SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

December 2021, Vol. 64 222302:1–222302:13
https://doi.org/10.1007/s11432-020-3228-8

Differential game-based analysis of multi-attacker multi-defender interaction

Qiuyue GAO, Huici WU*, Yunfei ZHANG & Xiaofeng TAO

National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876*, China*

Received 7 September 2020/Revised 25 January 2021/Accepted 23 March 2021/Published online 18 September 2021

Abstract Due to the increasing number of wireless terminals and progressively extensive interconnections among them, interaction between the attack group and defense group is becoming a dominant security manifestation in future wireless networks. This paper focuses on the modeling and analysis of multi-attacker to multi-defender interaction. First, considering the continuous interaction between the attack group and defense group in real-time, a differential game-based multi-attacker to multi-defender interaction model is explicated with paralysis threshold introduced to reduce the ping-pong effect in paralysis. Optimal control theory is then introduced to obtain the equilibrium strategy with Hamilton best control method and a proposed optimal strategy selection algorithm for multi-attacker to multi-defender interaction. Finally, simulations are provided to demonstrate the evolutionary trajectory of optimal attack and defensive strategies and the relationship between the paralysis threshold and the group strength evolution results. Numerical results show the attackers and defenders are aggressive to strengthen their groups initially and then gradually decrease their strength to obtain ideal cost-effectiveness ratios. Moreover, increasing the defense paralysis threshold within a certain range will be more conducive to improving the defense effectiveness.

Keywords differential game, multi-attacker to multi-defender interaction, optimal control theory, Hamilton function, equilibrium strategy

Citation Gao Q Y, Wu H C, Zhang Y F, et al. Differential game-based analysis of multi-attacker multi-defender interaction. Sci China Inf Sci, 2021, 64(12): 222302, https://doi.org/10.1007/s11432-020-3228-8

1 Introduction

With the explosive increase of communication equipment in future wireless networks, the progressively pervasive interconnection among them remarkably expands network attack surfaces and introduces potential challenges to network security [1,2]. Peculiarly, attack and defense interaction in massive machine type communications (mMTC) can be easily dominated by centralized machines, which makes cooperative attack and defense become an inescapable phenomenon and the most considerable form of cybersecurity [3]. It is urgently required for defenders to take dynamic and adaptive protective measures to deal with the increasing intricacy of the attacks.

Existing studies on network attack and security defense mainly focus on the interaction between single-attacker and single-defender. The interactions between an advanced persistent threat (APT) attacker and a defender are investigated in [4, 5], where the attack interval and scan interval are respectively chosen with the consideration of subjective decisions. A multi-attacker single-defender model is constructed in [6] where jamming attack and eavesdropping attack exist simultaneously. In addition, single-attacker multi-defender models are analyzed in [7, 8] where multiple friendly jammers join to defend against the eavesdropping attacker. Nevertheless, interaction among cooperative attackers and cooperative defenders will be the most considerable form of network security while multi-attacker multi-defender interaction has rarely been analyzed in existing works. The analysis of such interaction is urgently required to provide a more comprehensive theoretical insight for network security.

* Corresponding author (email: dailywu@bupt.edu.cn)

In this paper, we investigate the strategy interaction between the attack group and defense group in a multi-attacker multi-defender scenario. Multiple attackers (resp. defenders) are allied to awaken sleeping nodes and paralyze defense (resp. attack) nodes to enhance the attack (resp. defense) group strength, which is defined as the attack (resp. defense) intensity. The group strength is a function of the number of awakened nodes, retreated nodes, and paralyzed nodes and can be varied by awakening the sleeping nodes or retreating the participating nodes. Members of one group can be paralyzed if the relative strength gap between the attack group and defense group is greater than a predefined paralysis threshold which is introduced to reduce ping-pong effect in paralysis. In order to characterize the dynamic evolution of the system security state, differential equations are formulated for the group strength of attackers and defenders. Based on which a differential game model is constructed to describe the confrontation interaction between the attack group and defense group. By Hamilton optimal control method, existence of the game equilibrium is proven and the closed-form expressions for the equilibrium strategy are derived. Furthermore, an optimal strategy selection algorithm for the attack group and defense group is proposed to achieve the equilibrium. Finally, numerical results are provided to demonstrate the evolution of strategy and strength interaction. The impact of the paralysis threshold on strength evolution is also analyzed. The main contributions in our paper are epitomized as follows.

• Considering the dynamic and continuous interaction between attack group and defense group, the multi-attacker to multi-defender interaction is investigated. A differential game-based attack and defense model is constructed where the strategy choosing process is real-time.

• Existence of the equilibrium is proven and derived by Hamilton optimal control method. An optimal strategy selection algorithm is proposed to obtain the equilibrium attack and defense strategies.

• Numerical results are provided to demonstrate the evolutions of the attack and defense interaction. It is revealed that no matter how the paralysis threshold changes, both attack and defense groups tend to increase their strength initially but gradually decrease their strength with the progress of interaction. Moreover, improving the paralysis threshold will magnify the gap between groups and accelerate the evolution process.

The remainder of this paper is organized as follows. Related work is provided in Section 2. Section 3 constructs the system model for multi-attacker to multi-defender interaction. The optimal strategy selection algorithm for the differential game model is provided in Section 4. Numerical results are analyzed in Section 5. Lastly, Section 6 concludes our paper.

2 Related work

As a theoretical method for describing players' strategic interaction, game theory can be used to model and analyze the attack and defense process in network security. Stackelberg game, Markov game, and differential game are the most commonly applied models in existing references.

Stackelberg game is generally used in physical layer attack and defense to capture the characteristic of sequential decision-making [9]. In [10], the power control of jammer and secondary user (SU) in cognitive radio network is studied by Stackelberg game, where they perform the game against the target signal-to-interference-plus-noise-ratios. Furthermore, an eavesdropper in cognitive radio network is considered where SUs adjust the interference signal power to maximize data transmission rate and prevent the eavesdropper while the primary user adjusts the service load for spectrum access of SU and maximizes security rate [7]. Ref. [6] studies the power control of sensor and jammer in network physical transmission system by Stackelberg game. Especially, the jammer interferes both eavesdropper and remote controller. Multiple eavesdroppers are considered in [11], where the source selects partners for cooperation. In the two-layer game model, the top layer and bottom layer are formulated as Stackelberg game and power selection game, respectively. Moreover, multiple friendly jammers with a single antenna are considered to defend against eavesdroppers with multi-antenna in the downlink communications [8]. From a macro perspective, Stackelberg game is used to verify the effectiveness of honeypot against spoofing attacks in cognitive radio network [12].

The above studies are one-shot games with no consideration of the dynamic characteristics of attack and defense. In a more practical scenario, a one-shot game can be developed more than once, and players' behaviours can restrict the following decision-making process [13]. As a consequence, it is more felicitous to model the attack and defense interaction of multiple stages, which is generally analyzed by the Markov game. A moving target defense game based on the Markov model is formulated in [14]. The number of

detection systems is constantly changed by the defender, and privilege levels of the attacker correspond to different states of the Markov process. In addition, a Markov secure game model for computer networks is established and by handling nonlinear programming (NLP), the equilibrium strategies are obtained [15]. In [16], the strategic security decision is modeled by a stochastic game to defend the cross-layer attackers, in which the Markov decision process and matrix games are integrated.

However, the realistic security interaction is generally time-continuous which is not premeditated in the existing Markov game models. Some differential game-based studies concentrating on the attack-defense interaction can depict the continuous and dynamic process of network state evolution and real-time strategy selection. In reference to the epidemic dynamics model, Ref. [17] constructed a normal-infected-restored-malfunctioned (NIRM) model to study the state evolution process of network security. Equilibrium strategy selection of attacker and defender is deduced by a differential game-based security model. On this basis, Ref. [18] proposed a multi-stage security model which is the synthesis of Markov game and differential game. In [19], considering devices with heterogeneous computation demands in D2D networks, a dynamic model describing the spread of malicious software is established. The equilibrium is derived and verified to be bang-bang strategy. Moreover, Ref. [20] formulated a differential game for malware-defense in which the sensor network system selects strategies and minimized the cost while the malware maximizes it. Furthermore, the saddle point strategy is proven to exist and derived as bang-bang control strategy.

Nevertheless, the emergence of a great number of communication devices will bring more severe challenges to network security, triggering cooperative attack and cooperative defense becoming an inescapable phenomenon and the most considerable form of cybersecurity in future wireless networks. It is eagerly demanded to build a game model that can explicate a multi-attacker and multi-defender, continuous, dynamic, and real-time interaction process. Therefore, a differential game-based interaction model is built in the following sections.

3 Multi-attacker to multi-defender interaction system model

The schematic diagram of the system model is shown in Figure 1, where multiple states and their transitions are introduced for the modeling of the attack and defense interaction with propagation characteristics, such as distributed denial of service (DDoS) and APT. The system contains legitimate nodes, attackers, sleeping nodes, and paralyzed nodes. The legitimate nodes are defenders that cooperate to maintain the secure and efficient work of the system. The attackers cooperate as a group to control the sleeping nodes or attack the legitimate nodes. The sleeping nodes can be awakened by legitimate nodes or attackers and then act as defenders or attackers. Paralyzed nodes are those compromised legitimate nodes and paralyzed attackers which bring loss to groups due to their abnormal actions. Each node has the ability of self-regulating to accommodate the time varying circumstances in this system.

Node state transition of this model depends on the strategies of legitimate nodes and attackers and the attack-defense interaction. In the attack and defense interaction process, both groups aim to paralyze as many nodes of each other as possible while ensuring their own optimal utility by increasing or decreasing the strength of the group. For example, sleeping nodes awakened by attackers can empower the attack group, but additional cost is brought in simultaneously. Retreating nodes from the interaction can save cost for the group, but also increasing the risk of being compromised in the interaction. The paralyzed nodes lose their competitiveness and can only bring loss to the group. Therefore, it is essential to weigh the strategy cost and group strength when making decisions, rather than blindly enhancing the group strength.

In order to concisely analyze the multi-attacker to multi-defender interaction, we first establish the state transition model for one node, detailed as Figure 2. Abstractly, a node in the system is assumed to be in one of five identity states: sleeper (S), attacker (A), defender (D), paralyzed attacker (P_A), and paralyzed defender (P_D).

S: The sleeper, acting as candidate attacker or candidate defender, does not belong to any group but it will affect the attack and defense results once awakened.

A: The participating attacker in the attack and defense interaction, who can adjust its attack behaviours to change the interaction results.

D: The participating defender in the attack and defense interaction, who can adjust its defense behaviours to change the interaction results.

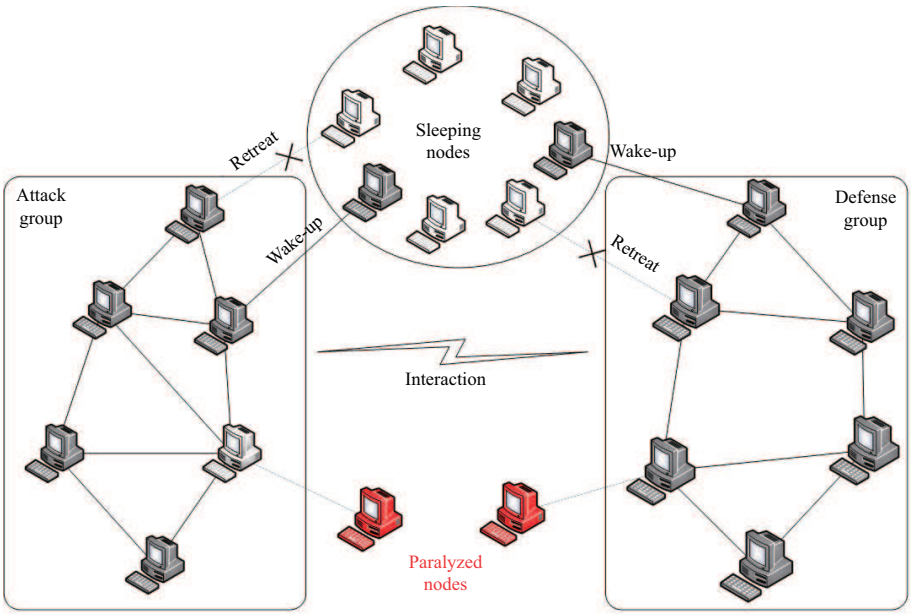

Figure 1 (Color online) Multi-attacker to multi-defender interaction system model.

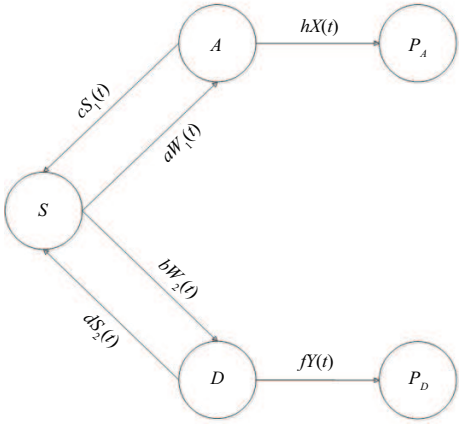

Figure 2 State transitions of one node.

P_A: The paralyzed attacker, which is compromised by the defense group, can no longer contribute to the attack group.

P_D: The paralyzed defender, which is compromised by the attack group, can no longer contribute to the defense group. In the attack and defense interaction process, the emergence of paralysis results from the strength disparity between the two groups. And this disparity is quantified by the paralysis threshold defined later.

Being one of the most important elements that affect the results of attack and defense interaction, the node strategies will determine the transition probability among the above five states. Conversely, the interaction results also have influence on the selection of attack and defense strategies. As shown by the arrow marks in Figure 2, the strategies contain wake-up strategy and retreat strategy. The state transitions of nodes at time t are as follows.

$S \to A$: When the attack group needs to increase strength to empower itself, the sleepers are awakened with intensity $W_1(t)$ and transformed into participating attackers. We introduce a parameter a to weigh the wake-up intensity of the attack group.

$A \to S$: When the attack group needs to decrease strength to save the cost, the attackers are retreated with intensity $S_1(t)$ and transformed into sleepers. We introduce a parameter c to weigh the retreat intensity of the attack group.

$A \to P_A$: When the strength of defense group is more dominant than that of attack group, the attackers

are paralyzed with intensity $X(t)$ and transformed into paralyzed attackers. We introduce a parameter h to weigh the paralysis intensity of attack group, which is positively correlated with the protection degree of defense measures.

$S \to D$: When the defense group needs to increase strength to empower itself, the sleepers are awakened with intensity $W_2(t)$ and transformed into participating defenders. We introduce a parameter b to weigh the wake-up intensity of the defense group.

$D \to S$: When the defense group needs to decrease strength to save the cost, the defenders are retreated with intensity $S_2(t)$ and transformed into sleepers. We introduce a parameter d to weigh the retreat intensity of the defense group.

$D \to P_D$: When the strength of the attack group is more dominant than that of the defense group, the defenders are paralyzed with intensity $Y(t)$ and transformed into paralyzed defenders. We introduce a parameter f to weigh the paralysis intensity of the defense group, which is positively correlated with the damage degree of attack measures.

To describe the dynamic strength evolution process, we define $A(t)$ and $D(t)$ as the group strength of attackers and defenders, respectively. Combining the above definitions and the state transitions in Figure 2, the evolution of group strength is represented as follows: the awakened nodes caused by wake-up strategy minus the retreated nodes caused by retreat strategy minus the paralyzed nodes. Thus, the evolution process of group strength is expressed as differential equations (1a) and (1b):

$$\dot{A(t)} = \frac{\mathrm{d}A(t)}{\mathrm{d}t} = aW_1(t) - cS_1(t) - hX(t), \tag{1a}$$

$$\dot{D(t)} = \frac{\mathrm{d}D(t)}{\mathrm{d}t} = bW_2(t) - dS_2(t) - fY(t). \tag{1b}$$

At $t = 0$, the initial strength condition of the attack group and defense group for the differential equations is given by (2a) and (2b), respectively:

$$A(0) = A_0, \tag{2a}$$

$$D(0) = D_0. \tag{2b}$$

The paralysis intensities $X(t, m)$ and $Y(t, n)$ are functions of the relative strength gap between the attack group and defense group. In order to reduce the ping-pong effect, an attack paralysis threshold m and a defense paralysis threshold n are introduced. When the ratio of $D(t) - A(t)$ and $A(t)$ exceeds m, the attackers will be paralyzed with intensity $X(t, m)$. Similarly, when the ratio of $A(t) - D(t)$ and $D(t)$ exceeds n, the defenders will be paralyzed with intensity $Y(t, n)$. Therefore, the paralysis intensities $X(t, m)$ and $Y(t, n)$ are given by (3a) and (3b), respectively:

$$X(t,m) = \begin{cases} D(t) - A(t), & \dfrac{D(t) - A(t)}{A(t)} \geqslant m, \\ 0, & \text{otherwise}, \end{cases} \tag{3a}$$

$$Y(t,n) = \begin{cases} A(t) - D(t), & \dfrac{A(t) - D(t)}{D(t)} \geqslant n, \\ 0, & \text{otherwise}. \end{cases} \tag{3b}$$

In (3a) and (3b), the paralysis intensities $X(t, m)$ and $Y(t, n)$ increase with respect to their opponent strength and decrease with respect to their own strength. In particular, when $m = n = 0$, once there is a disparity in strength, the weak group will be paralyzed, and there is no delay judgment caused by paralysis thresholds.

4 Optimal multi-attacker multi-defender strategy selection

In this section, the strength evolution differential equations in Section 3 are applied to construct the differential game-based multi-attacker to multi-defender interaction model. On the basis of proving the existence of game equilibrium, an optimal strategy selection algorithm for multi-attacker to multi-defender interaction is proposed to obtain the equilibrium strategy.

4.1 Differential game-based multi-attacker to multi-defender interaction model

Definition 1. Differential game model of multi-attacker to multi-defender interaction is expressed as (P, B, t, F, C, g, U), where

• $P = \{P_A, P_D\}$ denotes the set of players in the game, P_A and P_D represent the participating attackers and participating defenders, respectively.

• $B = \{W, S\}$ denotes the action set of attackers and defenders, W and S denote to wake-up nodes and to retreat nodes, respectively.

• $t \in [0, T]$ denotes the time in the attack and defense interaction process. With the consideration of continuous interaction between attack and defense groups in real-time, the strategies, group strength and their utility are all with respect to time t.

• $F = \{A(t), D(t)\}$ denotes the group strength of attackers and defenders at time t. $A(t)$ is the strength of attack group and $D(t)$ is the strength of defense group.

• $C = \{C_A(t) = \{W_1(t), S_1(t)\}, C_D(t) = \{W_2(t), S_2(t)\}\}$ is the control strategy set of attackers and defenders. $W_1(t)$ and $S_1(t)$ are the wake-up strategy and retreat strategy of attack group, respectively. $W_2(t)$ and $S_2(t)$ are the wake-up strategy and retreat strategy of defense group, respectively.

• $g = \{g_A(t), g_D(t)\}$ represents the strength evolution function of attack group and defense group, where $g_A(t) = \dot{A}(t)$, $g_D(t) = \dot{D}(t)$ with the initial group strength conditions $A(0) = A_0$ and $D(0) = D_0$. More details can be seen in (1a), (1b), (2a), and (2b).

• $U = \{U_A(t), U_D(t)\}$ represents the set of utility functions. $U_A(t)$ and $U_D(t)$ represent the utility functions of attack group and defense group, respectively.

For the attack group, participating nodes $A(t)$ provides positive while paralyzed nodes $X(t, m)$ provide negative impacts on the attack utility U_A. For simplicity, we define $X(t, m) \triangleq [D(t) - A(t)] \cdot \varepsilon(D(t) - A(t) - mA(t))$ where $\varepsilon(t)$ is a step function defined as $\varepsilon(t) = \left\{ \begin{smallmatrix} 0, & t < 0 \\ 1, & t \geqslant 0 \end{smallmatrix} \right.$. Considering that awakening nodes $W_1(t)$ brings cost to the group while retreating nodes $S_1(t)$ saves cost for the group, we define the strategy cost as $\frac{\alpha}{2}W_1^2(t) - \frac{\beta}{2}S_1^2(t)$, where α and β are the cost coefficients of wake-up and retreat strategy, respectively. In addition, the benefit and cost are ordinarily square form of state variables and strategy functions with constant term $\frac{1}{2}$ [21, 22]. With the above definitions and analysis, the instant utility for the attack group $u_A(t)$ is expressed as

$$u_A(t) = \frac{\gamma}{2}[A^2(t) - [D(t) - A(t)]^2 \cdot \varepsilon\left(D(t) - A(t) - mA(t)\right)] - \left[\frac{\alpha}{2}W_1^2(t) - \frac{\beta}{2}S_1^2(t)\right], \tag{4a}$$

where γ is the profit-loss coefficient for the attack group. Then, the total utility of the attack group is obtained by integrating over time $[0, T]$, i.e., $U_A = \int_0^T u_A(t)\mathrm{d}t$.

Similarly, the instant utility for the defense group $u_D(t)$ is expressed as

$$u_D(t) = \frac{\varphi}{2}[D^2(t) - [A(t) - D(t)]^2 \cdot \varepsilon(A(t) - D(t) - nD(t))] - \left[\frac{\eta}{2}W_2^2(t) - \frac{\xi}{2}S_2^2(t)\right], \tag{4b}$$

where φ is the profit-loss coefficient for the defense group. η and ξ are the cost coefficients of wake-up and retreat strategy, respectively. Then, the total utility of the defense group is $U_D = \int_0^T u_D(t)\mathrm{d}t$.

In (4a) and (4b), the profit-loss coefficients γ and φ can represent the importance of nodes such as degree centrality in the scenario considering network topology, network resources owned in the network resource competition scenario or privacy data stored in the privacy theft scenario. The cost coefficients α, β, η, and ξ are related to the difficulty of strategy implementation. It can be seen that the value of utility functions $u_A(t)$ and $u_D(t)$ increase with respect to the group strength $A(t)$ and $D(t)$ and decrease with respect to the number of paralyzed nodes $X(t, m)$ and $Y(t, n)$. With the implementation of wake-up strategies $W_1(t)$ and $W_2(t)$, the strategy cost and strength of both groups increase. As a result, the change of the value of utility functions cannot be determined. Similarly, with the implementation of retreat strategies $S_1(t)$ and $S_2(t)$, the strategy cost and strength of both groups decrease. Therefore, the change of the value of utility functions can also not be determined. This makes it necessary for players to weigh the constraints between strength and cost.

After the definition and analysis of utility functions of attack and defense groups, the game is carried out between the two groups to maximize their own utility through strategy adjustment. Therefore, the optimization goal for attack group and defense group is to find the optimal control strategies $\{W_1^*(t), S_1^*(t)\}$

Table 1 Summary of symbols

Symbol	Description
$A(t)/D(t)$	Strength of attack/defense group
$W_1(t)/W_2(t)$	Wake-up strategy of attack/defense group
$S_1(t)/S_2(t)$	Retreat strategy of attack/defense group
$X(t,m)/Y(t,n)$	Paralysis of attack/defense group
m/n	Paralysis threshold of attack/defense group
a/b	Wake-up coefficient of attack/defense group
c/d	Retreat coefficient of attack/defense group
h/f	Paralysis coefficient of attack/defense group
γ/φ	Profit-loss coefficient of attack/defense group
α/η	Wake-up cost coefficient of attack/defense group
β/ξ	Retreat cost coefficient of attack/defense group

and $\{W_2^*(t), S_2^*(t)\}$ to satisfy (5a) and (5b), respectively. Table 1 summarizes the commonly used symbols.

$$\max_{W_1(t),S_1(t)} U_A\left(W_1(t), S_1(t), W_2^*(t), S_2^*(t)\right), \tag{5a}$$

$$\max_{W_2(t),S_2(t)} U_D\left(W_1^*(t), S_1^*(t), W_2(t), S_2(t)\right). \tag{5b}$$

4.2 Optimal strategy solving for the multi-attacker to multi-defender interaction

In this subsection, we firstly define the equilibrium strategy and prove the existence of it. Then, we derive the closed-form expressions for the equilibrium based on the optimal control method. Finally, an optimal strategy selection algorithm is proposed to obtain the optimal attack and defense strategies.

Definition 2. Equilibrium strategy. If the strategy pair $(C_A^*(t), C_D^*(t))$ satisfies (6a) and (6b), then $(C_A^*(t), C_D^*(t))$ is defined as the equilibrium strategy.

$$\forall C_A(t), U_A\left(C_A^*(t), C_D^*(t)\right) \geqslant U_A\left(C_A(t), C_D^*(t)\right), \tag{6a}$$

$$\forall C_D(t), U_D\left(C_A^*(t), C_D^*(t)\right) \geqslant U_D\left(C_A^*(t), C_D(t)\right). \tag{6b}$$

To obtain the equilibrium strategy, Hamilton optimal method is applied [23]. Combining (1a) and (4a), the Hamilton function of attack group H_1 is defined as (7) through the introduction of the joint state variables $\lambda_1(t)$ and $\lambda_2(t)$.

$$\begin{aligned}
&H_1(t, C_A(t), C_D(t), \lambda_1(t), \lambda_2(t), m, n)\\
&= u_A(t) + \lambda_1(t) g_A(t) + \lambda_2(t) g_D(t)\\
&= \frac{\gamma}{2}[A^2(t) - [D(t) - A(t)]^2 \cdot \varepsilon\left(D(t) - A(t) - mA(t)\right)] - \frac{\alpha}{2} W_1^2(t) + \frac{\beta}{2} S_1^2(t)\\
&\quad + \lambda_1(t)[aW_1(t) - cS_1(t) - h[D(t) - A(t)] \cdot \varepsilon\left(D(t) - A(t) - mA(t)\right)]\\
&\quad + \lambda_2(t)[bW_2(t) - dS_2(t) - f[A(t) - D(t)] \cdot \varepsilon\left(A(t) - D(t) - nD(t)\right)].
\end{aligned} \tag{7}$$

Combining (1b) and (4b), the Hamilton function of defense group H_2 is defined as (8) through the introduction of the joint state variables $\mu_1(t)$ and $\mu_2(t)$.

$$\begin{aligned}
&H_2(t, C_A(t), C_D(t), \mu_1(t), \mu_2(t), m, n)\\
&= u_D(t) + \mu_1(t) g_A(t) + \mu_2(t) g_D(t)\\
&= \frac{\varphi}{2}[D^2(t) - [A(t) - D(t)]^2 \cdot \varepsilon(A(t) - D(t) - nD(t))] - \frac{\eta}{2} W_2^2(t) + \frac{\xi}{2} S_2^2(t)\\
&\quad + \mu_1(t)[aW_1(t) - cS_1(t) - h[D(t) - A(t)] \cdot \varepsilon(D(t) - A(t) - mA(t))]\\
&\quad + \mu_2(t)[bW_2(t) - dS_2(t) - f[A(t) - D(t)] \cdot \varepsilon(A(t) - D(t) - nD(t))].
\end{aligned} \tag{8}$$

Lemma 1. Equilibrium strategy $(C_A^*(t), C_D^*(t))$ exists in the differential game-based multi-attacker to multi-defender interaction model.

Proof. By Pontryagin maximum theorem, the joint state variables $\lambda_1(t)$, $\lambda_2(t)$, $\mu_1(t)$, and $\mu_2(t)$ satisfy

$$\begin{cases} H_1(t, C_A^*(t), C_D^*(t), \lambda_1(t), \lambda_2(t), m, n) \geqslant H_1(t, C_A(t), C_D^*(t), \lambda_1(t), \lambda_2(t), m, n), \\ H_2(t, C_A^*(t), C_D^*(t), \mu_1(t), \mu_2(t), m, n) \geqslant H_2(t, C_A^*(t), C_D(t), \mu_1(t), \mu_2(t), m, n). \end{cases} \tag{9}$$

Based on the strength evolution differential equations (1a), (1b) and the initial strength conditions (2a), (2b), the differential equations for group strength can be written as

$$\begin{cases} \overset{\bullet}{A^*}(t) = aW_1^*(t) - cS_1^*(t) - hX^*(t, m), \quad A^*(0) = A_0, \\ \overset{\bullet}{D^*}(t) = bW_2^*(t) - dS_2^*(t) - fY^*(t, n), \quad D^*(0) = D_0. \end{cases} \tag{10}$$

And according to the characteristics of Hamilton functions, the joint state variables are solved by

$$\begin{cases} \overset{\bullet}{\lambda_1}(t, m, n) = -\dfrac{\partial H_1\left(t, C_A^*(t), C_D^*(t), \lambda_1(t), \lambda_2(t), m, n\right)}{\partial A^*(t)}, \\ \overset{\bullet}{\lambda_2}(t, m, n) = -\dfrac{\partial H_1\left(t, C_A^*(t), C_D^*(t), \lambda_1(t), \lambda_2(t), m, n\right)}{\partial D^*(t)}, \\ \overset{\bullet}{\mu_1}(t, m, n) = -\dfrac{\partial H_2\left(t, C_A^*(t), C_D^*(t), \mu_1(t), \mu_2(t), m, n\right)}{\partial A^*(t)}, \\ \overset{\bullet}{\mu_2}(t, m, n) = -\dfrac{\partial H_2\left(t, C_A^*(t), C_D^*(t), \mu_1(t), \mu_2(t), m, n\right)}{\partial D^*(t)}. \end{cases} \tag{11}$$

Therefore, from (9)–(11), it can be proven that our multi-attacker to multi-defender interaction game model has equilibrium strategy according to Theorem 1 in [17]. With the definition in (11), the joint state variables λ_1, λ_2, μ_1, and μ_2 can be deduced as Lemma 2.

Lemma 2. The joint state variables are deduced in (12) and (13) for different attack and defense results, where the terminal state conditions are $\lambda_1(T) = 0$, $\lambda_2(T) = 0$, $\mu_1(T) = 0$, and $\mu_2(T) = 0$.

When $D(t) - A(t) \geqslant mA(t)$, i.e., the attack group is paralyzed and $X(t, m) \geqslant 0$,

$$\begin{aligned} &\overset{\bullet}{\lambda_1}(t, m, n) = -\gamma D(t) - h\lambda_1(t, m, n), \\ &\overset{\bullet}{\lambda_2}(t, m, n) = \gamma D(t) - \gamma A(t) + h\lambda_1(t, m, n), \\ &\overset{\bullet}{\mu_1}(t, m, n) = -h\mu_1(t, m, n), \\ &\overset{\bullet}{\mu_2}(t, m, n) = -\varphi D(t) + h\mu_1(t, m, n). \end{aligned} \tag{12}$$

When $A(t) - D(t) \geqslant nD(t)$, i.e., the defense group is paralyzed and $Y(t, n) \geqslant 0$,

$$\begin{aligned} &\overset{\bullet}{\lambda_1}(t, m, n) = -\gamma A(t) + f\lambda_2(t, m, n), \\ &\overset{\bullet}{\lambda_2}(t, m, n) = -f\lambda_2(t, m, n), \\ &\overset{\bullet}{\mu_1}(t, m, n) = \varphi A(t) - \varphi D(t) + f\mu_2(t, m, n), \\ &\overset{\bullet}{\mu_2}(t, m, n) = -\varphi A(t) - f\mu_2(t, m, n). \end{aligned} \tag{13}$$

Proof. Please refer to Appendix A.

Based on the joint state variables, the optimal strategies of the attack group and defense group are given by Theorem 1.

Theorem 1. The equilibrium strategies of the differential game-based multi-attacker to multi-defender interaction model are given by

$$\begin{aligned} &W_1^*(t) = \frac{a}{\alpha}\lambda_1(t, m, n), \quad S_1^*(t) = \frac{c}{\beta}\lambda_1(t, m, n), \\ &W_2^*(t) = \frac{b}{\eta}\mu_2(t, m, n), \quad S_2^*(t) = \frac{d}{\xi}\mu_2(t, m, n). \end{aligned} \tag{14}$$

Proof. According to the Hamilton functions of attack and defense groups in (7) and (8), calculate Hamiltonian partial derivations for attack and defense strategies and make them zero like (15a)–(15d).

$$\frac{\partial H_1}{\partial W_1(t)}_{|W_1(t)=W_1^*(t)} = -\alpha W_1^*(t) + a\lambda_1(t,m,n) = 0, \tag{15a}$$

$$\frac{\partial H_1}{\partial S_1(t)}_{|S_1(t)=S_1^*(t)} = \beta S_1^*(t) - c\lambda_1(t,m,n) = 0, \tag{15b}$$

$$\frac{\partial H_2}{\partial W_2(t)}_{|W_2(t)=W_2^*(t)} = -\eta W_2^*(t) + b\mu_2(t,m,n) = 0, \tag{15c}$$

$$\frac{\partial H_2}{\partial S_2(t)}_{|S_2(t)=S_2^*(t)} = \xi S_2^*(t) - d\mu_2(t,m,n) = 0. \tag{15d}$$

The optimal equilibrium strategies of the differential game-based model are attained through shifting terms, which are bound up with $\lambda_1(t,m,n)$, $\lambda_2(t,m,n)$, $\mu_1(t,m,n)$, and $\mu_2(t,m,n)$.

The above analysis demonstrates that the attack and defense strategies, states, and results are all functions with respect to time. The selection of attack and defense strategies has an impact on the network states and ulteriorly affects the interaction results. Conversely, the attackers and defenders will select the strategies in the light of attack and defense results. The indivisible connection among these elements results in the difficulty of obtaining the equilibrium strategy. As a result, Algorithm 1 provides the method to select the optimal strategies for attack and defense groups.

Firstly, at any time $t \in [0,T]$, compute the current attack group and defense group strength $A(t)$ and $D(t)$ based on the dynamic equations (1a), (1b), the initial conditions of group strength (2a), (2b) and the paralysis results (3a), (3b). Then, $\lambda_1(t,m,n)$, $\lambda_2(t,m,n)$, $\mu_1(t,m,n)$, and $\mu_2(t,m,n)$ are solved according to the calculation of group strength as Lemma 2. Finally, on the basic of Theorem 1, the optimal strategies for attack and defense groups $W_1^*(t)$, $S_1^*(t)$, $W_2^*(t)$, and $S_2^*(t)$ can be obtained from $\lambda_1(t,m,n)$ and $\mu_2(t,m,n)$. More details are shown in Algorithm 1.

Algorithm 1 Optimal strategy selection for attack and defense groups

Input: Differential game model (P,B,t,F,C,g,U). Initial group strength: $A(0)$, $D(0)$. Initial strategies: $W_1(0)$, $S_1(0)$, $W_2(0)$, $S_2(0)$. Paralysis thresholds: m, n. Coefficients of differential game model: α, β, γ, η, φ, ξ, a, c, b, d, f, h. Joint state variables: $\lambda_1(T)$, $\lambda_2(T)$, $\mu_1(T)$, $\mu_2(T)$.

Output: Optimal control strategies for attack and defense groups: $W_1^*(t)$, $S_1^*(t)$, $W_2^*(t)$, $S_2^*(t)$.

For $t \in [0,T]$

1. Compute the strength of attacker group and defender group $A(t)$ and $D(t)$ via (1a), (1b), (2a), (2b), (3a), and (3b);
2. Substitute the group strength $A(t)$ and $D(t)$ into (12) and (13);
3. Solve the joint state variables $\lambda_1(t,m,n)$, $\lambda_2(t,m,n)$, $\mu_1(t,m,n)$, and $\mu_2(t,m,n)$ via (12) and (13);
4. Substitute the joint state variables $\lambda_1(t,m,n)$, $\lambda_2(t,m,n)$, $\mu_1(t,m,n)$, and $\mu_2(t,m,n)$ into (14);
5. Obtain and return the optimal strategies $W_1^*(t)$, $S_1^*(t)$, $W_2^*(t)$, and $S_2^*(t)$ via (14).

5 Numerical results

Numerical results evaluate the differential game-based multi-attacker to multi-defender interaction model. Firstly, we discuss the effect of equilibrium strategies on the strength evolution. Moreover, the relationship between the paralysis threshold and strength evolution results is demonstrated.

In the numerical analysis, the change of parameter setting has little effect on the analysis of attack and defense results, as shown in Figure 3. Therefore, we choose the parameter configurations with obvious line characteristics in the following analysis for convenience's sake. The wake-up coefficients are set as $a = b = 0.04$. The paralysis coefficients are set as $f = h = 0.025$. The retreat coefficients are set as $c = d = 0.039$. The wake-up strategy cost coefficients are set as $\alpha = \eta = 1$. The retreat strategy cost coefficients are set as $\beta = \xi = 1.2$. The profit-loss coefficients are set as $\gamma = \varphi = 5$. In addition, the model in this paper is an initial-state-fixed and final-state-free model, so the choice of strategies and evolution process will vary with the end of time. 40 time units are taken as an example of the time duration in the following analysis for that there is no longer a turning point worth analyzing after 40, during which both groups reduce their strength until reaching 0.

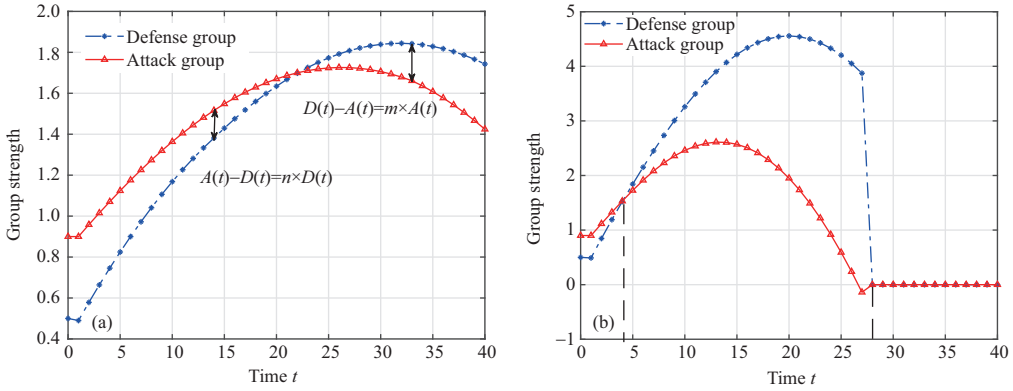

Figure 3 (Color online) The evolution trajectory of attack-defense states. (a) With wake-up coefficient 0.04; (b) with wake-up coefficient 0.05.

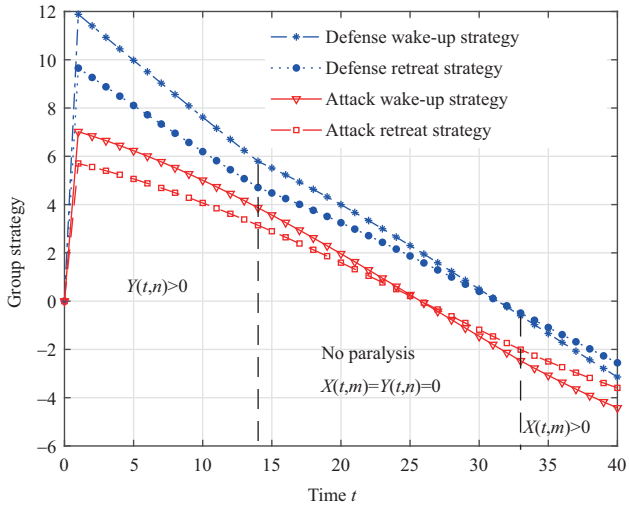

Figure 4 (Color online) The evolution trajectory of attack and defense strategies.

5.1 Evolution trajectory of attack and defense states

The initial strength of attack group is set as $A(0) = 0.9$, and the initial strength of defense group is set as $D(0) = 0.5$. Since the group strength is a mathematical variable concept in our model, the unit of it is not specified and can be detailed and defined in specific scenarios, such as the total number of terminals and the total computation resources occupied. Given the same paralysis thresholds $m = n = 0.1$, the evolution trajectory of attack and defense states and optimal strategies are demonstrated as Figures 3 and 4, respectively. The detailed analysis of the attack and defense interaction process is as follows.

0–1 s: At the beginning, neither group has implemented their strategies yet, and the strength of the attack group has reached the level to paralyze the defense group. Thus the strength of the attack group remains unchanged while the defense group sustains a certain degree of paralysis and its strength decreases.

1–14 s: The defense group starts increasing strength to catch up with the attack group with a higher rate, reaching a level of no paralysis in about 14 s. During this period, the attackers strengthen the attack group with a lower rate than the defenders to keep the dominant position and obtain benefits.

14–33 s: Starting from around 14 s, the defense group gradually reduces the growth rate of strength. At around 22 s, the attack group and defense group are equal in strength. During this phase, neither group is paralyzed, and the changes in strength are slightly smooth. But as time goes on and cost accumulates, at about 25 and 31 s, the retreat rate of attack group and defense group begins to surpass the wake-up rate, respectively. Both groups convert strategies so as to cut down the strategy cost and guarantee the effectiveness, resulting in a slight reduction of their strength.

33–40 s: The defense group strength has reached the level that can paralyze the attack group, causing the strength of the attack group to decrease at a high speed at around 33 s. And the defense group also

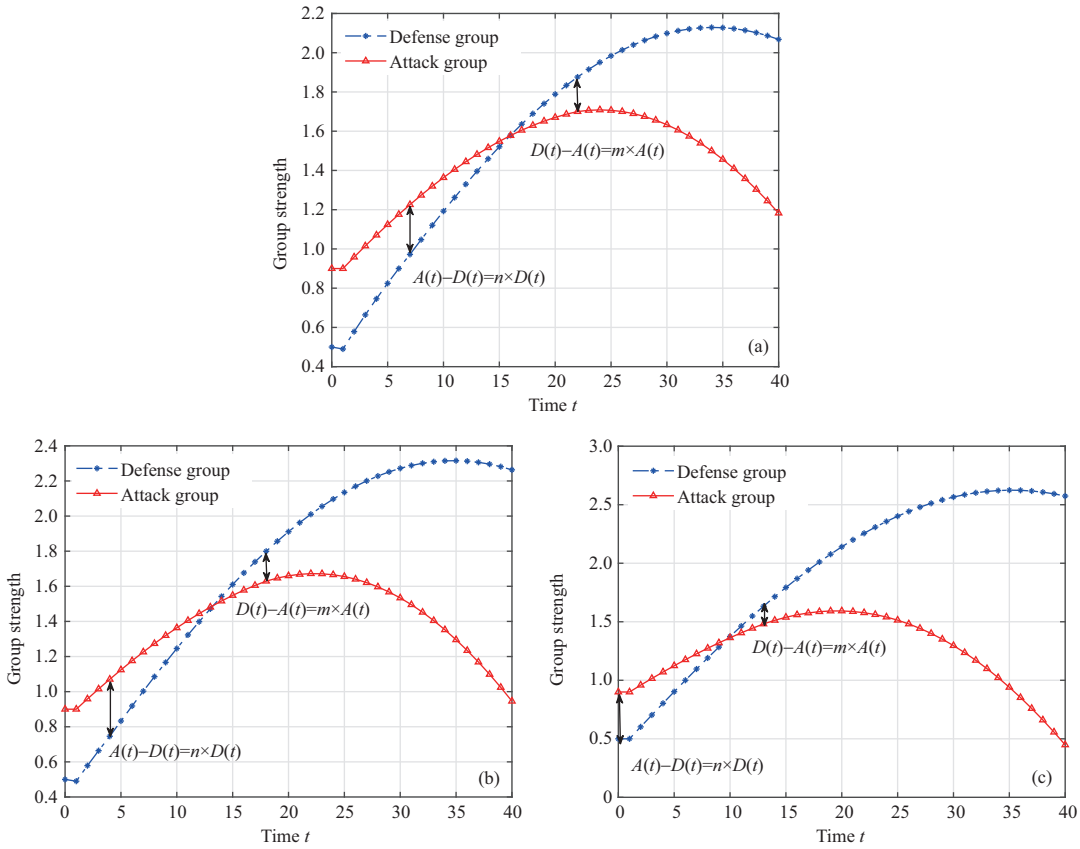

Figure 5 (Color online) The evolution trajectory of attack and defense states when (a) $n = 0.3$, (b) $n = 0.5$, and (c) $n > 0.8$.

begins to decrease the strength for a high cost-benefit ratio.

As shown in Figure 3, most of the time in the attack and defense interaction process, attackers and defenders prefer to strengthen their groups with varying intensities no matter at an advantage or disadvantage. The behaviours taken by the predominant group can be interpreted as continuing the triumphant pursuit. And the inferior one will strengthen its group with a higher rate to reduce the disparity between groups. However, both players tend to decrease their strength for cost-saving during the later attack and defense period. Therefore, it is suggested that the attackers and defenders should enforce effectual strategies as early as possible to occupy dominant positions. Otherwise, with the accumulation of cost, the loss may not be remedied in the later period.

As shown in Figure 4, at any time in the attack and defense interaction process, both groups implement the combination of wake-up strategy and retreat strategy with different intensities. From a more practical perspective, in the attack and defense interaction with large-scale nodes, the identities of nodes are predicted to transform frequently. The nodes have the probability of attacking opponents and have the capability of self-protection at the same time. And the continual transformations may lead to tremendous high-frequency and short-term attack-defense actions.

5.2 Paralysis threshold

In Subsection 5.1, all the parameters are constant, but the real parameters could be changeable, e.g., the paralysis threshold. Therefore, the paralysis threshold is considered to be controllable in this subsection, and its impact on the node state evolution results is analyzed. The results with defense paralysis threshold n set as 0.3, 0.5, 0.8 and beyond are provided in Figure 5, respectively.

Comparing Figures 3 and 5, it can be intuitively noticed that as the paralysis threshold of the defense group increases, the trends of the two curves of group strength become more and more polarized. Specifically, as Table 2 shows, the larger the paralysis threshold value within a certain range, the faster the strength growth rate of the defense group, the greater the peak value of the defense group strength, the earlier the time point when the two groups have the same strength, and the earlier the time when the

Table 2 Comparison of key data points

Item	$n = 0.1$	$n = 0.3$	$n = 0.5$	$n > 0.8$
Defense group being paralyzed (s)	0–14	0–7	0–4	–
Strategy switching point 1 (s)	14	7	4	0
Same strength point (s)	22	16	14	10
Strategy switching point 2 (s)	33	22	18	13
Attack group being paralyzed (s)	33–40	22–40	18–40	13–40
Difference in peak strength	0.118	0.42	0.644	1.032

attack group becomes paralyzed. Therefore, appropriately increasing the paralysis threshold can keep the strength at a higher growth level on its own, and can make the opponent's strength shrink faster.

However, when the paralysis threshold exceeds a certain critical value, no matter how it changes, the attack and defense process will no longer change. This is because neither group is paralyzed at the beginning. Only when there exists paralysis will the change of the paralysis threshold have a direct impact on up and down of the strength. And there is no doubt that the implementation of the strategy is another factor influencing the group strength. It is the synergy between the interaction results and strategies that makes the change of the paralysis threshold differently affect the attack and defense process. But when there is no paralysis, the change of the paralysis threshold will not affect the variety of group strength. Only the implementation of the strategy affects the increase and decrease of the group strength, and the unilateral role of the strategy makes the attack and defense process no longer generate differences.

In summary, within the critical range, the larger the paralysis threshold, the more conducive to widening the gap between groups. However, once the paralysis threshold exceeds a certain value, the interaction process will no longer change. Therefore, improving the paralysis threshold conduces to quickly expanding the gap with the opponent.

6 Conclusion

The interaction among cooperative attackers and cooperative defenders has been investigated considering the attacker group and defender group. We have formulated a differential game-based multi-attacker to multi-defender interaction model in which both groups implement optimal strategies to maximize their own utility functions. By introducing optimal control theory, an optimal strategy selection algorithm for multi-attacker to multi-defender interaction is proposed with Hamilton functions to obtain the equilibrium strategy. Finally, numerical results have evaluated how the interaction strategies and results are mutually restricted. It has shown that both the attack group and defense group are aggressive to strengthen their groups at the beginning but gradually decrease their strength afterward to guarantee the optimal utility. Moreover, the results have also verified that the paralysis threshold has a profound impact on the interaction results. Raising the paralysis threshold within a certain range is more conducive to launching a short-term but high-intensity interaction.

Future work can focus on the multi-attacker and multi-defender interaction model with long-term and multi-stage for that most of the parameters in this paper are fixed and can only satisfy the attack and defense requirements in a short time. Therefore, our model may be extended to a multi-stage model in order to fit the time-varying characteristic of long-term attack and defense interaction. In addition, the diverse attributes of heterogeneous devices existing in the networks and the accessibility of communication links can be considered so as to improve the genuineness of the differential game model.

Acknowledgements This work was supported in part by Beijing Municipal Natural Science Foundation (Grant No. 4212005), in part by National Natural Science Foundation of China (Grant Nos. 61932005, 61901051).

References

1 Tariq F, Khandaker M, Wong K, et al. A speculative study on 6G. 2019. ArXiv:abs/1902.06700
2 Giordani M, Polese M, Mezzavilla M, et al. Toward 6G networks: use cases and technologies. IEEE Commun Mag, 2020, 58: 55–61
3 Gao Q Y, Wu H C, Zhang J Z, et al. Multi-attacker multi-defender interaction in mMTC networks via differential game. In: Proceedings of IEEE/CIC International Conference on Communications in China (ICCC), 2020. 1250–1255
4 Xiao L, Xu D J, Mandayam N B, et al. Attacker-centric view of a detection game against advanced persistent threats. IEEE Trans Mobile Comput, 2018, 17: 2512–2523
5 Xu D J, Xiao L, Mandayam N B, et al. Cumulative prospect theoretic study of a cloud storage defense game against advanced persistent threats. In: Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2017. 541–546

6 Wang K, Yuan L, Miyazaki T, et al. Jamming and eavesdropping defense in green cyber-physical transportation systems using a stackelberg game. IEEE Trans Ind Inf, 2018, 14: 4232–4242
7 Yao Y J, Zhou W Y, Kou B H, et al. Dynamic spectrum access with physical layer security: a game-based jamming approach. IEEE Access, 2018, 6: 12052–12059
8 Wu H C, Tao X F, Han Z, et al. Secure transmission in MISOME wiretap channel with multiple assisting Jammers: maximum secrecy rate and optimal power allocation. IEEE Trans Commun, 2017, 65: 775–789
9 Jia L L, Xu Y H, Sun Y M, et al. Stackelberg game approaches for anti-jamming defence in wireless networks. IEEE Wirel Commun, 2018, 25: 120–128
10 Xiao L, Chen T H, Liu J L, et al. Anti-jamming transmission stackelberg game with observation errors. IEEE Commun Lett, 2015, 19: 949–952
11 Zhang N, Cheng N, Lu N, et al. Partner selection and incentive mechanism for physical layer security. IEEE Trans Wirel Commun, 2015, 14: 4265–4276
12 Ahmed I K, Fapojuwo A O. Stackelberg equilibria of an anti-jamming game in cooperative cognitive radio networks. IEEE Trans Cogn Commun Netw, 2018, 4: 121–134
13 Agah A, Das S K. Preventing DoS attacks in wireless sensor networks: a repeated game theory approach. Int J Netw Secur, 2007, 5: 145–153
14 Chowdhary A, Sengupta S, Huang D, et al. Markov game modeling of moving target defense for strategic detection of threats in cloud networks. 2018. ArXiv:abs/1812.09660
15 Wang C C, Shi C H, Wang C, et al. An analyzing method for computer network security based on Markov game model. In: Proceedings of IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016. 454–458
16 Huang K X, Zhou C J, Qin Y Q, et al. A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems. IEEE Trans Ind Electron, 2020, 67: 2371–2379
17 Zhang H W, Jiang L, Huang S R, et al. Attack-defense differential game model for network defense strategy selection. IEEE Access, 2019, 7: 50618–50629
18 Huang S R, Zhang H W, Wang J D, et al. Markov differential game for network defense decision-making method. IEEE Access, 2018, 6: 39621–39634
19 Zhang L T, Xu J. Differential security game in heterogeneous device-to-device offloading network under epidemic risks. IEEE Trans Netw Sci Eng, 2020, 7: 1852–1861
20 Shen S G, Li H, Han R, et al. Differential game-based strategies for preventing malware propagation in wireless sensor networks. IEEE Trans Inform Forensic Secur, 2014, 9: 1962–1973
21 Guo R, Chang G R, Qin Y H, et al. DG-based active defense strategy to defend against DDoS. In: Proceedings of International Conference on Multimedia and Ubiquitous Engineering (MUE 2008), 2008. 191–196
22 Wang M X, Xu H T, Yang S S, et al. Non-cooperative differential game based energy consumption control for dynamic demand response in smart grid. China Commun, 2019, 16: 107–114
23 Bressan A. Noncooperative differential games. Milan J Math, 2011, 79: 357–427

Appendix A Proof of Lemma 2

When $D(t) - A(t) \geqslant mA(t)$, the Hamiltonian of attack group can be represented as

$$\begin{aligned}
&H_1(t, C_A(t), C_D(t), \lambda_1(t), \lambda_2(t), m, n)\\
&= \frac{\gamma}{2}\{A^2(t) - [D(t) - A(t)]^2\} - \frac{\alpha}{2}W_1^2(t) + \frac{\beta}{2}S_1^2(t) + \lambda_2(t)[bW_2(t) - dS_2(t)] + \lambda_1(t)[aW_1(t) - cS_1(t) - hD(t) + hA(t)]\\
&= -\frac{\gamma}{2}D^2(t) + \gamma A(t)D(t) - \lambda_1(t)hD(t) + \lambda_1(t)hA(t) - \frac{\alpha}{2}W_1^2(t) + \frac{\beta}{2}S_1^2(t) + \lambda_2(t)[bW_2(t) - dS_2(t)] + \lambda_1(t)[aW_1(t) - cS_1(t)]. \qquad \text{(A1)}
\end{aligned}$$

The Hamiltonian of defense group can be represented as

$$\begin{aligned}
&H_2(t, C_A(t), C_D(t), \mu_1(t), \mu_2(t), m, n)\\
&= \frac{\varphi}{2}D^2(t) - \frac{\eta}{2}W_2^2(t) + \frac{\xi}{2}S_2^2(t) + \mu_1(t)[aW_1(t) - cS_1(t) - hD(t) + hA(t)] + \mu_2(t)[bW_2(t) - dS_2(t)]\\
&= \frac{\varphi}{2}D^2(t) - \mu_1(t)hD(t) + \mu_1(t)hA(t) - \frac{\eta}{2}W_2^2(t) + \frac{\xi}{2}S_2^2(t) + \mu_1(t)[aW_1(t) - cS_1(t)] + \mu_2(t)[bW_2(t) - dS_2(t)]. \qquad \text{(A2)}
\end{aligned}$$

Combining (A1) and (A2), Eq. (12) can be obtained by solving the partial derivative for group strength.

When $A(t) - D(t) \geqslant nD(t)$, the Hamiltonian of attack group can be represented as

$$\begin{aligned}
&H_1(t, C_A(t), C_D(t), \lambda_1(t), \lambda_2(t), m, n)\\
&= \frac{\gamma}{2}A^2(t) - \frac{\alpha}{2}W_1^2(t) + \frac{\beta}{2}S_1^2(t) + \lambda_1(t)[aW_1(t) - cS_1(t)] + \lambda_2(t)[bW_2(t) - dS_2(t) - fA(t) + fD(t)]\\
&= \frac{\gamma}{2}A^2(t) - \lambda_2(t)fA(t) + \lambda_2(t)fD(t) - \frac{\alpha}{2}W_1^2(t) + \frac{\beta}{2}S_1^2(t) + \lambda_1(t)[aW_1(t) - cS_1(t)] + \lambda_2(t)[bW_2(t) - dS_2(t)]. \qquad \text{(A3)}
\end{aligned}$$

The Hamiltonian of defense group can be represented as

$$\begin{aligned}
&H_2(t, C_A(t), C_D(t), \mu_1(t), \mu_2(t), m, n)\\
&= \frac{\varphi}{2}\{D^2(t) - [A(t) - D(t)]^2\} - \frac{\eta}{2}W_2^2(t) + \frac{\xi}{2}S_2^2(t) + \mu_1(t)[aW_1(t) - cS_1(t)] + \mu_2(t)[bW_2(t) - dS_2(t) - fA(t) + fD(t)]\\
&= \varphi A(t)D(t) - \frac{\varphi}{2}A^2(t) - \mu_2(t)fA(t) + \mu_2(t)fD(t) - \frac{\eta}{2}W_2^2(t) + \frac{\xi}{2}S_2^2(t) + \mu_1(t)[aW_1(t) - cS_1(t)] + \mu_2(t)[bW_2(t) - dS_2(t)]. \qquad \text{(A4)}
\end{aligned}$$

Combining (A3) and (A4), Eq. (13) can also be obtained by solving the partial derivative for group strength.

With initial boundary conditions $A(0) = A_0$, $D(0) = D_0$, the joint state variables need to be fixed in the final states. Thus, the boundary conditions $\lambda_1(T) = 0$, $\lambda_2(T) = 0$, $\mu_1(T) = 0$, $\mu_2(T) = 0$ should be satisfied.