IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 19, 2018, accepted October 10, 2018, date of publication November 9, 2018, date of current version April 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2880214

Attack-Defense Differential Game Model for Network Defense Strategy Selection

HENGWEI ZHANG[1, 2], **LV JIANG**[1], **SHIRUI HUANG**[1], **JINDONG WANG**[1] **AND YUCHEN ZHANG**[1]
[1]Zhengzhou Institute of Information Science and Technology, Zhengzhou 450001, China
[2]Science and Technology on Information Assurance Laboratory, Beijing 100093, China

Corresponding author: Hengwei Zhang (wlby_zzmy_henan@163.com).

This work was supported in part by the National Natural Science Foundation of China under Grant 61521003 and 61572517 and in part by the Henan Science and Technology Research Project under Grant 182102210144.

ABSTRACT The existing game-theoretic approaches for network security problems mostly use the static game or the multi-stage dynamic game. However, these researches can not meet the timeliness requirment to analyze the network attack and defense. It is better to regard the attack and defense as a dynamic and real-time process, in which way the rapidity and continuity of network confrontation can be described more precisely. Referring to the epidemic model SIR, we formulated the novel model NIRM to analyze the evolution of network security states. Based on the mentioned above, the attack-defense differential game model was constructed by introducing the differential game theory. Then we figured out the solution of saddle-point strategies in the game. By analyzing the game equilibrium, the algorithm of optimal defense strategies selection in the real-time confrontation was designed, which is more targeted and has greater timeliness. Finally by simulation experiments, we demonstrated the validity of the model and method proposed in this paper, and drew some instructive conclusions on network defense deployment.

INDEX TERMS Network security, Network attack and defense, Security states evolution, Differential game, Attack-defense analysis, Optimal strategy selection.

I. INTRODUCTION

Since the rapid development of network and information technology, along with the close integration of cyberspace and physical space, the network infrastructure has become the neural system of social activities in the information era [1]. As a result, it is an urgent issue to enhance network security defense capabilities, when being faced with lots of challenges in the field of cyberspace security [2]. The essence of cyber security is attack and defense. Therefore, it is practically significant to explore the network security analysis methods and active defense systems from the attack-defense perspective, which has become a research hotspot in recent years [3].

The game theory has very good agreement with the network attack and defense, which has the features of objective opposition, relationship non-cooperation and strategic dependence [4]. Currently, the researches on game models for the network attack-defense behaviors and defense decision-making analysis have achieved some results. Jiang *et al.* [5] proposed an attack-defense behavior analysis method based on the game model, and adopted a zero-sum game under complete information static conditions to conduct defense decision-making research. Focusing on the attack behaviors in social networks, White *et al.* [6] conducted attack-defense analysis and defense decision-making based on the complete information static game model. Because of the antagonistic relationship between the attacker and defender, it is very difficult to grasp the other players' behaviors and payoffs information. Thus the researches based on the complete information game theory have serious shortcomings in practice. In response to this problem, Liu *et al.* [7] introduced incomplete information static game theory and realized the effectiveness evaluation of different anti-worms defense strategies with the incomplete game information restriction conditions. Yu *et al.* [8] used the static Bayesian game theory to construct the attack-defense model, and investigated the defense decision-making issue by analyzing the Bayesian Nash equilibrium. In the attack-defense process, since the actions of the attacker and the defender generally do not have simultaneity, it has better research value to establish a network attack-defense model by the dynamic game theory. Lin *et al.* [9] constructed the dynamic

The associate editor coordinating the review of this manuscript and approving it for publication was Haider Abbas.

game model to select the best strategic choice in active defense. In addition, Wang *et al.* [10] and Jiang *et al.* [4] constructed an attack-defense stochastic game model, carried out quantitative analysis on network attack and defense, and proposed an optimal defense strategy selection method. Wang *et al.* [11] and Yu *et al.* [12] improved the security state transition model of network system in attack and defense stochastic games, and investigated the network survivability and network attacks. However, it is difficult to calculate the state transition probability exactly. Take into consideration the influence of attack-defense behavior information on the strategy selection, Zhang *et al.* [13], [14] constructed the attack-defense signaling game model. By analyzing refined Bayesian Nash equilibrium, the information security risk assessment and defense strategy selection were studied.

The above researches are based on the one-shot game between the attacker and defender, while network security analysis must be consistent with the actual attack-defense scenarios. Because of the multi stages and continuity of actual confrontation, it is more reasonable to consider attack-defense process as a multi-stage game [15]. Taking the WSN defense mechanism as background [16], Dadsk *et al.* studied anti-DDOS attack method in the wireless network based on the attack-defense repeated game model. Zhang *et al.* [17] built up a multi-stage attack-defense signaling game model based on incomplete information dynamic game theory, and investigated the defense decision-making in multi-stage attack and defense under limited information conditions.

However, employing the multi-stage dynamic game model can only answer the network security questions regarding that attack-defense process is intermittent and discrete. Nowadays the cyberspace confrontation has become increasingly fierce, and the attack and defense have developed towards a rapid, real-time, and diversified direction. The analysis methods based on traditional dynamic games can no longer meet actual requirements. The attack-defense process is generally divided into multiple stages for analysis. Actually the length of time in each stage changes dynamically, rather than keeping the same. Besides, as the development of technology, the attack-defense process gradually changes with high frequency. As a result, it is hard to keep the conditions of decision-making unchanged at all times. Therefore, it is urgent to establish a game model that can analyze the dynamic, continuous, and real-time attack-defense process, and study the defense decision-making method with respect to the time factor. Differential game is a theoretical method to describe the continuous control process in the confrontation with real-time changes in time [18]. It can describe the dynamic and continuous evolution process of system state and control strategies, which has the better capacity to analyze the real-time attack-defense behaviors and study the optimal selection of defense strategies. Unlike dynamic games, the security state of the network system changes dynamically in the differential game, and the results of attack and defense are directly influenced and constrained by the time factor, which is real-time. Therefore, both the control strategies and the payoffs of the attacker and defender are denoted by differential equations, which are the continuous paths in the phase space containing the time variable. Moreover, the game equilibrium is a functional form and its solution is a variational problem [19]. Because it is hard to construct, solve and analyze the attack-defense differential game model, there are few publish literature discussing the mentioned methods.

In this article, we draw on the infectious diseases dynamics theory [20] to construct a state evolution model NIRM to analyze the evolution process of network system security states. Then the attack-defense differential game model is constructed. Based on the model, we put forwards attack-defense strategy control functions and return integration functions, to describe the selection of strategies and the changes of players' payoffs. By the solution and analysis of the saddle-point strategy, we obtain the equations to describe the optimal strategy control trajectory, and design a real-time selection algorithm of the optimal defense strategy. Compared with the existing work, this method can analyze the attack-defense behaviors in continuous and real-time confrontation, and the result of network defense decision-making has greater timeliness, pertinence and guiding significance.

II. ATTACK-DEFENSE DIFFERENTIAL GAME MODEL

Based on the dynamic process of network security state transition, we construct an attack-defense differential game model to analyze the decision-making behaviors of both players over time, aiming at deal with the challenges of rapid and high-frequency changes in attack-defense process. Then taking this as a tool, we study defense strategy selection methods with continuous and real-time decision-making capability.

A. EVOLUTION OF SECURITY STATES IN ATTACK AND DEFENSE

The SIR model in infectious disease dynamics theory describes the dynamic process of disease infection and outbreaks in the population [21]. In network attack and defense, the attacker exploits the vulnerability of network nodes. Then it infiltrates and infects other nodes in the system from individual nodes, which is obviously similar to the spread and destruction of infectious diseases. The attack and defense, that occur in the network with a large number of nodes, is also an evolutionary dynamic process. On the one hand, the security states of the nodes that make up the system are constantly migrating. On the other hand, the number of nodes in different security states changes dynamically. In order to portray this process, we extend it to analogize the nodes to individuals referring to the SIR model. According to the actual network attack and defense, the evolutionary states in the SIR model are expanded to four states, and the nodes are divided into four categories according to their security states. Moreover, taking the strategy selection and confrontation results of both players as the key factors for the node states migration, we construct a security state evolution model NIRM.

The NIRM model contains four states: normal state N (Normal), infected state I (Infected), restored state R (Restored), and malfunctioned state M (Malfunctioned). Among them,

- N: The network node is in normal working condition, but the node may be attacked due to its inherent vulnerability.
- I: The network node is penetrated or infected by the attack strategy, but its quality of service has not yet declined. Furthermore, the attacker can use this node to attack neighboring nodes.
- R: The network node is protected by the defense strategy and is immune to the attack strategy.
- M: The network node is in a state of serious deterioration in service quality or loss of service capability

The migration modes of network nodes in the above four states are shown in Fig. 1.

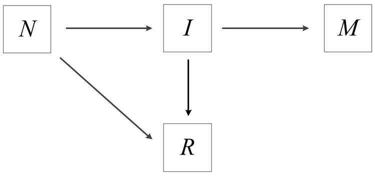


FIGURE 1. **Four migration modes between different states in NIRM model.**

Supposing Q as the total number of network nodes, the number of nodes in the above four states at time t is recorded as $N(t)$, $I(t)$, $R(t)$ and $M(t)$. Then $\forall t \in [t_0, T]$, $N(t), I(t), R(t), M(t) \in \mathbb{N}$ and $N(t)+I(t)+R(t)+M(t) = Q$.

In the NIRM model, there are four migration modes for network node states.

$N \rightarrow I$: Faced with an attack strategy, if the defense strategy fails, the node is penetrated or infected by the attacker. At this time, the attack damage effect is still in the latent period, and the node service quality is not lost. However, the attacker can use this node to attack the adjacent node for a wider range of attacks. For example, an attacker uses a virus strategy to infect a network node, but not destroy it immediately. Instead, it temporarily lurks and spreads by infected nodes to fight for the destruction of a larger number of nodes in the system.

$N \rightarrow R$: As the defense strategy succeeds, normal nodes have the immunity to attacks. For example, a defender installs a patch or updates anti-virus software to defend against a virus attack.

$I \rightarrow R$: The defense strategy identifies the infected node successfully and clears the infiltration or infection. As a result, the defender restricts the attack damage effect that has not appeared yet, avoids the loss of the infected node and transforms the node into the immune state. However, the attack visa infected node to neighboring nodes before the state migration, can not be remedied. For example, the virus can be removed by updating the node's anti-virus software, but the consequences of virus spread before cannot be eliminated.

$I \rightarrow M$: When suffering an attack, if the defense strategy fails, the damage effect will occur, and the infected node will lose service function. Then the damaged node cannot be remedied and can no longer be used to attack adjacent nodes. For example, although the infected node updates anti-virus software, it still fails to remove the virus before the virus attack. Finally the virus attack may cause the node to crash and exit the network system.

By the conclusion from the researches on the infectious disease dynamics theory and analysis of the migration paths, we find that there are two main reasons that affect the state of nodes in the network system. (a) The number of normal nodes directly connected to the infected node. An attacker can use an infected node to attack adjacent normal nodes. Therefore, the larger the number of normal nodes adjacent to infected nodes is, the faster infected nodes may increase. As a result, the security risk tends to increase. (b) The game results between attack and defense strategies. The result is the key factor in determining the state transition. For a specific node, the confrontation result directly determines its state transition path. The specific analysis of the evolution process is as follows.

Assuming that nodes are deployed in the network system with density α, for a network node, the number of nodes connected to it is $\alpha\pi r^2$. Among them, r represents the network connection distance of two nodes. When $r = 1$, it means that two nodes are directly connected. For a node in infected state I, the number of adjacent nodes that can directly communicate with it is $\alpha\pi$. At time t, the proportion of normal nodes in all nodes is $N(t)/Q$. Therefore in the entire network system, if assuming that the number of network nodes is large and the infected nodes are far away from each other, the number of normal nodes directly connected with the infected node at time t will be $\theta\pi I(t)N(t)/Q$, when ignoring the overlap effect of the infected nodes' influence range. If the defense strategy fails, the above normal node will be transformed into an infected one.

The confrontation result of attack-defense strategies is the key factor in determining the state transition. Then we describe a network attack and defense example to illustrate the security state changing process of a network node in detail. According to the attack strength, we divide the attack strategies into three types: strong-intensity attack A_H, medium-intensity attack A_M, and weak-intensity attack A_L, whose average attack strength can be expressed in turn as $\overline{e_A^H}, \overline{e_A^M}, \overline{e_A^L} \in [0, 1]$. Then we define the mixed strategy of attacker as $P_A(t) = (p_A^H(t), p_A^M(t), p_A^L(t))$, in which $p_A^H(t)$, $p_A^M(t)$ and $p_A^L(t)$ denote the possibilities to select attack strategies A_H, A_M and A_L relatively. Thus when the attacker uses a mixed strategy $P_A(t) = (p_A^H(t), p_A^M(t), p_A^L(t))$ at time t, the expected attack utility is $a(t) = p_A^H(t)\overline{e_A^H} + p_A^M(t)\overline{e_A^M} + p_A^L(t)\overline{e_A^L}$, abbreviated as a.

Similarly, defense strategies are divided into D_H, D_L according to the defense strength, and their average defense strength are $\overline{e_D^H}, \overline{e_D^L} \in [0, 1]$ respectively. If the defender uses a mixed strategy $P_D(t) = (p_D^H(t), p_D^L(t))$ with $p_D^H(t), p_D^L(t)$ denoting the selection possibilities of D_H and D_L relatively at time t, the expected defense utility is expressed as $d(t) = p_D^H(t)\overline{e_D^H} + p_D^L(t)\overline{e_D^L}$, abbreviated as d. Then we use the difference between attack and defense utility $\eta(t) = a(t) - d(t)$ to indicate the success of the attack, with $|\eta(t)| \in [0, 1]$. If $\eta(t) > 0$, it means that the attack is successful, otherwise it indicates that the attack failed.

To analyze the state transition path by the attack and defense expected utility $\eta(t)$, we can get the following transition parameters η_{NI}, η_{NR}, η_{IR}, and η_{IM} that denote the possibility of state transition respectively:

$$\eta_{NI} = \begin{cases} 0, & \eta(t) \le 0 \\ \eta(t), & \eta(t) > 0, \end{cases} \quad \eta_{NR} = \begin{cases} |\eta(t)|, & \eta(t) \le 0 \\ 0, & \eta(t) > 0, \end{cases}$$
$$\eta_{IM} = \begin{cases} 0, & \eta(t) \le 0 \\ \eta(t), & \eta(t) > 0, \end{cases} \quad \eta_{IR} = \begin{cases} |\eta(t)|, & \eta(t) \le 0 \\ 0, & \eta(t) > 0. \end{cases} \tag{1}$$

In summary, we can describe the security state changing process of the network nodes by the state evolution differential equations based on NIRM model as follows.

$$\begin{cases} \overset{\bullet}{N} = -\eta_{NI}(t)\alpha\pi I(t)N(t)/Q - \eta_{NR}(t)N(t) \\ \overset{\bullet}{I} = \eta_{NI}(t)\alpha\pi I(t)N(t)/Q - \eta_{IM}(t)I(t) - \eta_{IR}(t)I(t) \\ \overset{\bullet}{R} = \eta_{NR}(t)N(t) + \eta_{IR}(t)I(t) \\ \overset{\bullet}{M} = \eta_{IM}(t)I(t) \\ \forall t \in [t_0, T], \quad N(t) + I(t) + R(t) + M(t) = Q \\ N(t), I(t), R(t), M(t) \in \mathbb{N} \end{cases} \tag{2}$$

B. NETWORK ATTACK-DEFENSE DIFFERENTIAL GAME MODEL

Based on the evolution of network security state during the attack and defense, we can construct the attack-defense differential game model.

Definition 1: Network Attack-Defense Differential Game Model can be expressed as a eight-tuple $ADDG = (N, \Theta, B, t, x, S, f, U)$, where

① $N = (N_{\mathrm{D}}, N_{\mathrm{A}})$ is the set of players in the attack and defense game. Among them, N_{D} is the defender and N_{A} is the attacker;

② $\Theta = (\Theta_D, \Theta_A)$ is the type space for the defender and attacker. It is the private information for players, in which $\Theta_D = \{D_i | i = 1, 2, \cdots, n\}$ and $\Theta_A = \{A_j | j = 1, 2, \cdots, m\}$;

③ $B = (DS, AS)$ is the action space. $AS = (\delta_1, \delta_2, \cdots, \delta_g)$ and $DS = (\beta_1, \beta_2, \cdots, \beta_k)$ denote the action sets of the attacker and defender respectively, with their action numbers not less than 1 (i.e., $g, k \ge 1$);

④ t represents the moment in the attack-defense differential game with $t \in [t_0, T]$. The system states, the control strategy trajectories of both players, and the game payoffs are all functions with respect to t;

⑤ $x(t) = \{(N(t), I(t), R(t), M(t)) | N(t) + I(t) + R(t) + M(t) = Q\}$ is the state variable of the network system. $N(t)$, $I(t)$, $R(t)$ and $M(t)$ denote the number of nodes in the normal state N, the infected state I, the restored state R, and malfunctioned state M in the system at time t respectively. Moreover, Q denotes the total number of nodes;

⑥ $S = (D(t), A(t))$ denotes the control strategies of players at time t. Among them, $D(t) = \{P_D(t) | P_D(t) = (p_D^i(t)), 1 \le i \le n\}$ is the mixed strategies chosen by defenders at time t, where $p_D^i(t)$ is the probability of selecting different types of defense strategies satisfying $\sum_{i=1}^{n} p_D^i(t) = 1$. Similarly, the attack mixed strategy at time t is $P_A(t) = \{(p_A^j(t) | 1 \le j \le m\}$ with $\sum_{j=1}^{m} p_A^j(t) = 1$. The control strategy is a function of time variable t, initial state $x(t_0)$ and current state $x(t)$, also denoted as $P_A(t) = P_A(t, x(t_0), x(t))$ and $P_D(t) = P_D(t, x(t_0), x(t))$;

⑦ $f = \{f_N, f_I, f_R, f_M\}$ is the state transition function. Among them, $f_N = \frac{\mathrm{d}N(t)}{\mathrm{d}t} = \overset{\bullet}{N}$, $f_I = \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \overset{\bullet}{I}$, $f_R = \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \overset{\bullet}{R}$, $f_M = \frac{\mathrm{d}M(t)}{\mathrm{d}t} = \overset{\bullet}{M}$. More specific analysis of state transitions can be seen in Section II(A);

⑧ $U = (U_D, U_A)$ is the players' payoff functions. For the attack-defense differential game during $[t_0, T]$, the payoff function is $U = \int_{t_0}^{T} g(t, x(t), P_A(t), P_D(t))\,\mathrm{d}t$, where U is an integral function that dynamically changes with time. Compared with the traditional multi-stage dynamic game, the detailed analysis is as follows.

Based on the game model definition and the analysis in Section II, in the network system, when the network node state changes from the normal state N to the infected state I, the return coefficient r_1 denotes to the harm for the node and its adjacent node when being infected. When the node transforms from the infected state I or the normal state N to the restored state R, the return coefficient r_2 is denoted to the expected loss that the restored node can reduce after being immune to attack. When the node transforms from the infected state I to the malfunctioned state M, let return coefficient r_3 be the loss caused by the damage to service function of the node. In the actual attack-defense game, since there are many factors affecting the return coefficient, the return coefficient is generally a nonlinear formula. To facilitate the following analysis, we define return coefficients $r_1, r_2, r_3 \in [0, 10]$ by the statistical average referring to [22]. The exact calculation method of the return coefficient will be studied in our future work.

According to the above analysis, the defense return $r_D(t)$ and attack return $r_A(t)$ at t are

$$\begin{aligned} r_D(t) = {} & r_2[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)] \\ & - r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q] - r_3[\eta_{IM}(t)I(t)], \end{aligned} \tag{3}$$

$$\begin{aligned} r_A(t) = {} & r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q] \\ & + r_3[\eta_{IM}(t)I(t)] - r_2[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)]. \end{aligned} \tag{4}$$

Both the attacker and defender will consume the corresponding strategy cost when implementing the strategy, which is generally proportional to the strategy performance. Referring to [16], the strategy execution cost at time t are

$$\begin{aligned} v_D &= \frac{d^2}{2} c_D \left(N(t)+I(t)+R(t)+M(t)\right), \\ v_A &= \frac{a^2}{2} c_A \left(N(t)+I(t)+R(t)+M(t)\right). \end{aligned} \tag{5}$$

Among them, c_D and c_A are the cost/utility coefficients for defense and attack strategies respectively, with $c_D, c_A \in [1, 10]$.

Among them, c_D and c_A are the cost/utility coefficients for defense and attack strategies respectively. Moreover, they are dimensionless coefficients, which represent the ratio of strategic cost to effectiveness. The smaller the values of c_D and c_A are, the better the cost performances of the strategy are. Both the attacker and defender pursue the strategies with smaller cost/utility coefficients, which are relatively more difficult. In general, in order to denote the proportional relationship between cost and utility, and to facilitate calculation and post-processing conveniently, we set $c_D, c_A \in [1, 10]$ [16], [22].

Take the strategy return and execution cost into account comprehensively, the payoff functions of the attacker and defender in the differential game are

$$\begin{aligned} &U_D(P_A(t), P_D(t)) \\ &\quad = \int_{t_0}^{T} r_2[\eta_{NR}N + \eta_{IR}I] - r_1[\eta_{NI}\alpha\pi IN/Q] \\ &\qquad - r_3[\eta_{IM}I] - \frac{c_D}{2} d^2 \left(N+I+R+M\right)] \, \mathrm{d}t, \qquad (6) \\ &U_A(P_A(t), P_D(t)) \\ &\quad = \int_{t_0}^{T} r_1[\eta_{NI}\alpha\pi IN/Q] - r_2[\eta_{NR}N + \eta_{IR}I] \\ &\qquad + r_3[\eta_{IM}I] - \frac{c_A}{2} a^2 \left(N+I+R+M\right)] \, \mathrm{d}t. \qquad (7) \end{aligned}$$

III. OPTIMAL DEFENSE STRATEGY SELECTION

A. THE SOLUTION OF SADDLE-POINT STRATEGY

Given the attack-defense differential game *ADDG*, the strategies of both players are interdependent, and the strategy pair $(P_A^*(t), P_D^*(t))$ composed of their optimal strategies are called the saddle-point strategy in the attack- defense differential game.

Definition 2: Saddle-point strategy. In the attack-defense differential game *ADDG*, if there is a strategy pair $(P_A^*(t), P_D^*(t))$ satisfying

$$\begin{cases} \forall P_A(t), \; U_A(P_A(t)^*, P_D(t)^*) \geq U_A(P_A(t), P_D(t)^*) \\ \forall P_D(t), \; U_D(P_A(t)^*, P_D(t)^*) \geq U_D(P_A(t)^*, P_D(t)), \end{cases}$$

then we call $(P_A^*(t), P_D^*(t))$ the saddle-point strategy in attack-defense differential game, also known as the saddle-point strategy of both attacker and defender.

According to differential game theory [23], the saddle-point existence theorem of attack-defense differential game is briefly proved as follows.

Theorem 1: The saddle-point strategy $(P_A^*(t), P_D^*(t))$ for attack-defense differential game exists, if there is a common-state function $K_i(t) : [t_0, T] \times \Re^k \to \Re, \; i \in (D, A)$ that allows the following conditions (8-10) hold.

$$\begin{cases} P_A^*(t) = \underset{P_A(t)}{\arg\max}\{f\left(t, x^*(t), P_A(t), P_D^*(t)\right) K_A(t) \\ \qquad\qquad + g\left(t, x^*(t), P_A(t), P_D^*(t)\right)\} \\ P_D^*(t) = \underset{P_D(t)}{\arg\max}\{f\left(t, x^*(t), P_A^*(t), P_D(t)\right) K_D(t) \\ \qquad\qquad + g\left(t, x^*(t), P_A^*(t), P_D(t)\right)\} \end{cases} \tag{8}$$

$$\begin{cases} \dfrac{d}{dt} x^*(t) = f(t, x^*(t), P_A^*(t), P_D^*(t)) \\ x^*(t_0) = x(t_0) \end{cases} \tag{9}$$

$$\begin{cases} \dfrac{d}{dt} K_A(t) = -\dfrac{\partial}{\partial x^*}\{f\left(t, x^*(t), P_A^*(t), P_D^*(t)\right) K_A(t) \\ \qquad\qquad + g\left(t, x^*(t), P_A^*(t), P_D^*(t)\right)\} \\ \dfrac{d}{dt} K_D(t) = \dfrac{\partial}{\partial x^*}\{f\left(t, x^*(t), P_A^*(t), P_D^*(t)\right) K_D(t) \\ \qquad\qquad + g\left(t, x^*(t), P_A^*(t), P_D^*(t)\right)\} \end{cases} \tag{10}$$

Proof: According to the definition of saddle point strategy, the Hamilton function H can be constructed.

$$\begin{aligned} &H\left(t, K_i(t), x, P_A(t), P_D(t)\right) \\ &\quad = f\left((t, x(t), P_A(t), P_D(t)\right) K_i(t) \\ &\qquad + g\left(t, x(t), P_A(t), P_D(t)\right), \quad i \in \{D, A\} \end{aligned} \tag{11}$$

Then we transform the proof into proving the existence of the function $K_i(t) : [t_0, T] \times \Re^k \to \Re, \; i \in (D, A)$, which makes the solution $(P_A^*(t), P_D^*(t))$ of following Hamilton equations (12) satisfying (13) exists.

$$\begin{cases} \dfrac{d}{dt} K_i(t) = -\dfrac{\partial}{\partial x^*} H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right) \\ \dfrac{d}{dt} x^*(t) = \dfrac{\partial}{\partial K_i(t)} H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right) \\ x^*(t_0) = x(t_0) \end{cases} \tag{12}$$

$$\begin{aligned} &H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right) \\ &\quad = \max_{(P_A(t), P_D(t))} H\left(t, K_i(t), x^*, P_A(t), P_D(t)\right) \end{aligned} \tag{13}$$

According to the Pontryagin Maximum Principle in the optimal control theory [23], the existence of the function $K_i(t)$ can be proved, and when $t \in [t_0, T]$, the mapping $t \to H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right)$ is constant. Therefore, we can prove the theorem that there is a saddle-point strategy in the attack-defense differential game *ADDG*.

Based on the proved theorem, the solution of saddle-point strategy $(P_A^*(t), P_D^*(t))$ are put forward.

For the defender, the Hamilton function is constructed based on the attack-defense differential game model *ADDG* as follows:

$$
\begin{aligned}
&H\left(t, K_D(t), x, P_A(t), P_D(t)\right) \\
&\quad = g\left(t, x, P_A(t), P_D(t)\right) \\
&\qquad + \sum_{x \in \{N,I,R,M\}} K_D^x(t) f\left((t, x, P_A(t), P_D(t)\right) \\
&\quad = r_2[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)] - r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q] \\
&\qquad - r_3[\eta_{IM}(t)I(t)] - \frac{d^2}{2}c_D\left(N(t)+I(t)+R(t)+M(t)\right) \\
&\qquad - K_D^N(t)[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q + \eta_{NR}(t)N(t)] \\
&\qquad + K_D^I(t)\,[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q - \eta_{IM}(t)I(t) - \eta_{IR}(t)I(t)] \\
&\qquad + K_D^R(t)\,[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)] + K_D^M(t)\,\eta_{IM}(t)I(t) \\
&\quad = \eta_{NI}(t)\cdot\alpha\pi I(t)N(t)/Q\left(K_D^I(t) - K_D^N(t) - r_1\right) + \eta_{NR}(t) \\
&\qquad \cdot N(t)\left(K_D^R(t) - K_D^N(t) + r_2\right) \\
&\qquad + \eta_{IR}(t)\cdot I(t)\left(K_D^R(t) - K_D^I(t) + r_2\right) + \eta_{IM}(t) \\
&\qquad \cdot I(t)\left(K_D^M(t) - K_D^I(t) - r_3\right) - \frac{d^2}{2}c_D \\
&\qquad \times \left(N(t)+I(t)+R(t)+M(t)\right)
\end{aligned} \tag{14}
$$

Then for $x \in \{N(t), I(t), R(t), M(t)\}$, we can obtain the common-state function $K_D(t) = (K_D^x(t))^{\mathrm{T}} = (K_D^N(t), K_D^I(t), K_D^R(t), K_D^M(t))^{\mathrm{T}}$ by calculating (15-18).

$$
\begin{aligned}
\frac{d}{dt}K_D^N(t) &= -\frac{\partial}{\partial\, N(t)}H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) \\
&= [r_1\eta_{NI}^*(t)\alpha\pi I^*(t)/Q - r_2\eta_{NR}^*(t)] \\
&\quad + K_D^N(t)\,[\eta_{NI}^*(t)\alpha\pi I^*(t)/Q \\
&\quad + \eta_{NR}(t)] - K_D^I(t)\,\eta_{NI}^*(t)\alpha\pi I^*(t)/Q \\
&\quad - K_D^R(t)\,\eta_{NR}^*(t) + \frac{c_D}{2}d^2
\end{aligned} \tag{15}
$$

$$
\begin{aligned}
\frac{d}{dt}K_D^I(t) &= -\frac{\partial}{\partial\, I(t)}H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) \\
&= -r_2\,\eta_{IR}^*(t) + r_1\,\eta_{NI}^*(t)\alpha\pi N^*(t)/Q + r_3\,\eta_{IM}^*(t) \\
&\quad + K_D^N(t)[\eta_{NI}^*(t)\alpha\pi N^*(t)/Q] \\
&\quad - K_D^I(t)[\eta_{NI}^*(t)\alpha\pi N^*(t)/Q \\
&\quad - \eta_{IM}^*(t) - \eta_{IR}^*(t)] \\
&\quad - K_D^R(t)\eta_{IR}^*(t) - K_D^M(t)\eta_{IM}^*(t) + \frac{c_D}{2}d^2
\end{aligned} \tag{16}
$$

$$
\frac{d}{dt}K_D^R(t) = -\frac{\partial}{\partial\, R(t)}H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) = \frac{c_D}{2}d^2 \tag{17}
$$

$$
\frac{d}{dt}K_D^M(t) = -\frac{\partial}{\partial M(t)}H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) = \frac{c_D}{2}d^2 \tag{18}
$$

Similarly, for the attacker we can obtain the common-state function vectors $K_A^N(t), K_A^I(t), K_A^R(t), K_A^M(t)$.

For the convenience of following explanation, we construct the auxiliary formulas as follows:

$$
\begin{aligned}
&\frac{dK_D^N(t)}{dt} = \lambda_D^N(t), \quad \frac{dK_D^I(t)}{dt} = \lambda_D^I(t), \\
&\frac{dK_D^R(t)}{dt} = \lambda_D^R(t), \quad \frac{dK_D^M(t)}{dt} = \lambda_D^M(t),
\end{aligned} \tag{19}
$$

$$
\begin{aligned}
&\frac{dK_A^N(t)}{dt} = \lambda_A^N(t), \quad \frac{dK_A^I(t)}{dt} = \lambda_A^I(t), \\
&\frac{dK_A^R(t)}{dt} = \lambda_A^R(t), \quad \frac{dK_A^M(t)}{dt} = \lambda_A^M(t).
\end{aligned} \tag{20}
$$

By calculating the common-state function vectors $(K_D^N(t), K_D^I(t), K_D^R(t), K_D^M(t)\ \ )^{\mathrm{T}}$ and $(K_A^N(t), K_A^I(t), K_A^R(t), K_A^M(t))^{\mathrm{T}}$, the dynamic programming method is used to solve the saddle-point strategy. To explain more clearly, the attack and defense examples in Section II(A) are used for specific analysis.

First, we calculate the following dynamic programming problem.

$$
\begin{aligned}
&\forall P_A(t), P_D(t), \quad t \in [t_0, T],\ x \in \{N(t), I(t), R(t), M(t)\} \\
&\times \begin{cases}
H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) \\
\quad \geq H\left(t, K_D(t), x^*, P_A^*(t), P_D(t)\right) \\
H\left(t, K_A(t), x^*, P_A^*(t), P_D^*(t)\right) \\
\quad \geq H\left(t, K_A(t), x^*, P_A(t), P_D^*(t)\right) \\
\dfrac{dK_D^N(t)}{dt} = \lambda_D^N, \quad \dfrac{dK_D^I(t)}{dt} = \lambda_D^I, \ \dfrac{dK_D^R(t)}{dt} = \lambda_D^R, \\
\quad \dfrac{dK_D^M(t)}{dt} = \lambda_D^M \\
\dfrac{dK_A^N(t)}{dt} = \lambda_A^N, \quad \dfrac{dK_A^I(t)}{dt} = \lambda_A^I, \ \dfrac{dK_A^R(t)}{dt} = \lambda_A^R, \\
\quad \dfrac{dK_A^M(t)}{dt} = \lambda_A^M \\
\dfrac{\mathrm{d}N^*(t)}{\mathrm{d}t} = -\eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q - \eta_{NR}(t)N^*(t) \\
\dfrac{\mathrm{d}I^*(t)}{\mathrm{d}t} = \eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q \\
\quad - I^*(t)\left(\eta_{IM}^*(t) + \eta_{IR}^*(t)\right) \\
\dfrac{\mathrm{d}R^*(t)}{\mathrm{d}t} = \eta_{NR}^*(t)N^*(t) + \eta_{IR}^*(t)I^*(t), \\
\quad \dfrac{\mathrm{d}M^*(t)}{\mathrm{d}t} = \eta_{IM}^*(t)I^*(t) \\
N^*(t_0) = N(t_0), \quad I^*(t_0) = I(t_0), \\
\quad R^*(t_0) = R(t_0), \quad M^*(t_0) = M(t_0)
\end{cases}
\end{aligned} \tag{21}
$$

Then we can get $(K_D^N(t), K_D^I(t), K_D^R(t), K_D^M(t))$ and $(N^*(t), I^*(t), R^*(t), M^*(t))$.

Setting $\frac{\partial H^*}{\partial p_D^H(t)} = 0$, we can calculate it and obtain $P_D^*(t) = (\ p_D^H(t)^*, p_D^L(t)^*\ \ )$. Among them, $p_D^H(t)^*$ and $p_D^L(t)^*$ can be expressed as (22) and (23), shown at the bottom of the next page, respectively. Similarly, we can set $\frac{\partial H^*}{\partial p_A^H(t)} = 0$, $\frac{\partial H^*}{\partial p_A^M(t)} = 0$ to obtain $P_A^*(t) = (\ p_A^H(t)^*, p_A^M(t)^*, p_A^L(t)^*)$, among which $p_A^H(t)^*, p_A^M(t)^*$ and $p_A^L(t)^*$ can be expressed as (24-26), shown at the bottom of the next page, respectively.

TABLE 1. Comparison consequences with other literature.

Literature	Game Type	Player Type	Game Process	Decision-making Timeliness	Model Versatility	Equilibrium Solution	Application
[8]	Incomplete information static game	1	–	No consideration	Poor	Detailed	Strategy selection
[11]	Incomplete information dynamic game	2	Single-stage	No consideration	Poor	Simple	Performance evaluation
[16]	Incomplete information dynamic game	2	Single-stage	Poor	Poor	Simple	Mechanism analysis
[17]	Incomplete information dynamic game	n	Discrete Multi-stage	Poor	Good	Detailed	Strategy selection
This paper	Differential game	n	Continuous	Good	Good	Detailed	Strategy selection

In equations (22-26), $H^* = H(t, K(t), x^*, P_A^*(t), P_D^*(t))$, and $\eta\,(t) = [a\,(t) - d\,(t)$ denote the attack-defense effectiveness. When $\eta(t) > 0$, it indicates that the attack is successful at time t, that is, the defense fails. When $\eta(t) \leq 0$, it means the attack at time t is defeated, that is the defense successes. If the positive and negative attributes of $\eta(t)$ are different, $P_D^*(t)$ and $P_A^*(t)$ will have different results, which indicates that the optimal strategies of both players are strategically dependent.

B. OPTIMAL DEFENSE STRATEGY SELECTION ALGORITHM DESIGN AND ANALYSIS

Based on the above analysis, we design the optimal defense strategy selection algorithm for attack-defense differential games.

The algorithm shows that its time and space computational complexity are directly related to the number of attack and defense strategies m and n. Among them, the time complexity of the steps (1)~(8), (10) and (11) is linearly related to the number of attack-defense strategies m and n, that is $O(f^k)$. The time complexity of step (9) are exponentially related to m and n, that is $O(f^{mn})$. The required storage space to solve the algorithm depends on the network security state variable and the intermediate value of the equilibrium solution, which is linearly related to the number of attack and defense strategies m, n and the number of security states. Thus the space complexity is $O(4g(m, n))$.

Compared the method proposed in this article with other literature, the results are shown in Table 1. Our model and method can analyze the continuous and real-time attack-defense process and achieve the optimal strategy selection, which can meet the higher needs in actual network confrontation.

The player type means whether the players are divided in the model and how many types of players there are in the game. Actually, there are great differences in technical capabilities, action costs, and return targets between players, which is difficult for their opponents to grasp in detail. Therefore, it is more realistic and accurate to distinguish the players into different types for analysis. Timeliness of

$$p_D^H(t)^* = \begin{cases} \dfrac{[r_2 + K_D^R(t) - K_D^N(t)]N^*(t) + [r_2 + K_D^R(t) - K_D^I(t)]I^*(t) - \overline{e_D^L} c_D Q}{(\overline{e_D^H} - \overline{e_D^L}) c_D Q}, & \eta(t) \leq 0 \\ \dfrac{[r_1 + K_D^N(t) - K_D^I(t)]\alpha\pi I^*(t)N^*(t)/Q + [r_3 + K_D^I(t) - K_D^M(t)]I^*(t) - \overline{e_D^L} c_D Q}{(\overline{e_D^H} - \overline{e_D^L}) c_D Q}, & \eta(t) > 0 \end{cases} \tag{22}$$

$$p_D^L(t)^* = 1 - p_D^H(t)^* \tag{23}$$

$$p_A^H(t)^* = \begin{cases} \dfrac{[r_2 + K_A^N(t) - K_A^R(t)]N^*(t) + [r_2 + K_A^I(t) - K_A^R(t)]I^*(t) - \overline{e_A^L} c_A Q}{(\overline{e_A^H} - \overline{e_A^L}) c_A Q}, & \eta(t) \leq 0 \\ \dfrac{[r_1 + K_A^I(t) - K_A^N(t)]\alpha\pi I(t)N^*(t)/Q + [r_3 + K_A^M(t) - K_A^I(t)]I^*(t) - \overline{e_A^L} c_A Q}{(\overline{e_A^H} - \overline{e_A^L}) c_A Q}, & \eta(t) > 0 \end{cases} \tag{24}$$

$$p_A^M(t)^* = \begin{cases} \dfrac{[r_2 + K_A^N(t) - K_A^R(t)]N^*(t) + [r_2 + K_A^I(t) - K_A^R(t)]I^*(t) - \overline{e_A^L} c_A Q}{(\overline{e_A^M} - \overline{e_A^L}) c_A Q}, & \eta(t) \leq 0 \\ \dfrac{[r_1 + K_A^I(t) - K_A^N(t)]\alpha\pi I^*(t)N^*(t)/Q + [r_3 + K_A^M(t) - K_A^I(t)]I^*(t) - \overline{e_A^L} c_A Q}{(\overline{e_A^M} - \overline{e_A^L}) c_A Q}, & \eta(t) > 0 \end{cases} \tag{25}$$

$$p_A^L(t)^* = 1 - p_A^H(t)^* - p_A^M(t)^* \tag{26}$$

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

```
Input: Attack-Defense Differential Game Model ADDG
Output: The optimal defense strategy $P_D^*(t)$
BEGIN
1. Initialize ADDG $= (N, \Theta, B, t, x, S, f, U)$.
2. Construct defender type space $\Theta_D$ and attacker type space $\Theta_A$.
2. Construct defense strategy space DS $= (\beta_1, \beta_2, \cdots, \beta_k)$ and attack strategy space AS $= (\delta_1, \delta_2, \cdots, \delta_g)$.
3. Construct the state evolution differential equations $\dot{x}(t) = \{f_N, f_I, f_R, f_M\}$ according to equation (2).
4. Initialize the constant parameters $r_1, r_2, r_3, c_D, c_A$.
6. Establish the Hamilton functions $H(t, K_D(t), x, P_A(t), P_D(t))$ and $H(t, K_A(t), x, P_A(t), P_D(t))$ of the differential game.//According to the method in Section II and Section III, we construct Hamilton functions;
7. For defenders, calculate $K_D(t) = (K_D^x(t))^{\mathrm{T}}$ according to equations (15-18).
8. For attackers, calculate $K_A(t) = (K_A^x(t))^{\mathrm{T}}$ similarly.
9. Calculate the equation (21) in the Section III, and solve $K_D(t)$, $K_A(t)$ and $(N^*(t), I^*(t), R^*(t), M^*(t))$ based on the dynamic programming method.
10. For defenders, according to $\frac{\partial H^*}{\partial p_D^i(t)} = 0$, calculate $p_D^i(t)^*, 1 \le i \le n$.
11. For attackers, according to $\frac{\partial H^*}{\partial p_A^j(t)} = 0$, calculate $p_A^j(t)^*$, $1 \le j \le m$.
12. Return $P_D(t) = \left\{p_D^i(t)^* \,|1 \le i \le n\right\}$. //output the optimal defense strategies.
END
```

decision-making refers to the effective time of the selected optimal strategy. Only taking into consideration the one-shot confrontation process, it can be regarded as a single-stage attack-defense game, and the selected optimal strategy can only be applied to a single stage. If the attack and defense are regarded as a dynamic and multi-stage process, then we can use discrete and multi-stage game model for analysis, with the optimal strategies in each discrete stage of the game. Since the attack-defense speed in the network is accelerating and the action transitions tend to be high-frequency, defense decision-making need to be continuous and real-time to improve the timeliness of decision-making results. Otherwise, the selected optimal strategy may not adapt to the transition of attack-defense rhythm and lose its effectiveness. The differential game model introduces the time factor into the attack-defense analysis and calculates the control strategy equations with respect to time. Then we can achieve the optimal strategy selection at any time, which has better timeliness than other literature. The model versatility means whether the type set and the strategy set in the model can be extended to n. If yes, it illustrates that the model has better versatility. Otherwise, it illustrates that the model is only suitable for certain situations and has poor applicability. Equilibrium solution denotes whether the computational solution for the equilibrium is given in the work. The equilibrium of Markov differential game changes in real time, thus the solution process is more complicated. Without detailed calculation methods and steps, it will reduce the practical application value.

IV. SIMULATION EXPERIMENT AND ANALYSIS

A. DESCRIPTION OF THE EXPERIMENTAL ENVIRONMENT

By simulation experiments, we intended to verify the network attack-defense differential game model and the optimal defense strategy selection method proposed in this article. In the experiment, we applied the simulation tool used widely, Scalable Simulation Framework (SSFNet) [24], which can simulate network attack-defense scenarios with different scales and initial states by setting different parameters. In order to improve the authenticity of the simulation experiments, we utilized an autonomous system connection dataset derived from the Route Views Project referring to [25] to design the topological structure of the experimental system. The dataset used is that of 2018.6.16 (NetTFData20180616103000) and we set the number of nodes $Q = 1000$ in the simulation experiment.

Referring to [16], [17], [26], [27] and MIT's attack-defense behavior database [28], we analyzed the attack action information and classified them into (strong-intensity A_H, medium-intensity A_M, and weak-intensity A_L) three types with their average attack strength based on the attack intensity, as shown in Table 2. Similarly, the defense action information is analyzed, and the average defense strength is calculated by integrating all the indicators, as shown in Table 3.

TABLE 2. Description of the attack actions.

No.	Attack aciton	Attack strength	Attack type	Average strength
1	Remote buffer overflow	0.95	A_H	0.82
2	Install Trojan	0.8		
3	Steal account and crack it	0.7		
4	Send abnormal data to GIOP	0.5	A_M	0.45
5	LPC to LSASS process	0.4		
6	Shutdown Database server	0.45		
7	Oracle TNS Listener	0.35	A_L	0.3
8	Ftp rhost attack	0.3		
9	Sr-Hard blood	0.25		

B. EXPERIMENTAL ANALYSIS

In the experiment, we set constant parameters $r_1 = 2, r_2 = 4, r_3 = 9, c_D = 5, c_A = 4.3$. Among them, r_1, r_2, and r_3 are return coefficients, which are used to calculate the defense

TABLE 3. Description of the defense actions.

No.	Defense action	Defense strength	Defense type	Average strength
1	Limit packets from ports	0.8	D_H	0.71
2	Install Oracle patches	0.8		
3	Reinstall Listener program	0.8		
4	Uninstall delete Trojan	0.7		
5	Limit access to MDSYS.SDO_CS	0.7		
6	Renew root data	0.6		
7	Restart Database server	0.6		
8	Limit SYN/ICMP packets	0.5	D_L	0.34
9	Add physical resource	0.5		
10	Repair database	0.4		
11	Correct homepage	0.4		
12	Delete suspicious account	0.3		
13	Redeploy firewall rule and filtrate malicious packets	0.3		
14	Patch SSH on Ftp Sever	0.2		

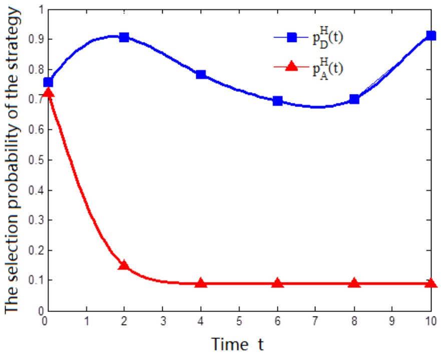


FIGURE 2. The optimal strategy control trajectory of $p_A^H(t)^*$ and $p_D^H(t)^*$.

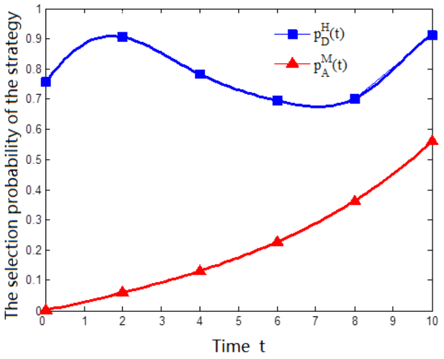


FIGURE 3. The optimal strategy control trajectory of $p_A^M(t)^*$ and $p_D^H(t)^*$.

return and attack return in the attack-defense game. c_D and c_A are the cost/utility coefficients of the defense or attack strategy, which is used to calculate the strategy execution cost. More detailed analysis can be seen in Section II. Based on the methods and conclusions in [22], we use statistical averages to set the values of return coefficients r_1, r_2, and r_3, according to the topology of the experimental system and the distribution of network nodes. Based on the method and conclusion in [16], according to the data of Table 2 and Table 3, the cost/utility coefficients of different types of strategies $c_{D_H} = 6$, $c_{D_L} = 4$, $c_{A_H} = 7$, $c_{A_M} = 4$, and $c_{A_L} = 2$ can be obtained. Thus we set $c_D = 5$ and $c_A = 4.3$ by arithmetic mean method.

The attack and defense lasts for 10 mins, that is $t \in [0, 10]$. By Matlab 2014, we can achieve the optimal defense strategy selection algorithm, and obtain the optimal strategy control trajectories of both attacker and defender, as shown in Fig. 2 - Fig. 4.

(1) As shown in Fig. 2, when t =0, the network is in the initial state with $p_A^H(0)^* = 0.72$, that is the attacker adopts a high probability 0.72 to select a strong-intensity attack strategy A_H. Then $p_A^H(t)^*$ begins to decrease rapidly, and in the attack-defense process after $t = 0.6$, the selection probability of the strong-intensity attack strategy $p_A^H(t)^* < 0.5$. Starting from $t = 3$, the probability $p_A^H(t)^*$ approaches 0.09, which basically keeps the same thereafter.

The attacker adopts a strong-intensity attack strategy A_H with a high probability during $t \in [0, 0.6]$, aiming to attack the defender with the maximum ability and implement "Blitz" in a short period of time. In this way, the attacker can maximize the number of normal nodes that transformed into the infected nodes, and attempt to make the infected nodes transform into the malfunctioned state M, which increases the real-time and expected loss of the network system performance. Because of the high execution cost of A_H, the attacker only adopts this strategy to make the defender be caught off guard in a short period of time. Then the attacker reduces the selection probability of this strategy to ensure a higher cost-effectiveness ratio. After $t = 3$, the probability of the strategy A_H remains low with $p_A^H(t)^* = 0.09$.

(2) As shown in Fig. 3, the probability that the attacker adopts a medium-intensity attack strategy A_M is increasing during $t \in [0, 3]$, but it remains at a very low level with $p_A^M(t)^* < 0.1$. After $t = 6$, the selection probability of strategy A_M increases to $p_A^M(t)^* > 0.2$. At $t = 10$, the probability to use this strategy eventually increases to $p_A^M(t)^* = 0.53$.

Considering the cost of implementing the strategy, the attacker who wants to gain an advantage in the attack-defense process, will inevitably strengthen the utilization of medium-intensity attack strategy A_M in order to obtain a better attack effect and cost-effectiveness ratio.

(3) As shown in Fig. 4, when $t = 0$, $p_A^L(t)^* = 0.28$, that is, the attacker adopts a low probability 0.28 to select the weak-intensity attack strategy A_L, when the network is in the

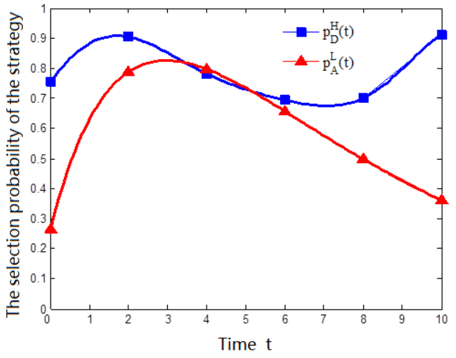


FIGURE 4. The optimal strategy control trajectory of $p_A^L(t)^*$ and $p_D^H(t)^*$.

initial state. During $t \in [0, 3]$, the probability of selecting strategy A_L increases rapidly and reaches a peak $p_A^L(t)^* = 0.81$ at time $t = 3$. In the subsequent attak and defense, the probability to select this strategy gradually decreases, and at $t = 10$, $p_A^L(t)^* = 0.38$.

In the actual network attack and defense, because of the first-mover advantage, the attacker uses the high-intensity strategy to make a sudden attack, and strives to maximize the attack effect when the defender is caught off guard, as known as the "Blitz" attack mode. So $p_A^H(t)^* \gg p_A^L(t)^*$ and $p_A^H(t)^* > 0.5$ in $t \in [0, 0.6]$. However, the raid effect can only last for a short period of time. When the defender detects and adjusts defense measures, the effect of strong-intensity attack will be significantly reduced. Taking into consideration the cost of implementing the strategy, the probability of selecting the strong-intensity attack strategy $p_A^H(t)^*$ will rapidly decrease and the probability of the weak-intensity attack strategy $p_A^L(t)^*$ will rapidly increase. Subsequently, during $t \in [3, 10]$, the attack-defense process enters a stalemate. In this phase, the attackers tend to adopt strategies A_M and A_L with relatively low attack intensity and implementation cost, to harass and tempt the defender for defense loopholes and attack priorities. At this time, $p_A^H(t)^* \ll p_A^M(t)^*, p_A^L(t)^*$.

(4) By analyzing Fig. 2-4 comprehensively, it demonstrates that the defender should select strong-intensity defense strategy D_H with a high probability $p_D^H(t)^* \geq 0.76$ as the optimal defense strategy. Because D_H has a high defense capability, and can minimize expected losses when strong-intensity attacks suddenly outbreaks, which is the best defense against "Blitz". Therefore, the probability $p_D^H(t)^*$ increases continuously during this period of time, and then peaks at 0.89 at $t = 2$.

Then the probability $p_D^H(t)^*$ gradually decreases because the attacker tends to adopt the lower-intensity strategies A_M and A_L after the raid effect disappears. At the same time, the defender starts to reduce the selection of strong-intensity defense strategy considering the defense costs. However, in order to ensure a better defensive effect, the probability $p_D^H(t)^*$ remains at a high level, with $p_D^H(t)^* > 0.67$ during $t \in [2, 7]$. After $t = 7$, the probability to select the medium-strength attack strategy increases significantly. To repair infected nodes as soon as possible and avoid the later losses, the selection probability of the strong-intensity defense strategy increases rapidly, with $p_D^H(t)^* = 0.91$ at $t = 10$.

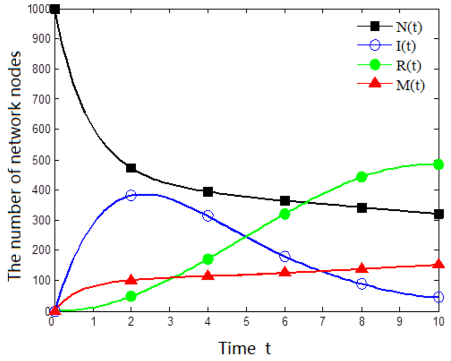


FIGURE 5. The evolution process of network nodes in different states.

In the attack-defense process, the number of network nodes in different states changes with time as shown in Fig. 5. Note that, to facilitate the evolution of nodes in different states in this experiment, the curves of the nodes' numbers in Fig. 5 are fitted by discrete data, rather than a actual continuous curve.

(5) During $t \in [0, 2]$, due to the attacker's first-mover advantage and raid effect, the attacker gains advantage in a short time. The number of infected node $I(t)$ rapidly increases, while the number of malfunctioned node $M(t)$ increases greatly. Therefore during this period of time, the number of network nodes in the normal state N has dramatically decreased, with $N(0) = 1000$ and $N(2) = 464$ decreasing by 53.6% in a short period of time. During $t \in [2, 3]$, the defense strategy effectively controlled the network attacks, and the number of infected nodes showed a downward trend. However, in the attack and defense process, the number of infected nodes will not be reduced to 0, because the attack effect cannot be completely eliminated. At time $t = 3$, the attacker maintains a low probability to select the strong-intensity attack strategy, while the defender maintains a high selection probability of the strong-intensity defense strategy. Therefore, the number of repaired nodes R significantly increases, whereas the number of malfunctioned nodes $M(t)$ increases slowly.

From the analysis of above simulation results, it shows that the attacker has the most significant attack effect during $t \in [0, 2]$, which causes the defender to suffer serious losses during this time. Then from $t = 2$, the defender controls the attack effectively, by real-time decision-making and adjustment of the optimal defense strategy. Therefore, according to the analysis of the optimal strategy trajectory, we propose the following suggestions: (1) The defender should increase defense investment in peacetime and improve defense capabilities, to avoid serious losses caused by suddenly attacked due to inadequate preparation. (2) Improve the efficiency of defense decision-making. Thus, the defender should shorten the time of defense decision-making, to achieve targeted and timely response to network attacks and avoid greater losses. (3) Facing the advance, sudden and central network attack, the defender should use proactive defense and camouflage measures, such as honeypot networks. In this way, the defender can lure and confuse the attacker's direction and goals for more emergency response times, which avoids serious losses if they are caught off guard. The optimal defense strategy selection method based on attack-defense differential game proposed in this paper realizes continuous and real-time defense decision-making, which can effectively improve the timeliness of defense decision-making, and greatly shorten the adjustment time of defense strategy. Faced with network attack deploying rapidly and changing in high-frequency, it has better practicality and guidance than the other defense decision-making methods based on traditional dynamic games.

V. CONCLUSION

Currently, attack-defense analysis based on game theory mostly assumes that both attacker and defender only conduct one-shot confrontation. Even if some scholars adopt the dynamic attack-defense game model, the network confrontation is also treated as a discrete and multi-stage process. However, in the actual network security problems, the traditional dynamic game analysis can no longer meet the actual requirements in the continuous attack and defense. Thus, we investigated the network attack-defense behavior in the continuous process and constructed the attack-defense differential game model. Then, we proposed a solution for saddle-point strategy and designed the optimal defense strategy selection algorithm. Finally, the validity of the model and method was verified by simulation experiments. Based on the analysis of experimental data, we put forward some suggestions for network defense. The research provides an effective model for attack and defense under continuous and real-time conditions, so that it can be more valuable for the selection of defense strategies.

Our future work includes researches on typical proactive defense mechanisms such as honeypot network and mobile target defense, and the analysis of the mentioned mechanism on defense response time to improve defense effectiveness. Besides, we intend to conduct the research with stochastic game and differential game to improve the application range of the model. Moreover, we intend to develop the network attack-defense efficiency and game payoff calculation methods, improving the accuracy of the calculation from the perspective of multi attributes.

ACKNOWLEDGEMENT

(Hengwei Zhang and Lv Jiang contributed equally to this work.)

REFERENCES

[1] B. Fang, "A hierarchy model on the research fields of cyberspace security technology," *Chin. J. Netw. Inf. Secur.*, vol. 1, no. 1, pp. 3961–3966, 2015.

[2] L. Gordon and M. Loeb, "Budgeting process for information security expenditures," *ACM. Commun.*, vol. 49, no. 10, pp. 121–125, 2016.

[3] J. Zhu, B. Song, and Q. Huang, "Evolution game model of offense-defense for network security based on system dynamics," *J. Commun.*, vol. 35, no. 1, pp. 54–61, 2014.

[4] Y. Wang, J. Yu, W. Qu, H. Shen, X. Cheng, and C. Lin, "Evolutionary game model and analysis methods for network group behavior," *Chin. J. Comput.*, vol. 38, no. 2, pp. 282–300, 2015.

[5] W. Jiang and B. Fang, "Defense strategies selection based on attack-defense game model," *J. Comput. Res. Develop.*, vol. 47, no. 12, pp. 818–827, 2014.

[6] J. White, J. S. Park, C. A. Kamhoua, and K. A. Kwiat, "Game theoretic attack analysis in online social network (OSN) services," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw.*, Aug. 2015, pp. 1012–1019.

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

[8] D. Yu, J. Wang, and H. Zhang, "Active defense strategy selection based on static Bayesian game," *J. Xidian Univ.*, vol. 43, no. 1, pp. 163–169, 2016.

[9] W. Lin *et al.*, "Research on active defense technology in network security based on non-cooperative dynamic game theory," *J. Comput. Res. Develop.*, vol. 48, no. 2, pp. 306–316, 2014.

[10] W. Jiang, B. X. Fang, and Z. H. Tian, "Research on defense strategies selection based on attack-defense stochastic game model," *J. Comput. Res. Develop.*, vol. 47, no. 10, pp. 1714–1723, 2013.

[11] W. Chunlei, M. Qing, and D. Yiqi, "Network survivability analysis based on stochastic game model," in *Proc. 4th Int. Conf. Multimedia Inf. Netw. Secur.*, Nov. 2012, pp. 99–104.

[12] M. Yu, C. Liu, X. Qiu, and S. Zhao, "Modelling and analysis of phishing attack using stochastic game nets," in *Proc. Int. Conf. Cyberspace Technol.*, 2016, vol. 46, no. 3, pp. 300–305.

[13] H. Zhang and D. Yu, "Network security threat assessment based on signaling game," *J. Xidian Univ.*, vol. 43, no. 3, pp. 137–143, 2016.

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

[15] S. Shen, Y. Li, and H. Xu, "Signaling game based strategy of intrusion detection in wireless sensor networks," *Comput. Math. Appl.*, vol. 62, no. 6, pp. 2404–2416, 2011.

[16] A. Dadsk, "Preventing DDoS attacks in wireless sensor networks: A repeated game theory approach," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 2, pp. 145–153, 2015.

[17] H. Zhang and T. Li, "Optimal active defense based on multi-stage attack-defense signaling game," *Acta Electronica Sinica*, vol. 45, no. 2, pp. 431–439, 2017.

[18] W. Zhuang, *Study on Emergency Decision Making of Major Projects Based on Dynamic Differential Game Theory*. Jinan, China: School Mathematics Shandong Univ., 2014.

[19] H. Fan, S. Wang, and Q. Fu, "Mathematical description for information pattern of discrete-time two-person stochastic differential games," *Acta Electronica Sinica*, vol. 42, no. 2, pp. 1355–1361, 2015.

[20] *Analysis of Malicious Code Macroscopical Behavior*. Accessed: Oct. 26, 2017. [Online]. Available: http://blog. sciencenet.cn/blog-453322-1001684.html

[21] A. Martin, *Evolutionary Dynamics: Exploring the Equations of Life*. Boston, MA, USA: Harvard Univ. Press, 2013.

[22] L. Richard and W. Joshua, "Analysis and results of the network intrusion detection evaluation," in *Proc. 19th Int. Workshop Recent Adv. Intrusion Detect*, May 2016, pp. 162–182.

[23] W. K. Y. David and A. P. Leon, *Differential Games Theory*. New York, NY, USA: Springer, 2014.

[24] *Scalable Simulation Framework*. Accessed: Feb. 16,2017. [Online]. Available: http://www.ssfnet.org

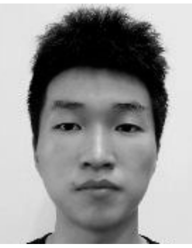
[25] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet quarantine: Requirements for containing self-propagating code," in *Proc. 20nd Annu. Conf. IEEE Comput. Commun. Societies*, San Francisco, CA, USA, Mar. 2015, pp. 1901–1910.

[26] R. Hu, X. M. Dong, and D. L. Wang, "Defense mechanism against node replication attacks and Sybil attacks in wireless sensor networks," *Acta Electronica Sinica*, vol. 43, no. 4, pp. 744–752, 2015.

[27] M. Wan, H. K. Zhang, and W. L. Shang, "An efficient approachto defend DoS attack against mapping cache under identifier-based universal network," *Acta Electronica Sinica*, vol. 43, no. 10, pp. 1941–1947, 2015.

[28] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, "CSI/FBI computer crime and security survey," in *Computer Security Institute*. San Francisco, CA, USA: IEEE Press, 2016, pp. 48–66.

HENGWEI ZHANG received the Ph.D. degree from the Zhengzhou Institute of Information Science and Technology, China, where he is currently an Associate Professor. His research interests include analysis of network attack and defense based on game theory, cloud service resource management, and intelligent system security testing and evaluation.



LV JIANG received the B.S. degree from the Zhengzhou Institute of Information Science and Technology, China. He is currently pursuing the M.S. degree with the State Key Laboratory of Mathematical Engineering and Advanced Computing. His main research interests include moving target defense and network proactive defense.

SHIRUI HUANG received the B.S. degree from the Zhengzhou Institute of Information Science and Technology, China. He is currently pursuing the M.S. degree with the State Key Laboratory of Mathematical Engineering and Advanced Computing. His main research interests include network security threat warning and active defense based on game theory.

JINDONG WANG is currently a Professor with the Zhengzhou Institute of Information Science and Technology. His research interests include information security management and resource dynamic management.

YUCHEN ZHANG received the Ph.D. degree from the Zhengzhou Institute of Information Science and Technology, China, where he is currently an Associate Professor. His research interests include network security situational awareness, and network information defense.