_2, \cdots, t_\lambda\}$, that is, the probability of attacker type t_k is ε_k, $1 \leq k \leq \lambda$. The defender population has only one type t and the probability of this type is 1.

4) $S = (S_A^k, S_D)$ is a set of attack-defense strategies, $S_A^k = \{A_1, A_2, \cdots, A_n\}$ is the optional strategies space of the attacker with type t_k, $S_D = \{D_1, D_2, \cdots, D_m\}$ is the optional strategies space of the defender, where $m, n \in N^+$ and $m, n \geq 2$, $1 \leq i \leq n$, $1 \leq j \leq m$, n and m are the total number of attack and defense strategies respectively.

5) $U = (U_A, U_D)$ is the set of payoff functions, U_A and U_D are the payoff functions of the attacker and defender respectively. It refers to the profit value of player obtaining from its strategy. The function $U_A(t_k, A_i, D_j)$ is related to the player type space and strategy space. $a_{kij} \in U_A$ and $d_{kij} \in U_D$ respectively denote the payoff value of the t_k type attacker and defender when their strategy combination is (A_i, D_j).

Remarks:

1. In condition 1), the general attack-defense scenario includes multiple participants. To simplify our analysis, our model abstracts multiple participants with the same type as a player population.

2. In condition 2), the motivation behind our Bayesian game formulation is that, generally an attacker/defender game is an incomplete information game where only the defender is uncertain about the type of his opponent (regular or malicious) [29]. Besides, the security defense servers for the information system. Because of the needs of open service, product advertising, social supervision, and commercial interests, the defense strategies taken by defenders are public knowledge to some extent. Therefore, we consider that there is only one type 't' for the defenders, which is common knowledge to the two players [29]. The scenario of one type defender is more practical. The type of attacker is related with its attacking behaviors and is the attacker's private information. Thus, we take into account of multiple different types of attackers $t_1, t_2, \cdots, t_\lambda$ for satisfying the flexibility and the scalability of our game structure.

3. In condition 4), for the extraction of attack-defense strategies, we first analyze network environment information, including network topology, connectivity and vulnerability information, etc. Among which, topology is obtained based on network structure statistics, network connectivity is achieved based on the network firewall filtering rules, and vulnerability is gained using vulnerability scanning tool like Nessus, In addition, through analyzing vulnerability upgrade, rules adjustment of firewall access, configuration updates of security devices, etc., we extract defense strategies set.

Furthermore, through collecting the alert data of firewalls, host logs, intrusion prevention systems, virus detection systems and other sensors, we can analyze attack behaviors. Finally, through referring to the database of attack-defense behaviors published by MIT Lincoln Laboratory [31], we can extract the feasible strategies of attacker and defender.

4. In the classic complete rational game model, Nash equilibrium is explained as the optimal reaction between both two sides of attacker and defender, but no forming process of Nash equilibrium is given. The emphasis of this paper is to analyze the evolutionary process of attack-defense strategies. In addition, we try to simulate the process of strategies learning and adjustment. We also describe the dynamic evolutionary track of strategy.

C. PAYOFF QUANTIFICATION OF ATTACK-DEFENSE STRATEGIES

Payoff quantification of attack-defense strategies is the basis for selecting the optimal defense strategy. The accuracy of quantification directly affects the results of defense strategy selection. Jiang *et al.* [3] summarize a large number of attack-defense strategies and their classification, and propose a quantifiable method of payoff based on benefit/cost, but they do not consider the benefit returned by defender's counterattack. In this paper, we further optimize it.

Definition 2: Attack Benefit AB is the network resource value obtained by an attacker, which reflects the attacker's ability to control target network resources.

Definition 3: Attack Cost AC is the cost of human, time and material resources for obtaining the network resources or damaging the system.

Definition 4: Defense Benefit DB includes direct benefit and indirect benefit. Direct benefit refers to the reward of security strengthen by the defender's safety countermeasures for repairing the vulnerability of network resource. Jiang *et al.* [3] and Liu *et al.* [12] only consider the direct benefit. We further provide supplements of indirect benefit. It is the reward of defender gaining through collecting the evidences of attack such as attacker's pattern, sequence, scale and path. For example, the port scanning time, port number, source IP address, and destination IP address can be used to track and locate the source of the attacker. These measures can bring indirect benefits to defenders and increase the difficulty of subsequent attacks, which can deter potential attackers.

Definition 5: Defense Cost DC is the cost that defenders spend on strengthen the vulnerability of the system. It includes human and time costs on investment in security devices, and resources loss cost on affecting the normal operation of the service.

Definition 6: Attack-defense payoff matrix M_k indicates the payoff values of attacker and defender, in which a_{kij} and d_{kij} respectively represent attacker's and defender's payoff when the strategies are (A_i, D_j) and the attacker type is t_k, where $\forall k = 1, \cdots, \lambda, i = 1, \cdots, n, j = 1, \cdots, m$.

$$M_k = \begin{bmatrix} a_{k11}, d_{k11} & a_{k12}, d_{k12} & \cdots & a_{k1m}, d_{k1m} \\ a_{k21}, d_{k21} & a_{k22}, d_{k22} & \cdots & a_{k2m}, d_{k2m} \\ \cdots & \cdots & \ddots & \cdots \\ a_{kn1}, d_{kn1} & a_{kn2}, d_{kn2} & \cdots & a_{knm}, d_{knm} \end{bmatrix}$$

D. EVOLUTIONARY STABLE EQUILIBRIUM

Based on the attack-defense evolutionary game model proposed in Section III-A, this section first gives the concept of attack-defense evolutionary stable strategy, and then analyzes how to use the dynamic evolutionary equation to calculate the evolutionary stable equilibrium. Finally, we design the optimal defense strategy selection algorithm based on evolutionary stable equilibrium.

Evolutionary Stable Strategy (ESS) [30] is the optimal strategy for the game system formed during the long-term strategy evolution. The strategy is balanced and stable, which is able to resist the intrusion of other strategies. The definition of network attack-defense evolutionary stable strategy is as follows.

Definition 7: For any attacker population with type t_k, the attacker population randomly selects the strategy space $S_A^k = (A_1, A_2, \cdots, A_n)$ with probability $P = (p_{k1}, p_{k2}, \cdots, p_{kn})$. Meanwhile, the defender population randomly selects the strategy space $S_D = (D_1, D_2, \cdots, D_m)$ with probability $Q = (q_1, q_2, \cdots, q_m)$. It indicates that individual player in the attacker population and defender population randomly select and implement the pure strategy with probability distributions P and Q in the actual game process respectively. We take strategy $\sigma^* = (P, Q)$ as the attack-defense evolutionary stable strategy. For any $\sigma \neq \sigma^*$, $U(\sigma^*, \sigma^*)$ indicates the payoff when the players in the populations of attacker and the defender choose the co-strategy σ^*. $U(\sigma^*, \sigma)$ indicates the payoff when there is a mutation of natural selection for some players. The above definition follows when the following conditions are met:

i. (equilibrium) $U(\sigma^*, \sigma^*) \geq U(\sigma, \sigma^*)$

ii. (stability) $U(\sigma^*, \sigma^*) = U(\sigma, \sigma^*) \Rightarrow U(\sigma^*, \sigma) > U(\sigma, \sigma)$

The first condition guarantees that σ^* is the Nash equilibrium strategy. It means attackers' or defenders' unilateral change of the strategy will not be profitable. When σ is mostly consist of σ^* and contains a few other strategies, it satisfies that σ^* is the optimal response, otherwise other strategies have the possibility of invasion and development. The second condition guarantees that if there exist the other optimal response σ, then it requires that when facing σ, σ^* is better. It also guarantees if there is a mutation of strategy to σ, σ is impossible to further develop.

The mechanism depicted in Definition 7 indicates that in any attack-defense game evolutionary model, if most players in the population select the stable strategy, then a small number of strategy mutants in the population will not affect the entire population. The attack-defense system will keep in the state of evolutionary stable equilibrium. Unless there is

a higher-payoff strategy, the system will not deviate from the current stable state and will remain in that state. Therefore, the evolutionary stable attack-defense strategy has stronger predictability and robustness ability.

The above definition directly gives the condition of whether the strategy evolves but does not depict the track of selecting the strategy ultimately. In the adversarial process of network attack-defense in the reality, the rational degree of players is relatively low since that attackers and defenders do not have common understanding of each other's payoffs. The learning speed of information security strategy and dynamic adjustment ability is not fast, so this paper depicts the track of attack-defense strategies by improving replicator dynamic equation [28] with randomness, which describes the uncertainty characteristic of biological evolution. We define it as the stochastic replicator dynamic:

Definition 8: Stochastic replicator dynamic differential equations

$$\frac{dp}{dt} = \omega p\left(U(S) - \overline{U}\right)$$

The formula shows that the change rate of the population proportion of player adopting strategy S in the entire population dp/dt is directly proportional to the proportion of player selecting this strategy. Moreover, it is also directly proportional to the range of the expected payoff over the average payoff $(U(S) - \overline{U})$.

The conventional replicator dynamic equation adopts a deterministic dynamics to update the evolution, and the individual learns from the individual behavior of the population of highest-payoff with the probability 1. Considering that in the actual attack-defense game process, individual gain different payoffs when referring to different a strategy, this causes the randomness of the strategy learning. Based on this consideration, we add the randomness of referring payoff to the original replicator dynamic equation. We describe the noise effect by bringing in the selecting intensity factor ω, $0 \le \omega \le 1$. The ω is assigned according to the player's historical data of selection. In detail, $\omega = 1$ represents the strong selection and $\omega \ll 1$ represents the weak selection. It means that some low-rational players in the population are allowed to select irrational strategies. In other words, the low-payoff strategy still has a small probability of being adopted by high-payoff individuals in natural selection. We think the improved replicator dynamic equation is more general and is more consistent with the reality.

From Definition 8, we can see that most bounded rationality players in the population will gradually undertake the strategy that have higher payoff than the average payoff, and give up the irrational low-payoff strategy. Therefore, the population proportion of the players adopting this strategy will change dynamically.

In order to construct the stochastic replicator dynamic equation over the proposed model, we first define the parameters, p_{ki} is the population proportion of the attack players (with type t_k) adopting strategy A_i, $\forall t_k$, $\sum_{i=1}^{n} p_{ki} = 1$, where $1 \le k \le \lambda$, $1 \le i \le n$. q_j indicates the population proportion of the defense players adopting the defense strategy D_j, where $\sum_{j=1}^{m} q_j = 1$, $1 \le j \le m$. We define the probability vectors $(p_{k1}, p_{k2}, \cdots, p_{kn})$ and $(q_1, q_2, \cdots, q_m)$ respectively represent the mixed strategies of the attacker (with type t_k) and the defender. We also set the defense payoff as U_{D_j} when selecting strategy D_j and the average defense payoff as $\overline{U}_D$. The attack payoff is U_{A_I} when selecting strategy A_i and the average payoff for attacker type t_k is $\overline{U}_{t_k}$.

(1) Stochastic replicator dynamic equation of defense strategy

The defender analyzes the prior probability distribution of attacker's types $P = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_\lambda)$ combining with the current defense situation. Since defenders have only one type t, the probability of the type of attacker inferred by the defender can be calculated by the following Bayesian formula.

$$Prob(t_k|t) = \frac{Prob(t_k, t)}{Prob(t)} = \varepsilon_k$$

Further, the expected payoff U_{D_j} of selecting different kind of defense strategy D_j for the defender is as follows:

$$\begin{cases} U_{D_1} = \varepsilon_1 \left(p_{11}d_{111} + p_{12}d_{121} + \cdots + p_{1n}d_{1n1}\right) + \cdots \\ \qquad + \varepsilon_\lambda \left(p_{\lambda 1}d_{\lambda 11} + p_{\lambda 2}d_{\lambda 21} + \cdots + p_{\lambda n}d_{\lambda n1}\right) \\ U_{D_2} = \varepsilon_1 \left(p_{11}d_{112} + p_{12}d_{122} + \cdots + p_{1n}d_{1n2}\right) + \cdots \\ \qquad + \varepsilon_\lambda \left(p_{\lambda 1}d_{\lambda 12} + p_{\lambda 2}d_{\lambda 22} + \cdots + p_{\lambda n}d_{\lambda n2}\right) \\ U_{D_j} = \varepsilon_1 \left(p_{11}d_{11j} + p_{12}d_{12j} + \cdots + p_{1n}d_{1nj}\right) + \cdots \\ \qquad + \varepsilon_\lambda \left(p_{\lambda 1}d_{\lambda 12} + p_{\lambda 2}d_{\lambda 2j} + \cdots + p_{\lambda n}d_{\lambda nj}\right) \\ \qquad = \sum_{k=1}^{\lambda}\left[\varepsilon_k \sum_{i=1}^{n}\left(p_{ki}d_{kij}\right)\right] \\ \cdots \\ U_{D_m} = \varepsilon_1 \left(p_{11}d_{11m} + p_{12}d_{12m} + \cdots + p_{1n}d_{1nm}\right) + \cdots \\ \qquad + \varepsilon_\lambda \left(p_{\lambda 1}d_{\lambda 1m} + p_{\lambda 2}d_{\lambda 2m} + \cdots + p_{\lambda n}d_{\lambda nm}\right) \end{cases}$$

Then, the average defense payoff is as follows:

$$\begin{aligned} \overline{U}_D &= q_1 U_{D_1} + q_2 U_{D_2} + \cdots + q_m U_{D_m} \\ &= \sum_{j=1}^{m}\left[q_j \sum_{k=1}^{\lambda}\left(\varepsilon_k \sum_{i=1}^{n}\left(p_{ki}d_{kij}\right)\right)\right] \end{aligned}$$

The change rate of the population proportion of selecting strategy D_j in the defender population varies with time is $\frac{dq_j}{dt}$. It reflects defender's learning and adjusting process of selecting strategy D_j through repeated games. Hence, the differential equation describing the change rate of selecting D_j is as follows:

$$\begin{aligned} \frac{dq_j}{dt} &= \omega q_j (U_{D_j} - \overline{U}_D) \\ &= q_j \left[\sum_{k=1}^{\lambda}\left(\varepsilon_k \sum_{i=1}^{n}\left(p_{ki} \times d_{kij}\right)\right)\right. \\ &\qquad \left. - \sum_{j=1}^{m}\left(q_j \sum_{k=1}^{\lambda}\left(\varepsilon_k \sum_{i=1}^{n}\left(p_{ki}d_{kij}\right)\right)\right)\right] \end{aligned}$$

(2) Stochastic replicator dynamic equation of attack strategy (with type t_k)

The expected payoff U_{A_i} of an attacker choosing a different attack strategy A_i is as follows:

$$\begin{cases} U_{A_1} = q_1 a_{k11} + q_2 a_{k12} + \cdots + q_m a_{k1m} \\ U_{A_2} = q_1 a_{k21} + q_2 a_{k22} + \cdots + q_m a_{k2m} \\ U_{A_i} = q_1 a_{ki1} + q_2 a_{ki2} + \cdots + q_m a_{kim} = \sum_{j=1}^{m} q_j a_{kij} \\ \cdots \\ U_{A_n} = q_1 a_{kn1} + q_2 a_{kn2} + \cdots + q_m a_{knm} \end{cases}$$

Then, we can get the average attack payoff is as follows:

$$\begin{aligned} \overline{U}_{t_k} &= p_{k1} U_{A_1} + p_{k2} U_{A_2} + \cdots + p_{kn} U_{A_n} \\ &= \sum_{i=1}^{n} \left(p_{ki} \sum_{j=1}^{m} (q_j a_{kij}) \right) \end{aligned}$$

For the attacker population with type t_k, the change rate over time of the game proportion of strategy selection A_i is $\frac{dp_{ki}}{dt}$. It depicts attacker's process of learning and improving strategy A_i after repeated games. The differential equation describing the change speed with time for strategy A_i is as follows:

$$\begin{aligned} \frac{dp_{ki}}{dt} &= \omega p_{ki} (U_{A_i} - \overline{U}_{t_k}) \\ &= \omega p_{ki} \left(\sum_{j=1}^{m} q_j a_{1ij} - \sum_{i=1}^{n} \left(p_{ki} \sum_{j=1}^{m} (q_j a_{kij}) \right) \right) \end{aligned}$$

The practical significance of the replicator dynamic equations for the attack-defense strategies are that: We take the defense strategy D_j as an example, if the individual defender player who chooses a pure strategy D_j gains the payoff U_{D_j}, which is less than the average payoff $\overline{U}_D$ of the defender population. Then the growth rate of the population proportion of defenders who select the strategy D_j is less than 0. On the contrary, if the individual player choosing a pure strategy D_j gains the payoff U_{D_j}, which is over the average payoff $\overline{U}_D$, then we can predict that the growth rate of the defenders selecting the strategy D_j is more than 0. In another case, if the individual payoff is exactly equal to the average payoff of the population, then the growth rate of selecting the strategy D_j is equal to 0.

Assign $F(p) = \frac{dp_{ki}}{dt}$, $G(q) = \frac{dq_j}{dt}$. By calculating the results of $Y(p, q) = \begin{bmatrix} F(p) \\ G(q) \end{bmatrix} = \begin{bmatrix} \frac{dp_{ki}}{dt} \\ \frac{dq_j}{dt} \end{bmatrix} = 0$, the evolutionary stable equilibrium of the network attack-defense game decisions is obtained from the solution.

IV. OPTIMAL DEFENSE STRATEGY SELECTION ALGORITHM

Based on the attack-defense evolutionary game model proposed in section III, we construct the stochastic replicator

Algorithm 1 Optimal Defense Strategy Selection Algorithm for Network Attack-Defense Game

Input Network information NetInf, Configuration information of device SafetyInf, Intrusion alert data information AlertInf

Output Optimal defense strategy Q

BEGIN

1) **Initialize** AIEGM $= (N, T, E, S, U)$

// Initialize attack-defense evolutionary game model

{

1-1) **Construct** $T_A = \{t_k\}, T_D = \{t\}, 1 \le k \le \lambda$

// According to the information of historical security events and NetInf, we construct the attacker type space

1-2) **Construct** $E_A = \{\varepsilon_k\}, E_D = \{\varepsilon\}, 0 \le \varepsilon_k \le 1$

// Analyze the probability distribution of attacker type space based on the historical security events

1-3) **Construct** $S_A = \{A_i\}, 1 \le i \le n$

// By analyzing security devices' configuration information SafetyInf and collecting defense strategy, we construct the space of attack strategy using [31]

1-4) **Construct** $S_A = \{D_j\}, 1 \le j \le m$

// By collecting real-time alert data AlertInf and analyzing characteristics of attack behavior, we construct defense strategy space using [31]

1-5) **Construct** $P_k = \{p_{ki}\}, \forall k, \exists 0 \le p_{ki} \le 1, \sum_{i=1}^{n} p_{ki} = 1$

// Construct the attack strategy selection vector P, in which the attacker of the type t_k selects attack strategy A_i with the probability $p_{ki} \in P$

1-6) **Construct** $Q = \{q_j\}, 0 \le q_j \le 1, \sum_{j=1}^{m} q_j = 1$

// Construct the defense strategy selection vector Q, in which the defender selects the defense strategy D_j with the probability $q_j \in Q$

}

2) **Calculate** $Prob(t_k|t)$

// Calculate the priori probability of the attacker typet_k from the view of the defender

3) **Set** $\omega, 0 \le \omega \le 1$

// Set the selecting intensity factor according to the player's historical selections

For $(k = 1; k \le \lambda; k++)$

For $(i = 1; i \le n; i++)$

For $(j = 1; j \le m; j++)$

{

4) **Calculate** $\begin{cases} a_{kij} = AB(t_k, A_i, D_j) - AC(t_k, A_i, D_j) \\ d_{kij} = DB(t_k, A_i, D_j) - DC(t_k, A_i, D_j) \end{cases}$

// By traversing each attacker type, we calculate the attack payoff and the defense payoff under different strategies combinations using [3].

}

For $(k = 1; k \le \lambda; k++)$

{

Algorithm 1 *(Continued.)* Optimal Defense Strategy Selection Algorithm for Network Attack-Defense Game

5) **Construct**

$$F(P_k) = \omega p_{ki}\left(\sum_{j=1}^{m} q_j a_{kij} - \sum_{i=1}^{n}\left(p_{ki}\sum_{j=1}^{m}\left(q_j a_{kij}\right)\right)\right)$$

// Construct the stochastic replicator dynamic equation for each strategy of attacker with type t_k

}

6) **Construct**

$$G(q) = \omega q_j\left[\sum_{k=1}^{\lambda}\left(\varepsilon_k\sum_{i=1}^{n}\left(p_{ki}\times d_{kij}\right)\right) - \sum_{j=1}^{m}\left(q_j\sum_{k=1}^{\lambda}\left(\varepsilon_k\sum_{i=1}^{n}\left(p_{ki}d_{kij}\right)\right)\right)\right]$$

// Construct the stochastic replicator dynamic equation for each strategy of defender

7) **Calculate** $Y = \begin{bmatrix} F(p) \\ G(q) \end{bmatrix} = 0$

// Calculate the evolutionary stable equilibrium

8) **Output** $Q = \{q_1, q_2, \cdots, q_m\}$

// Output the optimal defense strategies

END

dynamic equations of both the attacker and defender. By calculating the evolutionary stable equilibrium, the optimal selection algorithm of defense strategy is given as follows.

The time cost of the above algorithm focuses on step 4) and step 7). The step 4) traverses each element in the $n \times m$ payoff matrix of λ attacker types in turn, the number of operations is $O(\lambda mn)$, the computation complexity of solving the equations in the equation of step 7) is $O(\lambda\,(m+n)^3)$. The total complexity of the algorithm is $O(\lambda\,(m+n)^3)$. The storage cost of the algorithm focuses on the storage of payoff matrix and the middle vector of the equilibrium calculating. The storage of payoff matrix has higher complexity. It contains a total number of nm storage units. Therefore, the storage complexity is $O(nm)$.

V. EXPERIMENTS AND ANALYSES

This section takes the intrusion and proactive defense in the realistic network system as the example to verify the proposed attack-defense evolutionary game model and the corresponding equilibrium calculation method. Based on this, we summarize the general rules of strategy evolution. Furthermore, in order to analyze the impact of strategy payoff on strategy selection, the numerical experiments in two cases (considering/without considering the defense indirect benefits) are compared and analyzed. In the end, a comprehensive comparison among this paper and existing works is provided.

A. EXPERIMENTAL ENVIRONMENT

The structure of experimental network system is shown in Fig. 1, where the network security devices are consist of firewall, intrusion prevention system IPS and virus detection system VDS. The firewall forbids external host access the

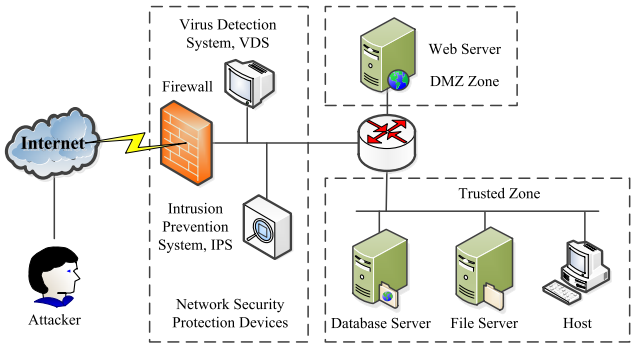

FIGURE 1. The architecture of experiment network system.

servers and hosts in the trusted zone. External host can only use the HTTP protocol (port 80) to communicate with the web server in the DMZ Zone. Meanwhile, the web server can communicate with the servers in the Trusted Zone and the servers in the Trusted Zone receive the service requests passively.

B. PAYOFF QUANTIFICATION

First, we initialize the parameters of the proposed model by using step 1) of Algorithm 1. For simplicity of analysis and discussion, we only consider with 2 by 2 games including two kinds of basic attack and defense strategies. When encountering other types of game structures, the calculation procedure and analysis method are similar.

There are two basic defense strategies 'D_1 = patch upgrade' and 'D_2 = service close'. Intrusion prevention system IPS and virus detection system VDS detect system vulnerabilities as well as download and install the new patch resources in the real time. Operated by the security administrator, the firewall can close the service.

Through real-time alerts generated by the running firewall, IPS, VDS and host security audit log, we preprocessed the alert data firstly. After correlating and analyzing the data, we obtain the information of attack behavior. According to the characteristics of attack behaviors [31], we get two basic attack strategies 'A_1 = DoS' and 'A_2 = Sniffer'.

DoS attacks can undertake reasonable service requests to overcommit service resources, leading legal users cannot get normal services. In essence, it is a proactive attack. Sniffer attacks include the scanning of ports, addresses, vulnerability, etc. The purpose is to collect information rather than to access it. It also will not affect the normal access of legal users and is a passive attack difficult to be found. According to the defender's historical experience, the attacker has two types 't_1 = adventure' and 't_2 = conservative'.

Based on the history experiences of defense, we can divide the attack types into 't_1 = adventure' and 't_2 = conservative', and the payoff matrices are

$$M_1 = \begin{bmatrix} a_{111}, d_{111} & a_{112}, d_{112} \\ a_{121}, d_{121} & a_{122}, d_{122} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} a_{211}, d_{211} & a_{212}, d_{212} \\ a_{221}, d_{221} & a_{222}, d_{222} \end{bmatrix}$$

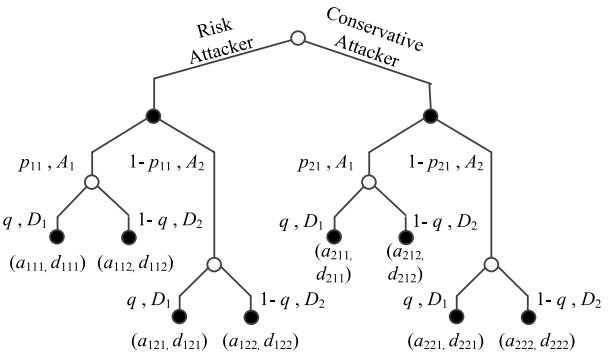

FIGURE 2. The game tree of experiment network.

The payoff matrices of different strategy combinations can be illustrated using the game tree in Fig. 2.

C. EQUILIBRIUM CALCULATION AND DEFENSE STRATEGY SELECTION

According to step 1-5) and step 1-6) of Algorithm 1, when the attack type is 't_1 = risk', the population proportion of players selecting the strategy 'A_1 = DoS' is $p_{11}(0 \le p_{11} \le 1)$. Meanwhile, the proportion of players selecting the strategy 'A_2 = Sniffer' is $p_{12} = 1 - p_{11}$. When the attack type is 't_2 = conservative', the proportion of game players selecting the strategy 'A_1 = DoS' is $p_{21}(0 \le p_{21} \le 1)$ and the player proportion of selecting the strategy 'A_2 = Sniffer' is $p_{22} = 1 - p_{21}$. The proportion of players in the defense population selecting the strategy 'D_1 = patch upgrade' is $q(0 \le q \le 1)$. Meanwhile, the proportion of game players selecting the strategy 'D_2 =service close' is $1 - q$. According to the statistics of historical data, the proportion of risk attackers is ε. Meanwhile, According to step 1-2) of Algorithm 1, the proportion of the conservative attacker is set as $1 - \varepsilon$. According to step 3) of Algorithm 1, we set the selecting intensity factor ω according to the players' security knowledge. Next, we show how to construct the stochastic replicator dynamic equations of attack-defense strategies.

1) RISK ATTACK STRATEGIES EVOLUTION EQUATION

According to step 5) of Algorithm 1, we get the differential equation of risk attacker's decision evolution is

$$\begin{aligned}\frac{dp_{11}}{dt} &= \omega p_{11}(U_{\text{DoS}} - \overline{U}_{t_1}) \\ &= \omega p_{11}(1 - p_{11})\,(q(a_{111} + a_{122} - a_{121} - a_{112}) \\ &\qquad + a_{112} - a_{122})\,.\end{aligned}$$

2) CONSERVATIVE ATTACK STRATEGIES EVOLUTION EQUATION

According to step 5) of Algorithm 1, we can get the differential equation of risk attacker's strategy evolution

$$\begin{aligned}\frac{dp_{21}}{dt} &= \omega p_{21}(U_{\text{DoS}} - \overline{U}_{t_2}) \\ &= \omega p_{21}(1 - p_{21})\,(q(a_{211} + a_{222} - a_{221} - a_{212}) \\ &\qquad + a_{212} - a_{222})\,.\end{aligned}$$

3) DEFENSE STRATEGIES EVOLUTION EQUATION

According to step 6) of Algorithm 1, we get the differential equation of defense strategy evolution is as follows:

$$\begin{aligned}\frac{dq}{dt} &= \omega q(U_{\text{Patch}} - \overline{U}_D) \\ &= \omega q(1 - q)(\varepsilon p_{11}(d_{111} + d_{122} - d_{112} - d_{121}) \\ &\quad + (1 - \varepsilon)p_{21}(d_{211} + d_{222} - d_{212} - d_{221}) \\ &\quad + \varepsilon\,(d_{121} + d_{222} - d_{122} - d_{221}) + d_{221} - d_{222}).\end{aligned}$$

Based on the above analysis, According to step 7) of Algorithm 1, we set the right-hand side of the above equations as 0.

$$\begin{aligned}&\{\omega p_{11}(1 - p_{11})\,(q(a_{111} + a_{122} - a_{121} - a_{112}) \\ &\qquad + a_{112} - a_{122}) = 0 \\ &\{\omega p_{21}(1 - p_{21})\,(q(a_{211} + a_{222} - a_{221} - a_{212}) \\ &\qquad + a_{212} - a_{222}) = 0 \\ &\begin{cases}\omega q(1 - q)(\varepsilon p_{11}(d_{111} + d_{122} - d_{112} - d_{121}) \\ +(1 - \varepsilon)p_{21}(d_{211} + d_{222} - d_{212} - d_{221}) \\ +\varepsilon(d_{121} + d_{222} - d_{122} - d_{221}) + d_{221} - d_{222}) = 0\end{cases}\end{aligned}$$

According to step 8) of Algorithm 1, The solution of the above equations is the attack-defense evolutionary stable equilibrium for decision-making. The defender's optimal defense strategy is randomly selecting strategies 'patch upgrade' and 'service close' with the probability q and $1 - q$ respectively.

D. RESULTS ANALYSES

In the following, numerical experiments were conducted using two cases: *Case 1* (including defense indirect benefits) and *Case 2* (excluding defense indirect benefits). The *Case 1* considers the benefit of defense counterattack while the *Case 2* does not consider. In addition, we make a comprehensive comparison and analysis.

(1) Case 1:

According to Definition 2 - Definition 5 in Section III-C, combined with the quantitative methods of payoff [3], we can get attack-defense payoffs of case 1 as shown in Table 1.

TABLE 1. Game payoff values of case 1.

Attacker		Defender	
		Patch Upgrade	Service close
Risk Type	DoS	$a_{111} = 50,\ d_{111} = 30$	$a_{112} = -40,\ d_{112} = 0$
	Sniffer	$a_{121} = 30,\ d_{121} = 10$	$a_{122} = -20,\ d_{122} = 0$
Conservative Type	DoS	$a_{211} = 20,\ d_{211} = 40$	$a_{212} = -10,\ d_{212} = 0$
	Sniffer	$a_{221} = 40,\ d_{221} = 20$	$a_{222} = -30,\ d_{222} = 0$

We take the strategy combination 't_1 = risk', 'A_1 = DoS'and 'D_1 = patch upgrade' as an example. The payoff calculation process is as follows.

1) The privilege obtained by attack is divided into three levels, namely, Remote privilege, User privilege and

Root privilege. The corresponding attack benefits AB are measured using 30, 50 and 100 respectively. The DoS attack obtains the root privilege of the system resource and therefore the attack benefit $AB = 100$. The human, time and resource costs of attack have 3 levels, namely, high, medium and low, which can be respectively measured using 50, 30 and 10. The DoS attacks need to use large number of puppets and have the features like long duration, high bandwidth traffic, and therefore the attack cost $AC = 50$. According to step 4) of Algorithm 1, the attack payoff is $AB - AC = 100 - 50 = 50$.

2) The direct benefit of defense results from the strengthen promotion of security. We divide it into three levels, namely high, medium and low, with the value of 100, 50 and 30. Meanwhile, the indirect value of security deterrence is measured using 30, 20 and 10. Among which, the benefit of 'patch upgrade' is 50, the indirect benefit of security deterrence is 10, so the total defense benefit is $DB = 50 + 10 = 60$. Defense costs include the consumption of time, human and resource for patch download, transmission and installation, so that defense cost $DC = 30$. According to step 4) of Algorithm 1, the defense payoff is $DB - DC = 60 - 30 = 30$.

Because the implementation of attack is illegal and has potential risks. The number of risk attackers in the real world is obviously less than the number of conservative attackers. The historical statistics show that the population proportion of risk attacker is $\varepsilon = 1/4$ and that of conservative attackers is $1 - \varepsilon = 3/4$.

The assignment of attack-defense stochastic replicator dynamic equations in section V-C is as follows:

$$\begin{cases} F(p_{11}) = \omega p_{11}(1 - p_{11})\,(40q - 20) = 0 \\ F(p_{21}) = \omega p_{21}(1 - p_{21})\,(20 - 40q) = 0 \\ G(q) = \omega q(1 - q)(20\varepsilon p_{11} + 20(1 - \varepsilon)p_{21} \\ \qquad\qquad +20 - 10\varepsilon) = 0 \end{cases}$$

We get 12 equilibrium solutions in the game system for the experimental network, in which $p_{11} = 0, p_{21} = -7/6$, $q = 1/2$, $p_{11} = 1, p_{21} = -3/2, q = 1/2$, $p_{11} = -7/2, p_{21} = 0, q = 1/2$, $p_{11} = -13/2, p_{21} = 1, q = 1/2$ do not meet the probability range requirement, so that we exclude them.

Moreover, the evolutionary stable strategy needs to satisfy the following conditions [28], namely, the growth rate of strategy evolution should not exceed 0. We analyze the local stability of the game system in Table 2.

$$\begin{cases} \dfrac{dF(p_{11})}{dp_{11}} = (1 - 2p_{11})(40q - 20) \le 0 \\ \dfrac{dF(p_{21})}{dp_{21}} = (1 - 2p_{21})(20 - 40q) \le 0 \\ \dfrac{dG(q)}{dq} = (1 - 2q)(5p_{11} + 15p_{21} + 17.5) \le 0 \end{cases}$$

According to the result in Table 2, we can get the evolutionary stable equilibrium point $p_{11} = 1, p_{21} = 0, q = 1$. We set the strategy of game system at initial moment as $p_{11} = 0.9, p_{21} = 0.9, q = 0.9, p_{11} = 0.1, p_{21} = 0.1, q = 0.1$ and $p_{11} = 0.1, p_{21} = 0.9, q = 0.1$ respectively. Setting $\varepsilon = 1/4$, $\omega = 1$ and Using Matlab2017 to simulate, we can get the phase cures of the system in Fig. 3. The evolutionary track of the risk attacker's strategy is shown in Fig. 4. Fig. 5 shows the evolutionary track of the conservative attacker's strategy.

TABLE 2. Equilibrium determination of attack-defense game system.

Equilibrium solution	Calculation
$p_{11}=0,\ p_{21}=0,\ q=0$	$F'(p_{11})<0, F'(p_{21})>0. G'(q)>0$
$p_{11}=0,\ p_{21}=0,\ q=1$	$F'(p_{11})>0, F'(p_{21})<0. G'(q)<0$
$p_{11}=0,\ p_{21}=1,\ q=0$	$F'(p_{11})<0, F'(p_{21})<0. G'(q)>0$
$p_{11}=0,\ p_{21}=1,\ q=1$	$F'(p_{11})>0, F'(p_{21})>0. G'(q)<0$
$p_{11}=1,\ p_{21}=0,\ q=0$	$F'(p_{11})>0, F'(p_{21})>0. G'(q)>0$
$p_{11}=1,\ p_{21}=0,\ q=1$	$F'(p_{11})<0, F'(p_{21})<0. G'(q)<0$
$p_{11}=1,\ p_{21}=1,\ q=0$	$F'(p_{11})>0, F'(p_{21})<0. G'(q)>0$
$p_{11}=1,\ p_{21}=1,\ q=1$	$F'(p_{11})<0, F'(p_{21})>0. G'(q)<0$

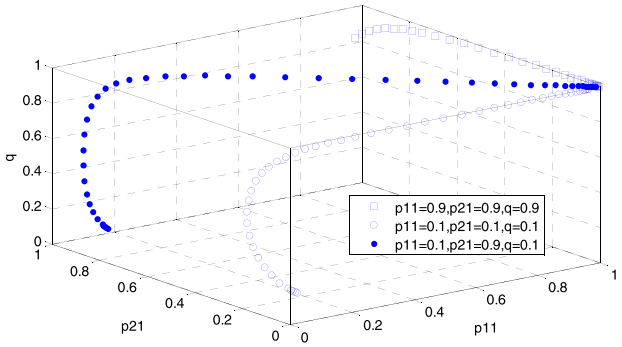

FIGURE 3. Phase diagram of attack-defense game evolutionary system when $\varepsilon = 1/4, \omega = 1$.

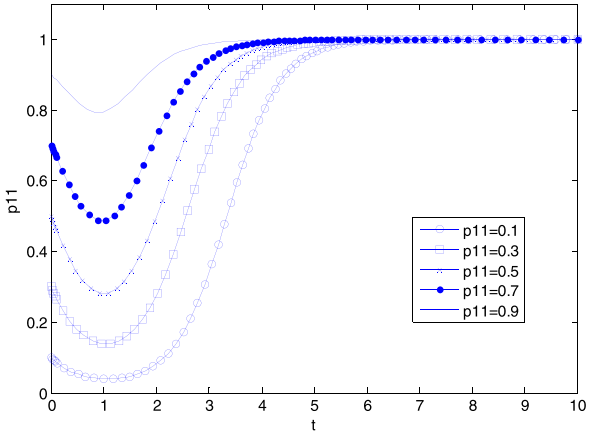

FIGURE 4. The evolutionary track of the risk attacker's strategy 'DoS' varies with time when $\varepsilon = 1/4, \omega = 1, p_{21} = 0.1, q = 0.1, p_{11} = 0.1, 0.3, 0.5, 0.7, 0.9$.

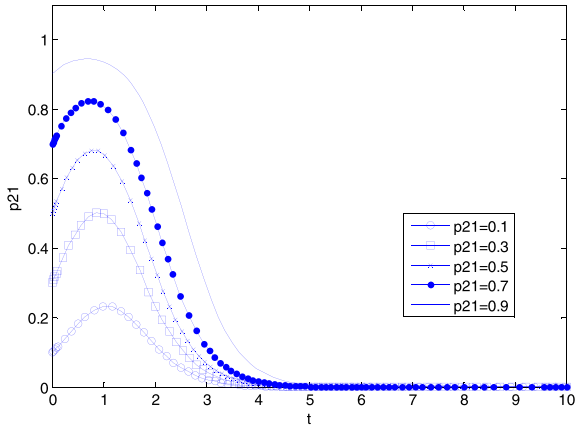

FIGURE 5. The evolutionary track of the conservative attacker's strategy 'DoS' varies with time when $\varepsilon = 1/4$, $\omega = 1$, $p_{11} = 0.1$, $q = 0.1$, $p_{21} = 0.1$, 0.3, 0.5, 0.7, 0.9.

Fig. 6 shows the evolutionary track of defender's strategy. The abscissa represents the evolutionary times of game system, and the ordinate represents the probability result of strategy selection. We will discuss them separately as below.

1) As can be seen from Fig. 3, the system will evolve to an equilibrium point in the end. We take $p_{11} = 0.9$, $p_{21} = 0.9, q = 0.9$ as an example. At the initial time, the population proportions of risk attacker and conservative attacker selecting 'DoS' attack strategy are both 0.9, the proportion of defenders selecting the strategy of 'patch upgrade' is 0.9. After continuous strategy learning and improving, the game system finally evolves to a stable equilibrium point (1, 0, 1), namely, the population of risk attackers undertakes the 'DoS' strategy while the population of risk attackers undertakes the 'Sniffer' strategy, and the optimal defense strategy of the defender population is 'patch upgrade'. The result is consistent with the fact that risk attackers are more likely to choose proactive and profitable 'DoS' attack, while conservative attackers prefer passive and moderate 'sniffer' attack. The defenders select pure strategy of 'patch upgrade', which will increase the attacker's difficulty of invasion and improve the defender's own payoff.

2) As shown in Fig. 4, we set $p_{21} = 0.1, q = 0.1$ at the initial time of system. It means that the conservative attacker randomly select pure strategy {DoS, Sniffer} with the mixed probability $\{p_{21} = 0.1, 1 - p_{21} = 0.9\}$ and the defender randomly choose strategy {patch upgrade, service close} with the mixed probabilities $\{q = 0.1, 1 - q = 0.9\}$. The tracks of risk attackers randomly choose strategy 'DoS' with different initial probabilities $p_{11} = 0.1, 0.3, 0.5, 0.7, 0.9$ are shown in Fig. 4. After strategy learning and improvement, the risk attacker of bounded rationality will finally select pure strategy 'DoS' with the probability 1. Moreover, this selection has a constant stability. It also can be seen that in the initial stage of the evolution, some players in the population try other strategies, so the population proportion choosing strategy 'DoS' decreases when $t < 1$. However, through continuous strategy adjustment, the population proportion choosing strategy 'DoS' turns to rise until it reaches 1 when $t > 1$. The results show that even if there are a few of mutants change to select 'Sniffer', because the payoff of mutants is less than the average payoff of the whole population, they will eventually give up the irrational selection 'Sniffer'. To sum up, the optimal defense strategy of ESS regarding network attack-defense proposed in this paper has the strong predictive ability and robustness capability as expected.

3) As shown in Fig. 5, we set $p_{11} = 0.1, q = 0.1$ at the initial time of system. It means that the risk attacker randomly choose a pure strategy from {DoS, Sniffer} with the mixed probabilities {0.1, 0.9} and the defender randomly choose a pure strategy from {patch upgrade, service close} with the mixed probabilities {0.1, 0.9}. The evolutionary track that risk attackers randomly choose 'DoS' with different initial probabilities $p_{11} = 0.1, 0.3, 0.5, 0.7, 0.9$ is shown in Fig. 5. This shows that after strategy learning and improvement, the risk attacker of bounded rationality will finally choose pure strategy 'Sniffer' with the probability 1. It can be seen that since some mutants try other strategies in the population of risk attacker, the proportion of population choosing strategy 'DoS' is increasing when $t < 1$. However, through continuous learning and improving, the proportion continues to decrease until it reaches 0 when $t > 1$. This indicates that players in the population of conservative attacker all select pure strategy 'Sniffer' finally, and the irrational strategy selection 'DoS' cannot develop further. Above results verify that the proposed attack-defense evolutionary game model can dynamically depict the track of strategy selection.

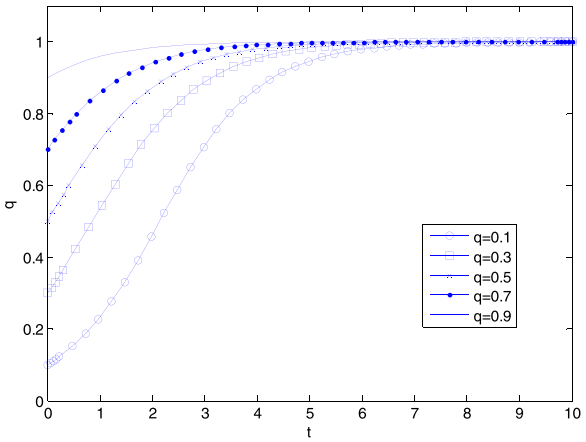

FIGURE 6. The evolutionary track of defender's strategy 'patch upgrade' varies with time when $\varepsilon = 1/4$, $\omega = 1$, $p_{21} = 0.1$, $p_{11} = 0.1$, $q = 0.1$, 0.3, 0.5, 0.7, 0.9.

4) As shown in Fig. 6, we set the initial state of the game system as $p_{11} = 0.1, p_{21} = 0.1$. It means that the initial strategies of both risk and conservative attackers are randomly selecting strategy 'DoS' with the probability 0.1. The initial defense strategy is respectively selecting the strategy 'patch upgrade' with the probability $p_{11} = 0.1$, 0.3, 0.5, 0.7, 0.9. The result of numerical simulation in Fig. 6 shows that after strategy learning and adjustment, the bounded

rationality defender will eventually select the pure strategy 'patch upgrade'. Therefore, the optimal security defense strategy is the 'patch upgrade', and this strategy has strong stability and robustness. In other words, regardless of the type of the attackers or their attack strategies, choosing the defense strategy 'patch upgrade' can make the defender compromise the defense cost and benefit.

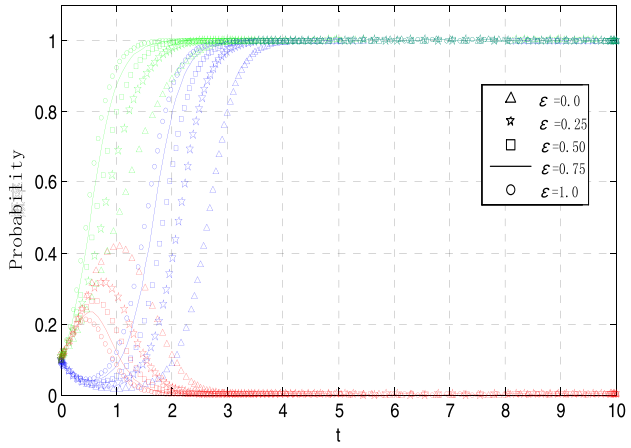

FIGURE 7. The effect of incomplete information on the evolutionary track of attack-defense strategy when $\omega = 1$, $p_{21} = 0.1$, $p_{11} = 0.1$, $q = 0.1$, $\varepsilon = 0, 0.25, 0.5, 0.75, 1$. (green = risk attacker's strategy 'DoS', red = conservative attacker's strategy 'DoS', blue = defender's strategy 'patch upgrade').

Secondly, in order to analyze the influence of probability distribution of types of the attacker on the evolution, we first consider the conventional replicator dynamics equation with deterministic selection, namely, $\omega = 1$. We set the initial state of the system as $p_{11} = 0.1, p_{21} = 0.1, q = 0.1$. For different $\varepsilon = 0, 0.25, 0.5, 0.75, 1$, we use Matlab2017 toolkit to respectively get the evolutionary tracks of strategy selection varying with time as shown in Fig. 7, where the abscissa indicates the time (reflects the number of repeated games), and the ordinate indicates the probability of selecting the strategy. The green, red and blue curves respectively represent the strategy evolutionary path of the risk attacker, conservative attacker and defender under different ε. As can be seen, the prior probability distribution of types of the attacker affects the convergence rate of the system, but does not affect the trend of the evolution. With the increasing of risk player proportion in the whole population of the attacker, the inflection point of the defense curve appears earlier and the system reaches the equilibrium quicker. Results prove that the proposed strategy selecting approach helps the defender make a prompt decision.

Finally, in order to analyze the impact of stochastic selection of mutant on strategy evolution, Setting the initial state of the system as $p_{11} = 0.1, p_{21} = 0.1, q = 0.1, \varepsilon = 0.25$ and respectively setting $\omega = 0.2, \omega = 0.4, \omega = 0.6, \omega = 0.8, \omega = 1$, we get the evolutionary tracks of defenders selecting the strategy of 'patch upgrade' shown in Fig. 8. When the payoffs are the same, the bigger selection intensity indicates the more referred payoff under natural selection,

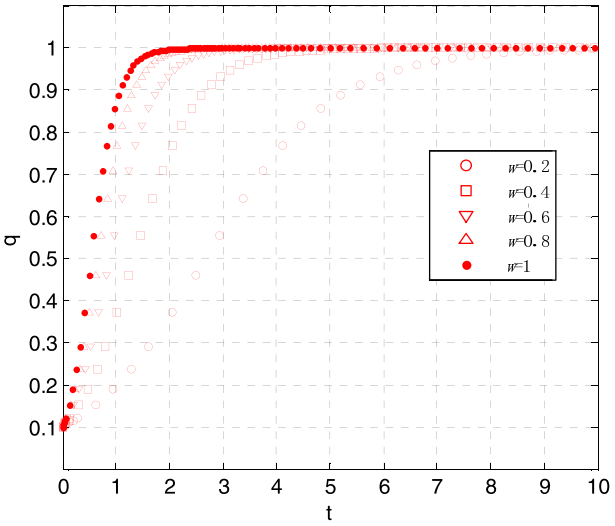

FIGURE 8. The effect of randomness on the evolutionary track of defender's strategy 'patch upgrade' when $p_{21} = 0.1$, $p_{11} = 0.1$, $q = 0.1$, $\varepsilon = 0.25$, $\omega = 0.2, 0.4, 0.6, 0.8, 1$.

then the system converges faster and the number of repeated games for reaching equilibrium is less. which is consistent with the basic law of attack-defense game. Therefore, individual player can avoid the ineffective game process by directly referring to the strategy with high-payoff, which can make the game system reach the equilibrium quicker.

(2) Case 2:

Based on the case 1, we further analyze the impact of strategy payoff change on selecting the defense strategy in case 2. Table 3 shows the payoff distribution in case 2. Compared with the Table 1 in case 1, we can see that the defense payoffs of different strategy combinations decrease because our case 2 do not consider indirect benefits of defense.

TABLE 3. Game payoff values of case 2.

Attacker		Defender	
		Patch Upgrade	Service close
Risk Type	DoS	$a_{111} = 50,\ d_{111} = 20$	$a_{112} = -40,\ d_{112} = 0$
	Sniffer	$a_{121} = 30,\ d_{121} = 0$	$a_{122} = -20,\ d_{122} = 0$
Conservative Type	DoS	$a_{211} = 20,\ d_{211} = 30$	$a_{212} = -10,\ d_{212} = 0$
	Sniffer	$a_{221} = 40,\ d_{221} = 10$	$a_{222} = -30,\ d_{222} = 0$

Similar to the above calculation process, we set the initial state of the game system as $p_{11} = 0.1, p_{21} = 0.1, \omega = 1, \varepsilon = 0.25$. After respectively setting initial $q = 0.1, 0.5, 0.9$, we obtain the evolutionary cures of case 1 and case 2 as shown in Fig. 9, where the abscissa t represents the number of game execution, and the ordinate q represents the probability of selecting the strategy 'patch upgrade' during each time of the game execution. We can derive that the defense strategy of case 1 evolves faster. The consideration of indirect benefits can affect the convergence speed of the game system. The equilibrium state of the game system is independent of its

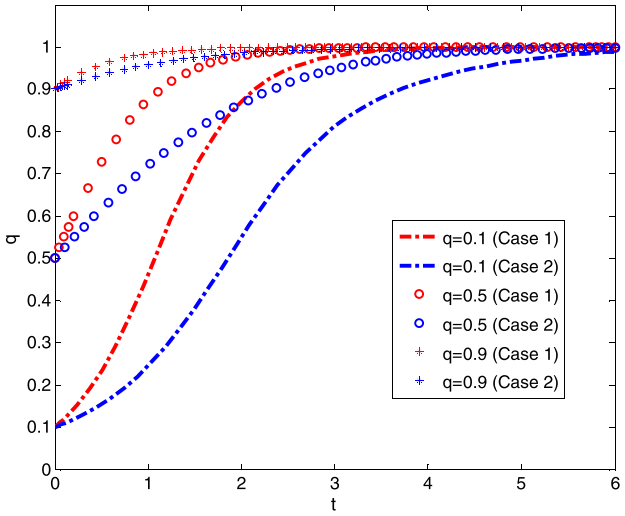

FIGURE 9. Comparisons of evolutionary curves of the defense strategy 'patch upgrade' under case 1 and case 2.

initial state. Although in both of the two cases, the probability of defender selecting 'patch upgrade' is 1. Since the case 1 considers the benefits of the counterattack, which helps to calculate the payoff accurately. The defender's countermeasures deter the underlying attacker and reduce the probability of attackers selecting radical 'DoS' strategy, which in turn encourages the defender to reach the equilibrium faster.

To sum up, combined with the experimental results of the two cases mentioned above, we can conclude that

•The attack-defense game model proposed in this paper is suitable for realistic incomplete information situations. By estimating the probability type distribution of the attacker, defenders can correctly predict the relationship between the type of attacker and its selected strategy. For defenders, the selection of defense strategy is based on its own type as well as the relationship between the type of attacker and attacker's strategy. Our approach realizes the tradeoff of maximum expected payoff of defense, which increases the scientificity and effectiveness of attack-defense decision-making.

•Based on the bounded rationality hypothesis of both attackers and defenders, this paper builds the attack-defense evolutionary game model, depicts the mechanism of strategy evolution by employing the replicator dynamic of biological evolutionary network, and considers that the game player gradually reaches the stable state by trying and keeping on exploring and interacting with other players. Numerical experimental results of Fig. 3 to Fig. 5 dynamically show the tracks of selections of the attacker and defender. The evolutionary path of the bounded rational defender shown in Fig. 5 can reflect the forming process of optimal defense strategy more scientifically and accurately. Our game model has a stronger interpret ability and the proposed optimal defense strategy has stronger robustness.

•In order to analyze the stochastic evolutionary behavior, we improve the replicator dynamic equation by adding the selecting intensity factor to objectively depict the randomness of selection. The modified replicator equation describes the strategy evolutionary mechanism of both sides of attacker and defender appropriately. We consider that the players gradually explore the evolutionary stable strategy by constantly trying under the interaction of strategy with other players. Experimental results shown in Fig. 8 indicate that when a small number of mutants refers to low-payoff strategies due to their limited ability of learning, this will not affect the trend of strategy evolution, but will affect the convergence rate of the system, namely, the system requires more repeated games to find the stable solution. Therefore, the proposed method in this paper has a preferable ability to explain the forming process of the optimal strategy and enhances the scientificity and practicability of game analysis.

•By adjusting the payoff values, it can affect the convergence speed of the game system, namely, the inflection point of evolutionary curve is different, and can guide the network security defense timely. By punishing the malicious attacker and improving the rewards of defense counterattacks, as illustrated in Fig. 9, it helps the defender make a quicker determination on selecting the optimal strategy, encourages both the attacker and defender to adopt strategies that are moderate, avoids the escalation of confrontation, and assists the security governance of network.

E. COMPARISONS AND DISCUSSIONS

The comparisons among our method and others are summarized in Table 4. We can derive.

1) In terms of information requirements, [4], [8], [15]–[17], [20], and [22] are based on the complete information hypothesis. However, because of the asymmetric information between the both sides of attacker and defender in actual network, players cannot accurately understand the opponent's payoff, which reduces the operability of existing models. Reference [10] and this paper build an attack-defense game model based on incomplete information condition. Particularly, we consider the uncertainty of the strategies and payoffs of the attacker and defender as the uncertainty of each other's type, because the type of player is closely related to its strategy payoff. Furthermore, we use Bayesian formula to calculate our belief of defender on the type of the attacker. Our method effectively enhances the practicality of the game model.

2) In terms of rationality, Li *et al.* [4], Serra *et al.* [8], and Liu *et al.* [10] assume that the attack-defense players are completely rational. The Nash equilibrium in [4] and [8] requires both attackers and defenders choose their own optimal strategies at the same time. However, the process is hard to be achieved in the reality. On the contrary, [15]–[17], [20], [22], and this paper consider that the game players are affected by the environment and their personal interests, they are bounded rational agents. The game players in network gradually find the optimal solution through strategy learning/improving mechanism under repeated game. This significantly improves the scientificity of attack-defense modeling.

TABLE 4. Performance comparisons among the proposed method and others.

type	Information	Rationality	Strategy independence	Evolution	Game type	Strategy type	Game structure	Equilibrium solution	Application	Generality
[4]	Complete	Complete	Non-cooperative	None	Static	Mixed	n	Detailed	Strategy selection	Medium
[8]	Complete	Complete	Non-cooperative	None	Static	Pure	n	Detailed	Strategy selection	Medium
[10]	Incomplete	Complete	Non-cooperative	None	Static	Pure	2	Detailed	Effectiveness assessment	Low
[15]	Complete	Bounded	Cooperative	Deterministic	Dynamic	Mixed	n	Detailed	Strategy selection	High
[16]	Complete	Bounded	Non-cooperative	Deterministic	Dynamic	Mixed	2	Simple	Security governance	Low
[17]	Complete	Bounded	Non-cooperative	Deterministic	Static	Mixed	n	Detailed	Strategy selection	Medium
[20]	Complete	Bounded	Non-cooperative and cooperative	Stochastic	Dynamic	Mixed	n	Detailed	Strategy robustness	High
[22]	Complete	Bounded	Cooperative	Deterministic	Dynamic	Mixed	n	Detailed	Privacy protection	High
Ours	Incomplete	Bounded	Non-cooperative	Stochastic	Dynamic	Mixed	n	Detailed	Strategy selection	High

3) In terms of game types and game structure, Li *et al.* [4] analyze the Nash equilibrium, Serra *et al.* [8] calculate the equilibrium solution using Pareto optimization algorithm, Liu *et al.* [10] take into account the Bayesian Nash equilibrium, and Huang *et al.* [17] explore the Nash equilibrium of attack-defense game system under different states with Markov decision process, and calculated the optimal solution by linear programming algorithm. The above studies all focus on how to solve the game solution, while the [15], [16], [20], [22], and ours show the dynamic process of strategy evolution, and analyze the strategy selection at different evolutionary times. In [8], the game structure focuses on three types of attackers while this paper is applicable to n types of attackers. In [16], the game structure only abstracts two simple attack-defense strategies, namely, whether to attack or not, and whether to increase the defense investment or not. This paper comprehensive considers the general game structure containing n kinds of attack strategies and m kinds of defense strategies.

4) In terms of the evolutionary behavior, [4], [8], and [10] do not consider the influence of natural selection, and there is no analysis with the strategies adjustment. Liu *et al.* [15], Zhu *et al.* [16], Huang *et al.* [17], and Du *et al.* [22] analyze the deterministic evolution, that is, the player always selects the high-payoff strategy during the evolutionary process. On the contrary, [20] and this paper consider the random genetic variations and stochastic environmental disturbances. The stochastic biological network under natural selection in [20] is modeled through Poisson-driven genetic variations and random environmental fluctuations. Moreover, its emphasis is the analysis of the transformation from the non-cooperative strategy selection to an equivalent multi-objective optimization problem and the solution of solving this problem. In contrast, we focus on how to apply the stochastic replicator dynamics based game theory to model the process of network attack-defense and calculate the optimal strategy. We consider the short sight of attack-defense players, which is more consistent with the reality of the network. For network security issue, we take new insight into the uncertain selection causing by the information asymmetry and strategy adjustment. In detail, according to the difference between players' cognitive abilities, we innovatively introduce the selection intensity parameter to model the stochastic law of strategy evolution. All above are more consistent with the actual attack-defense environment.

5) In terms of strategy type, strategy independence and equilibrium solution, Serra *et al.* [8] and Liu *et al.* [10] take into account the type of pure strategy. In fact, pure strategy is a special case of mixed strategies, and we consider the more general mixed strategies. Liu *et al.* [15] and Chen and Yeh [20] provide the investigations on cooperative and non-cooperative games. In detail, to optimize the intrusion detection strategy for lowering energy consumption and reducing alarm messages in a Sensor-Cloud, Liu *et al.* [15] describe how the physical sensor nodes and virtual sensor-service nodes should cooperate with each other in employing a defense strategy of monitoring and informing with evolutionary game theory. Zhu *et al.* [16] take new insights into the phenotypic robustness of non-cooperative and cooperative strategies from a stochastic Nash game perspective. Because the interests of the attackers and defenders are conflicting, we model the process of attack-defense over the framework of a non-cooperative game, which fits the characteristic of network security. Zhu *et al.* [16] undertakes the simple 2 by 2 games to model the security governance, but does not give the specific calculating process regarding its equilibrium. We give the detailed computing process shown in algorithm 1. Overall, the practical guidance of this paper is outstanding.

6) In terms of application scenario, [4], [8], [17], and this paper focus on the issue of strategy selection in the field of network attack-defense. Chen and Yeh [20] give the discussion about the phenotypic robustness and network

evolvability of strategy selection under natural selection. Liu *et al.* [10] evaluate the performance of worm attack-defense game. For social network, a game theoretic framework to model users' interactions that influence users' decisions as to whether to undertake privacy protection or not is established in [22]. Considering the security protection in the sensor-cloud computing environments, Liu *et al.* [15] formulate the cooperative defense decision-making problem among multiple intrusion detection systems as an evolutionary game. Overall, the mentioned topics are the extension of strategy selection. Therefore, the research issue of strategy selection is more general.

VI. CONCLUSION

Game theory is an effective tool to study the proactive defense of network security. At present, the research on attack-defense game with player's bounded rationality is still in its infancy. Besides, there are many restrictions on the information requirements, game structure, strategy type and equilibrium solution, which seriously affect the universality and effectiveness of the game models and methods.

This paper starts with the view of bounded rationality of players, breaks through the limit of complete information, builds attack-defense evolutionary game model under the condition of incomplete information, and expands the set of player types and strategies in existing game structure. By further improving the replicator dynamic mechanism of biological evolution theory, we construct the stochastic replicator dynamic equation of attack-defense strategies. Moreover, we describe the evolutionary tracks of both attackers and defenders. We also give the selection method of optimal defense strategy by solving the evolutionary stable equilibrium. Results of numerical experiment and comparison show that the proposed model and algorithm are suitable for practical application. Moreover, the dynamic analysis performance of selecting strategy and the ability of predicting the defense situation are improved, which provide effective guidance for proactive defense.

ACKNOWLEDGMENT

Thanks for the valuable review comments of every expert and editor.

REFERENCES

[1] C. T. Do *et al.*, "Game theory for cyber security and privacy," *ACM Comput. Surv.*, vol. 50, no. 2, 2017, Art. no. 30.

[2] W. Jiang, B. Fang, Z. Tian, and H. Zhang, "Research on defense strategies selection based on attack-defense stochastic game model," *Chin. J. Comput. Res. Develop.*, vol. 47, no. 10, pp. 1714–1723, 2010.

[3] W. Jiang, B.-X. Fang, Z.-H. Tian, and H.-L. Zhang, "Evaluating network security and optimal active defense based on attack-defense game model," *Chin. J. Comput.*, vol. 32, no. 4, pp. 817–827, 2009.

[4] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 3, no. 1, pp. 1–11, Mar. 2017.

[5] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 145–153, 2007.

[6] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[7] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big data analysis based security situational awareness for smart grid," *IEEE Trans. Big Data*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/7587350/

[8] E. Serra, S. Jajodia, A. Pugliese, A. Rullo, and V. S. Subrahmanian, "Pareto-optimal adversarial defense of enterprise systems," *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 3, 2015, Art. no. 11.

[9] Y.-Z. Wang, C. Lin, X.-Q. Cheng, and B.-X. Fang, "Analysis for network attack-defense based on stochastic game model," *Chin. J. Comput.*, vol. 33, no. 9, pp. 1748–1762, 2010.

[10] Y. Liu, D. Feng, and L. Wu, "Performance evaluation of worm attack and defense strategies based on static Bayesian game," *Chin. J. Softw.*, vol. 23, no. 3, pp. 712–723, 2012.

[11] H. Zhang, D. Yu, and J. Hang, "Defense policies selection method based on attack-defense signaling game model," *J. Commun.*, vol. 37, no. 5, pp. 39–49, 2016.

[12] J. Liu, H. Zhang, and Y. Liu, "Research on optimal selection of moving target defense policy based on dynamic game with incomplete Information," *Acta Electron. Sinica*, vol. 46, no. 1, pp. 82–89, 2018.

[13] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int. J. Netw. Secur.*, vol. 2, no. 2, pp. 131–137, 2006.

[14] S. Rass, A. Alshawish, M. A. Abid, S. Schauer, Q. Zhu, and H. De Meer, "Physical intrusion games—Optimizing surveillance by simulation and game theory," *IEEE Access*, vol. 5, pp. 8394–8407, 2017.

[15] J. H. Liu, J. Yu, and S. Shen, "Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 408–420, Feb. 2018.

[16] J. Zhu, B. Song, and Q. Huang, "Evolution game model of offense-defense for network security based on system dynamics," *J. Commun.*, vol. 25, no. 1, pp. 54–61, 2014.

[17] J. Huang, H. Zhang, and J. Wang, "Markov evolutionary games for network defense strategy selection," *IEEE Access*, vol. 5, pp. 19505–19516, 2017.

[18] J. Huang, H. Zhang, and J. Wang, "Defense strategies selection based on attack-defense evolutionary game model," *J. Commun.*, vol. 38, no. 1, pp. 168–176, 2017.

[19] Y. Hayel and Q. Zhu, "Epidemic protection over heterogeneous networks using evolutionary Poisson games," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1786–1800, Aug. 2017.

[20] B.-S. Chen and C.-H. Yeh, "Stochastic noncooperative and cooperative evolutionary game strategies of a population of biological networks under natural selection," *Biosystems*, vol. 162, pp. 90–118, Dec. 2017, doi: 10.1016/j.biosystems.2017.08.001.

[21] P. H. Liu and J. Liu, "Robustness of coevolution in resolving prisoner's dilemma games on interdependent networks subject to attack," *Phys. A, Stat. Mech. Appl.*, vol. 479, pp. 362–370, Aug. 2017.

[22] J. Du, C. Jiang, K.-C. Chen, Y. Ren, and H. V. Poor, "Community-structured evolutionary game for privacy protection in social networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 574–589, Mar. 2018.

[23] C. Jiang, Y. Chen, and K. J. R. Liu, "Evolutionary dynamics of information diffusion over social networks," *IEEE Trans. Signal Process.*, vol. 62, no. 17, pp. 4573–4586, Sep. 2014.

[24] C. Jiang, Y. Chen, and K. R. Liu, "Graphical evolutionary game for information diffusion over social networks," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 524–536, Aug. 2014.

[25] Y. Wang, J. Yu, and W. Qiu, "Evolutionary game model and analysis methods for network population behavior," *Chin. J. Comput.*, vol. 38, no. 2, pp. 282–300, 2015.

[26] J. C. Harsanyi, "Games with incomplete information played by 'Bayesian' players," in *Papers in Game Theory* (Theory and Decision Library), vol. 28. Dordrecht, The Netherlands: Springer, 1982. [Online]. Available: https://doi.org/10.1007/978-94-017-2527-9_7

[27] K. Sigmund and M. A. Nowak, "Evolutionary game theory," in *Current Biology CB*, vol. 38. Cambridge, MA, USA: MIT Press, 1997, pp. 847–858, doi: 10.1016/S0960-9822(99)80321-2.

[28] J. Tanimoto, *Fundamentals of Evolutionary Game Theory and its Applications* (Evolutionary Economics and Social Complexity Science). Tokyo, Japan: Springer, 2015. [Online]. Available: http://ktlabo.cm.kyushu-u.ac.jp/j_old/event/productFlyer_978-4-431-54961-1.pdf, doi: 10.1007/978-4-431-54962-8_2.

[29] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. ACM Workshop Game Theory Commun. Netw.*, 2006, Art. no. 4. [Online]. Available: https://doi.org/10.1145/1190195.1190198
[30] X.-J. Wang, J. Quan, and W.-B. Liu, "Study on evolutionary games and cooperation mechanism within the framework of bounded rationality," *Syst. Eng. Theory Pract.*, vol. 31, no. s1, pp. 82–93, 2011.
[31] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "CSI/FBI computer crime and security survey," *Inf. Manage. Comput. Secur.*, vol. 15, no. 3, pp. 78–101, 2006.

HAO HU was born in Chizhou, Anhui, China, in 1989. He received the B.S. and M.S. degrees from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2012 and 2015, respectively, where he is currently pursuing the Ph.D. degree. He is currently a Visiting Ph.D. Student with the Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences. His main research interests include network security, proactive defense, and secret image sharing.

YULING LIU was born in Jiyang, Shandong, China, in 1983. He received the Ph.D. degree from the University of Chinese Academy of Sciences in 2013. He took a successive postgraduate and doctoral program. His main research interests include network and system security assessment and big data security.

Since 2017, he has been an Assistant Researcher with the Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences.

HONGQI ZHANG was born in Tangshan, Hebei, China, in 1962. He received the Ph.D. degree from the Zhengzhou Information Science and Technology Institute in 2002. His main research interests include network security and classification protection.

Since 2013, he has been a Professor and a Ph.D. Supervisor with the Zhengzhou Information Science and Technology Institute. He is an Editor of the *Chinese Journal of Network and Information Security*.

Mr. Zhang received the first prize of National Teaching Prize in 2009 and the second prize of the National Science and Technology Progress Award in 2012 and the National Network Security Outstanding Teacher Award in 2017.

RUIXUAN PAN was born in Wulumuqi, Xinjiang, China, in 1995. She received the B.S. degree from Shihezi University in 2017. She is currently pursuing the M.S. degree with the Zhengzhou Information Science and Technology Institute. Her main research interests include network security and risk evaluation.