Reliability Engineering and System Safety 216 (2021) 107958

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Attack-defense game for critical infrastructure considering the cascade effect

Fu Chaoqi [a,*], Gao Yangjun [a], Zhong Jilong [b,**], Sun Yun [a], Zhang Pengtao [a], Wu Tao [a]

[a] *Equipment Management and UAV Engineering College, Air Force Engineering University, Xi'an 710038, China*
[b] *National Innovation Institute of Defense Technology , PLA Academy of Military Science, Beijing, 100071, China*

ARTICLE INFO

Keywords:
Complex networks
Cascade effect
Attacker-defender game
Equilibrium solutions

ABSTRACT

The important status of critical infrastructure makes it a target of attacks in the new era. Based on game theory, we analyze the offensive and defensive issues of critical infrastructure from a network perspective, and we propose a network offensive and defensive game model considering the impact of the cascade effect. We first establish a two-player game model for an attacker and a defender acting simultaneously. The nodes are categorized to achieve the transformation of the focus of the game from decision-making for the nodes to resource allocation, thereby simplifying the calculation space of the network game strategy. Both pure strategy and mixed strategy are carried out for the theoretical analysis and simulation of four kinds of optimization problems. With the pure strategy, the initial decision equilibrium is that the attacker's strategy is to attack the Equal Cost-Effective ratio nodes (ECE nodes), and the defender defends the High Cost-Efficient ratio nodes (HCE nodes). At this point, the defender's payoff is 0. With the mixed strategy, different optimization problems have different equilibrium solutions. In particular, the attacker adds a new equilibrium solution for the strategy with the cascading effect, which is related to the structural properties of the network. For the defender, the strategy is different when maximizing his/her own profit or minimizing the attacker's benefit. This can explain how the attacker and the defender can achieve a win-win situation.

1. Introduction

Critical infrastructure networks such as transportation, communication, and power networks play a vital role in modern society [1,2]. Any failure in these critical infrastructure networks will bring daily work and life to a standstill. The important status of critical infrastructure makes it a target of terrorist attacks in the new era and even a military target in wartime [3-5]. Examples include the terrorist attacks of 9/11 in 2001 and the rail junction of Chattanooga, which became a key military objective in the U.S. Civil War. The large scale of an infrastructure network, the complex interaction of various components, the limited protection resources, and the intelligence of saboteurs have caused safety research on critical infrastructure to face huge difficulties [6-10]. Complex network theory [11-15] provides a new method for the study of the interaction between critical infrastructure components from a holistic perspective, and game theory's [16-20] rigorous mathematical foundations offer an appropriate framework to model the confrontations between intelligent adversaries.

Traditionally, the method of probabilistic risk assessment (PRA) [3] is often used to analyze critical infrastructure security issues. This method is suitable for analyzing non-deliberate threats, but it cannot solve the problem of deliberate attacks and effective defense [4]. In recent years, game theory has been introduced to solve adversarial problems. Hausken et al. [21] reviewed and summarized 129 research references on system offense and defense, and they classified these issues based on three aspects: system structures, defense measures, attack tactics and circumstances. Brown et al. [1] built an attacker-defender game model for which the defender's object was to minimize the total operating costs, and the attacker's aim was to maximize the costs by attacking some components. Guan et al. [8] studied a multi-target attacker-defender game with budget constraints, and they found that defense resources should be allocated to the most valuable targets, and the attacker preferred to spread the resources to attack more targets. Zhang et al. [22-24] studied the multi-target defender-attacker games under the conditions of risk preference and multiple attack types, and further studied multi-target defender-attacker games by using a quantal

[*] Corresponding author.
[**] co-Corresponding author.
E-mail addresses: fuchaoqi2011@163.com (F. Chaoqi), z jilong@sina.cn (Z. Jilong).

https://doi.org/10.1016/j.ress.2021.107958
Received 7 February 2021; Received in revised form 10 August 2021; Accepted 16 August 2021
Available online 18 August 2021

response model, which gives a closer resource allocation to the real allocation than the game theoretic model does.

Chen et al. [25] studied the game between an N defender and an M attacker. The risk attitude of the attacker and the cooperative relationship between the attacker and the defender had a great influence on the result. Nochenson et al. [26] proposed an agent-based attacker-defender game in a computer network in which the attacker tried to maximize the amount of damage he/she caused, and the defender tried to minimize his/her loss subject to cost constraints. However, the targets in these studies were treated as independent targets, and their interrelationships were not considered [27-35]. Hausken et al. [31] studied the interdependence probability between two targets and the influence of a variety of system characteristics on the player's efforts. The game of multi-state systems under the influence of interdependence has also been studied [32]. The defender can take two defense methods, separation and protection, and this model can provide a reference for the study of partial failures of node functions. Zhang et al. [33] studied the resource allocation among multiple targets for a defender-attacker game with false targets considered. The general conclusion was that the optimal solution and the corresponding payoffs were highly related to the parameters. In order to optimize resource allocation in interdependent security issues, Zhuang et al. [34,35] studied the equilibrium strategy of multiple interdependent defenders, and a model was developed to evaluate the impact of wrong choices on stability.

Complex networks provide a new perspective for the analysis of a complex system; a critical infrastructure system is treated as a whole, and the value of each component depends not only on itself but also on its neighbors. Li et al. [36,37] defined the strategies and payoffs based on the topology structure of an infrastructure system. Two typical strategies were studied, and it was found that there was a critical value for cost-sensitive parameters that made the defender's strategy change between the target strategy and the random strategy. Furthermore, they studied the equilibrium solution with the Stackelberg game model [38]. Zeng et al. [39] proposed a Stackelberg game with asymmetric information, and the results showed that disclosing false information to the attacker yielded a higher equilibrium payoff than revealing complete information. Wu et al. [40] studied the interception analysis of the three-level game theory of an urban water pipe network. The worst-case disruption impact due to intentional attacks could be significantly mitigated by deploying protective resources over critical reservoirs. Shan et al. [41] use game theory to model attacks and defenses of smart grids at three levels, find that the defender's best response is not only a function of direct attacks but also of the spread from connected networks. However, in the network, the failure of one or a few nodes would cause other nodes to fail due to the coupling relationship between the nodes, and then produce a cascading effect, which would eventually lead to the collapse of a considerable number of nodes or even the entire network. This phenomenon was cascading failure. A large amount of the research results for complex networks have shown that the damage caused by cascading failure is far greater than the impact on the topology structure [42-45]. Additionally, the spread of cascading effects is more concealed than the structural damage and more difficult to protect. None of the above research studies about the attack-defense game of critical infrastructure networks have considered cascading failures.

In this study, we take a network science perspective to evaluate the attack-defense performance under the influence of the cascade effect. Being positioned within the classification structure provided by [21], the structure of the system studied in this research is composed of networks and interdependent systems, the defense measure is protection, and the attack tactics and circumstances are a combination of intentional and unintentional influences. The contribution of this research is threefold. (1) Considering the cascading impact, we propose a new network attack and defense model to study a game for which two participants act simultaneously. All of the nodes are divided into two types based on the cost-effectiveness ratio. The focus of the game is the resource allocation of the two types of nodes. The offensive and defensive decisions of each node are determined randomly, and the failure modes of the nodes include three types (i) attacked nodes without defense, (ii) cascading failed nodes, and (iii) isolated nodes off the network. (2) Both pure strategy and mixed strategy are carried out for the theoretical analysis and simulation of four kinds of optimization problems. The equilibrium solutions of the four optimization problems with the pure strategy rule are consistent. For the mixed strategy, the offensive and defensive parties will adopt different strategies for different optimization goals. (3) The attacker adds a new equilibrium strategy to the destruction of the network under the influence of the cascade, which is related to the structural properties of the network.

The rest of the paper is organized as follows. In Section 2, the network model and the attack-defense game model are introduced, and targets are classified. The analysis of the Nash equilibrium of the offense and defense strategy with pure strategy is described in Section 3. Section 4 describes a theoretical analysis of the four kinds of optimal combination problems with the mixed strategy. Section 5 describes the simulation experiments conducted for the attack-defense game on complex networks. Section 6 concludes the work.

2. Attacker-Defender game on network model

(1) NETWORK CASCADING FAILURE MODEL

In abstract terms, the infrastructures are a network that is formalized in terms of a simple undirected graph $G = (V,E)$, $V = \{v_1, v_2, \cdots, v_n\}$ is a set of nodes representing each infrastructure, and $E = \{e_1, e_2, \cdots, e_m\}$ is a set of edges representing the connection between the nodes. There are many cascading failure modes [21, 31, 32, 42, and 46], and the load-capacity model in Reference [46] is studied here. The node load is used to define the workload undertaken by a node in the network, such as the water flow per unit time of the node in the water network and the traffic flow in the transportation network. The load L_i of node v_i is correlated with its link degree k_i as $L_i = k_i^{\theta}$, and θ is the load parameter. When a node fails, the load is reassigned to its neighboring nodes according to the preferential distribution rule $\Delta L_{ij} = (L_i L_j)/\sum_{k\in\Gamma_i} L_k$, where ΔL_{ij} is the redistribution of the load from the failed node v_i to a functioning node v_j, and Γ_i is the set of nodes adjacent to the failed node v_i. The capacity is the maximum amount of work that the node can undertake, which can be divided into two parts, one is the normal load L_i assumed by the node v_i, and the other is the redundant capacity ΔC_i used to resist uncertain risks. The relationship between the capacity and the load satisfies$C_i = \alpha + \beta L_i = L_i + \Delta C_i$, and $\alpha$and $\beta$are the tolerance coefficients. If the redistributed load ΔL_i exceeds the redundant capacity $\Delta C_i$of nodev_i, it will be invalidated and cause a new energy shock. However, if the node resists the impact of the redistributed load, the redistributed load will disappear by disconnecting the edge in time. To simplify the model, we assume that there is a sequence of node failures, so we do not consider the superposition of the redistributed energy caused by multiple nodes.

Obviously, in the load-capacity model, the interdependence between two nodes is clear (the result whether one node will fail or not due to the redistributed load of another node), and the uncertainty comes from the combination of failed nodes, which will affect the redistributed load received by the node v_i, and thus affect the state of node v_i. The cascading failure model for the load-capacity model is different from the model in the references [31,32,47,48]. In the latter model, when a node fails, the interdependent nodes must have a risk probability that they will fail. What is clear between interdependent nodes is the probability of failure, but the result is uncertain.

(1) ATTACKER-DEFENDER GAME MODEL

In this article, two players are considered to simultaneously select nodes on the network as targets for attack and defense. The players know nothing about each other's strategies, and the game is a single shot game. When a node is attacked, it is removed from the network unless it is also selected as a defensive node. If the node is defended, the cascading effect is also eliminated. It is assumed that all information about the network is completely known to both players, and there is full knowledge about the opponent. Therefore, the attacker and the defender are playing at the same level. Fig. 1 shows a diagram of the node failure classification after the network is attacked.

In order to reflect the relevance and heterogeneity of nodes in the network, we choose the model described in Reference [29] to define the values of the nodes and their offensive and defensive costs according to the characteristics of the network topology. First, we defined the value of the node v_i corresponds to the load $L_i = k_i^\theta$. The value of a node is one of the important indicators of the decision-making of the attackers and defenders, and this value can be understood with its equivalent economic value. In the extreme case where $\theta = 0$, the value of each node is homogeneous. $\theta > 0$ reflects the difference of each node value based on the degree value. The cost of node v_i in attack and defense is a linear function of the value L_i, and $c_i^A = q_A k_i^\theta$and $c_i^D = q_D k_i^\theta$ are the attack cost and the defense cost of node v_i, respectively. $q_A$is the attack-cost-sensitive parameter, and q_D is the defense-cost-sensitive parameter. The payoff of the attacker destroying node v_i is $b_i^A = \sum\limits_{j \in \Upsilon_i} q_A k_j^\theta$, and $\Upsilon_i$is the set of failed nodes and isolated nodes caused by the attacking node v_i. The payoff of the defender is $b_i^D = q_A k_i^\theta$ if and only if the attacker's attack against node v_i is defended by the defender. The attack and defense game problems of both sides are expressed as:

$$\begin{array}{ll} Attacker: & \max\limits_{x_i \in S^A y_i \in S^D} B^A \ \ or \min\limits_{x_i \in S^A y_i \in S^D} B^D \\ Defender: & \max\limits_{x_i \in S^A y_i \in S^D} B^D \ \ or \min\limits_{x_i \in S^A y_i \in S^D} B^A \end{array} \begin{cases} x_i = 0 \ or \ 1 \\ y_i = 0 \ or \ 1 \end{cases}, \tag{1}$$

where$S^A$and $S^D$are attack and defense strategies, respectively. If node i is attacked, $x_i = 1$; otherwise, $x_i = 0$. The defender's behavior y_i is the same. B^A is the total payoff of the attacker, which is the sum of the values of all failed and isolated nodes for strategies$S^A$and S^D. B^D is the total payoff from a successful defense for strategiesS^A andS^D. The purpose of the game is to maximize one's own payoff or to minimize the opponent's payoff. Therefore, there are four sets of optimized problems: 1)$Attacker: \min B^D$, $Defender: \max B^D$; 2)$Attacker: \min B^D$, $Defender: \min B^A$; 3) $Attacker: \max B^A$, $Defender: \min B^A$; 4) $Attacker: \max B^A$, $Defender: \max B^D$.

In contrast to the previous model, our model takes into account the cascading effect, which causes a deviation between the attack cost and the benefit of some nodes. This also produces a significant change in the equilibrium solution of the game. For the attacker cost$c_i^A$to attack node v_i and to obtain the paybackb_i^A, the cost-effective ratio of node v_i is $r_i = b_i^A / c_i^A = \sum\limits_{j \in \Gamma_i} k_j^\theta / k_i^\theta$, where $r_i \geq 1$. Therefore, all of the nodes are divided into two categories: one category is called the high cost-efficient ratio nodes (HCE), which satisfy $r_i > 1$. The other category is called the equal cost-effective ratio nodes (ECE), which satisfy $r_i = 1$. For the HCE nodes, the higher the value of r_i, the more the attention paid. Therefore, the HCE nodes can be deliberately attacked from large to small according tor_i. However, the ECE nodes have the same appeal, so they have an equal chance of being attacked or defended, which can be achieved through a random process. Therefore, players do not pay attention to the decision-making of each node, and the focus of the game is converted to the resource allocation of two types of nodes, which greatly simplifies the calculation space of the offensive and defensive network game analysis. The available resources of the attacker and defender are defined as$TC_A$and TC_D, which are a function of the total load $TC = \sum_{i=1}^N k_i^\theta$, and N is the total number of nodes in the network. The offensive and defensive resources can be armed forces, equivalent capital/technology investment, or money. This reflects the resources invested by both offensive and defensive parties to achieve their destructive (protection) purposes. We appropriately abstract and simplify the attack and defense resources, which are universal approaches in current game research, and which will not lose generality.

3. Pure strategy solution model

The structural characteristics of the most natural and artificial networks conform to scale-free attributes. Therefore, we choose the scale-free network model as the research object [49], and the degree distributions follow$p(k) \sim k^{-\lambda}$, where λ is the degree exponent. The attack-defense model is biased towards the defender, as shown in Fig. 2, and the attacker's payoff is limited by the defender's available resources, although structural damage can produce some additional benefits.

We consider the most typical game scenario where the attacker and the defender have the same available resources $TC_A = TC_D = \sum\limits_{i \in HCE} k_i^\theta$, both equal to the total value of all HCE nodes. Additionally, $TC_A = TC_D = p{*}TC = p{*}\sum_{i=1}^N k_i^\theta$, where$p < 0.5$means that the total cost is less than half of the total network load. It is assumed that the attack and defense cost-sensitive parameters satisfy $q_D = q_A = 1$. Thus, the attitudes of the attacker and the defender on network nodes can be divided into HCE nodes and ECE nodes. Other situations can also be obtained

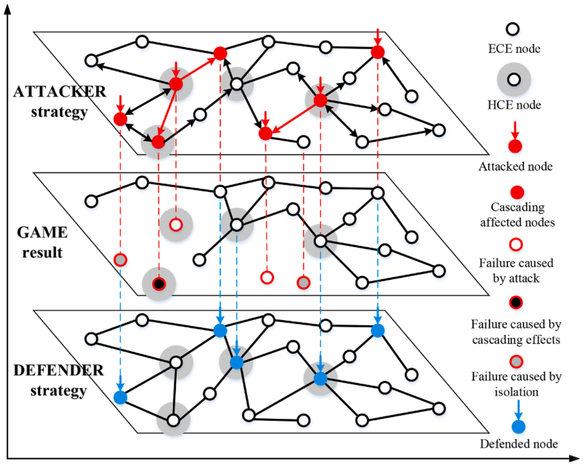


FIG. 1. Schematic diagram of attacker-defender game in the network (The red edges indicate the overload energy flow that can cause cascade failure).

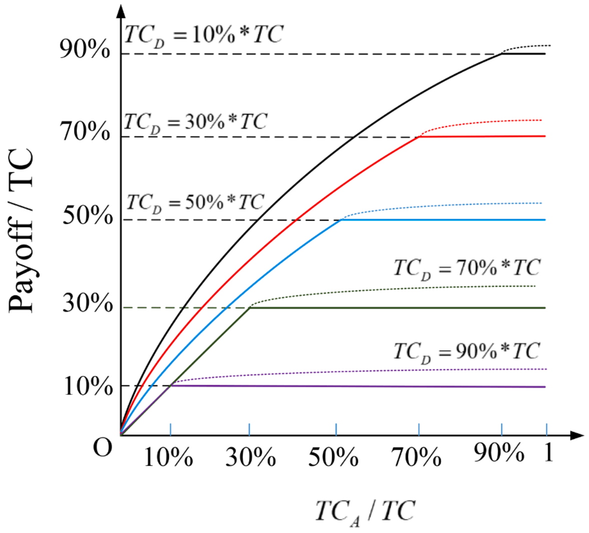


FIG. 2. Ideal relationship between $TC_A$and payoff under the restriction of TC_D.

with a similar analysis.

The payoff matrix with pure strategy in the attacker-defender game is shown in Fig. 3. Sets $\Pi_1$and$\Pi_2$in combination b and c in Fig. 3(a) are both for all failed nodes, including the nodes that fail due to cascading and isolated nodes off the network. Reference [15] found that a scale-free network was vulnerable to nodes with large degrees. Therefore, $\sum_{i\in\Pi_i} k_i^\theta \geq \sum_{i\in HCE} k_i^\theta$. $\Pi_A$andΠ_D in combination d in Fig. 3(a) are the sets of nodes that are successfully attacked and successfully defended, $0 \leq \sum_{i\in\Pi_A} k_i^\theta or \sum_{i\in\Pi_D} k_i^\theta \leq \sum_{i\in HCE} k_i^\theta$. Fig. 3(b) shows the simulation results for different strategy combinations. The simulation results of the four combinations of a, b, c, and d are consistent with the theoretical results in Fig. 3(a). Obviously, there are no dominant strategies for both attacker and defender, therefore, there is no pure-strategy equilibrium in this case.

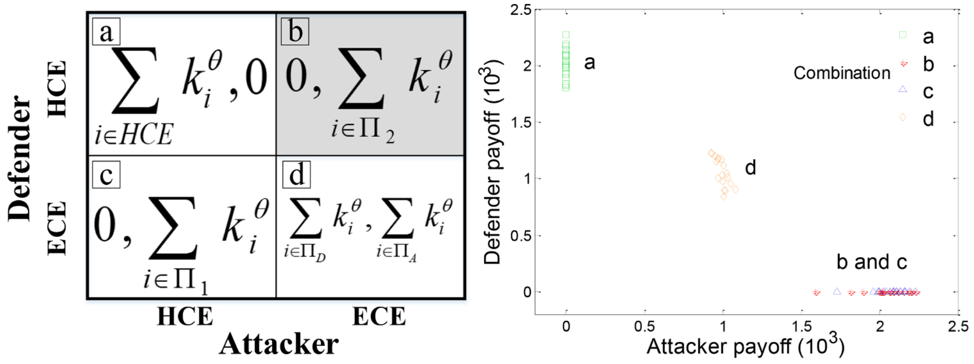
However, for the defender, the strategy of defending the HCE nodes can enable him to obtain the maximum payoff $\sum_{i\in HCE} k_i^\theta$and the minimum payoff 0. However, the strategy of defending the ECE nodes can enable him to obtain the maximum payoff $\sum_{i\in\Pi_D} k_i^\theta$, which is less than $\sum_{i\in HCE} k_i^\theta$. The minimum payoff is also 0. Therefore, according to the principle of maximum maximization $\underset{y_i\in S^D}{max}\ \underset{x_i\in S^A}{max}\ B^D$, the best option for the defender is to defend the HCE nodes. The same conclusion can be obtained from the perspective of minimizing the attacker's payoff, $\underset{y_i\in S^D}{min}\ \underset{x_i\in S^A}{min}\ B^A$.

For the attacker, the minimum payoff for attacking the HCE nodes is 0, while the minimum payoff for attacking the ECE nodes is $\sum_{i\in\Pi_A} k_i^\theta$, and according to the principle of maximum minimization $\underset{x_i\in S^A}{max}\ \underset{y_i\in S^D}{min}\ B^A$, the best option for the attacker is to attack the ECE nodes. According to the analysis of minimizing the defender's payoff, the maximum payoff of the defender when the HCE nodes are attacked is $\sum_{i\in HCE} k_i^\theta$, and the maximum payoff of the defender when the ECE nodes are attacked is $\sum_{i\in\Pi D} k_i^\theta$. The latter is smaller than the former, and according to the principle of minimum maximization $\underset{x_i\in S^A}{min}\ \underset{y_i\in S^D}{max}\ B^D$, the best option for the attacker is to attack the ECE nodes.

Therefore, in the attack and defense game with pure strategy, for all four optimization problems, the initial decision results should all appear in combination b, the strategy of the attacker is to attack the ECE nodes, and the defender defends the HCE nodes.

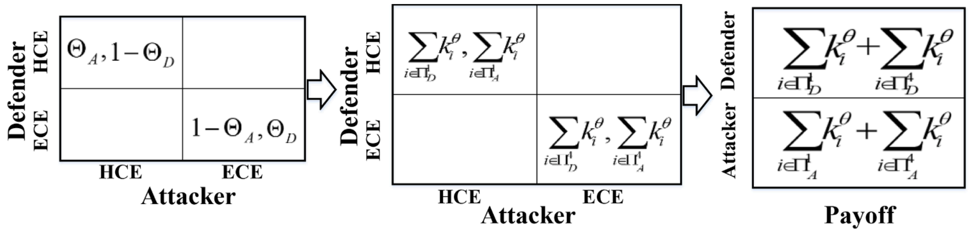
4. Mixed strategy solution model

As previously analyzed, the defender should have a greater advantage. However, the result with pure strategy is not a satisfactory result. Resources are indivisible with pure strategy, so attackers and defenders can only invest their resources in one of two categories: high value (HCE) and equal value (ECE), which limits the effective use of resources. Next, we analyze the impact of the "mixed strategy", which is different from the standard mixed strategy (in which binary options are played randomly). The "mixed strategy" in this article is based on the expression of pure strategy. In a mixed strategy, the resources are divisible; that is, the resource allocation strategies of the offensive and defensive parties are not limited to one of ECE or HCE, and offensive and defensive resources can be arbitrarily allocated to different types of targets (ECE nodes and HCE node). In this case, the defender will obtain different results. The mixed strategy tendency of the defenders and the coping



(a) Theoretical payoff matrix (b) Simulation payoff results

FIG. 3. Payoff result of the attacker-defender game with pure strategy.


Defender
HCE
ECE
$\Theta_A, 1-\Theta_D$
$1-\Theta_A, \Theta_D$
HCE
ECE
Attacker
Defender
HCE
ECE
$\sum_{i\in\Pi_D^1} k_i^\theta, \sum_{i\in\Pi_A^1} k_i^\theta$
$\sum_{i\in\Pi_D^1} k_i^\theta, \sum_{i\in\Pi_A^1} k_i^\theta$
HCE
ECE
Attacker
Defender
Attacker
$\sum_{i\in\Pi_D^1} k_i^\theta + \sum_{i\in\Pi_D^1} k_i^\theta$
$\sum_{i\in\Pi_A^1} k_i^\theta + \sum_{i\in\Pi_A^1} k_i^\theta$
Payoff

(a) Resource allocation (b) Payoffs under HCE and ECE nodes (c) Total payoffs

FIG. 4. Payoff with mixed strategy (Θ_A, Θ_D).

Table 1
Main notations used in this section.

Notation	Description	Notation	Description
Decision Variables			
Θ_A	Proportion of available resources with which the attacker attacks the HCE nodes.	Θ_D	Proportion of available resources with which the defender protects the ECE nodes.
Objective Functions			
B^A	Payoffs for the attacker.	B^D	Payoffs for the defender.
Parameters			
TC	Total load of the network, which is also the total value of the network.	TC_A	Available resources of the attacker, which are proportional to TC.
TC_D	Available resources of the defender, which are proportional to TC.	p	Ratio of invested resources to total value
$\overline{B}^D_{ECE}$	Average payoff obtained by the defender when the attacked ECE nodes are all defended.	$\overline{B}^D_{HCE}$	Average payoff obtained by defender when the attacked HCE nodes are all defended.
B^A_{HCE}	Payoffs of failed HCE nodes to attackers.	B^A_{ECE}	Payoffs of failed ECE nodes to attackers.
D	Number of HCE nodes	A	Number of ECE nodes
N	Total number of network nodes	$\overline{C}_T$	Average cost of all the nodes.
$\overline{C}_{HCE}$	Average cost of all the HCE nodes.	$\overline{C}_{ECE}$	Average cost of all ECE nodes.
C^A_{HCE}	The total cost of successfully attacked HCE nodes	C^A_{ECE}	The total cost of successfully attacked ECE nodes.
$R_{\Theta_A\Theta_D}$	Increase ratio of the overflow benefits caused by isolated ECE nodes.	$Z(\Theta_A, \Theta_D)$	This is an uncertain variable, affected by Θ_A and Θ_D.
$R_{\Theta_D\Theta_A}$	Increase ratio of the additional payoffs of the HCE nodes that fail due to cascading effects and being isolated.	Z_{ECE}	Profit generated by the failure of the ECE nodes due to cascade or isolation.
Z_{HCE}	Profit generated by the failure of the HCE nodes due to isolation.	$\langle k \rangle$	The average degree of the HCE-network.
$\langle k^2 \rangle$	The average degree of the second moment of the HCE-network.	P_C	The critical occupation probability

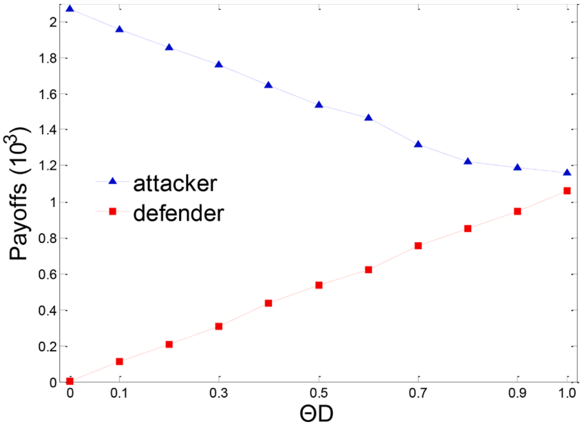


FIG. 5. The relationship between the payoff andΘ_D ($\Theta_A = 0$).

strategies of the attackers is discussed based on combination b in Fig. 3 (a).

For the mixed strategy, the target nodes of the attacker and the defender are selected randomly. It is assumed that $\Theta_D \in [0, 1]$ is the proportion of available resources that the defender plans to use to protect the ECE nodes, and the remaining $1 - \Theta_D$ proportion of resources is used to protect the HCE nodes. $\Theta_A \in [0, 1]$ is the proportion of available resources that the attacker attempts to use to attack the HCE nodes, and the remaining $1 - \Theta_A$ proportion of resources is used to attack ECE nodes. Fig. 4(a) and 4(b) show the resource allocation and corresponding payoffs of the ECE nodes and the HCE nodes in the network for the mixed strategy (Θ_A, Θ_D). Fig. 4(c) shows the total benefit obtained by the attacker and the defender for the mixed strategy. With the pure strategy, the result of the equilibrium solution is that the defender's payoff is 0. For the mixed strategy, both the defender and the attacker have more strategy space, therefore, the defender is more inclined to adopt mixed strategies than the attacker to strive for more payoffs. The main notations used in this section are shown in Table 1.

Fig. 5 shows how the payoff changes when the defender increases Θ_D, and the attacker keeps his/her strategy with $\Theta_A = 0$. The specific parameters of the network model are shown in Section 5. All the data comes from the simulation calculation described in Section 5. Obviously, the defender adopts a mixed strategy to change the result from combination b to combination d. However, the combination d with pure strategy is not an equilibrium solution, and the attacker takes action against the defender's mixed strategy.

For the mixed strategy (Θ_A, Θ_D), the payoff of the defender can be expressed as:

$$\begin{aligned} B^D &= \overline{B}^D_{ECE}\frac{\Theta_D TC_D}{\overline{C}_{ECE}} * \frac{1}{N-D} * \left(A - \frac{\Theta_A TC_A}{\overline{C}_{ECE}}\right) + \Theta_A TC_A(1-\Theta_D)\frac{\overline{B}^D_{HCE}}{\overline{C}_{HCE}} \\ &= \overline{B}^D_{ECE}\frac{\Theta_D P * TC}{\overline{C}_{ECE}} * \frac{1}{\frac{TC}{\overline{C}_T} - \frac{P * TC}{\overline{C}_{HCE}}} * (1-\Theta_A)\frac{P * TC}{\overline{C}_{ECE}} + \Theta_A P * TC(1-\Theta_D)\frac{\overline{B}^D_{HCE}}{\overline{C}_{HCE}}. \\ &= \frac{\Theta_D P * \overline{B}^D_{ECE}}{\overline{C}_{ECE}} * \frac{\overline{C}_T * \overline{C}_{HCE}}{\overline{C}_{HCE} - P * \overline{C}_T} * (1-\Theta_A)\frac{P * TC}{\overline{C}_{ECE}} + \Theta_A P * TC(1-\Theta_D)\frac{\overline{B}^D_{HCE}}{\overline{C}_{HCE}} \end{aligned} \tag{2}$$

The first item is the payoff obtained by the defender transferring the available resources to protect the ECE nodes in proportion Θ_D after the attacker transfers the available resources of $\Theta_A * TC_A$. The number of HCE nodes and the number of ECE nodes are $D = \frac{p * TC}{\overline{C}_{HCE}}$ and $A = \frac{p * TC}{\overline{C}_{ECE}}$, respectively. Usually, A is greater than D. $\overline{B}^D_{ECE}$ is the average payoff obtained by the defender when the attacked ECE nodes are all defended, and $\overline{C}_{ECE}$is the average cost of all ECE nodes. The second item is the payoff of being successfully defended when the attacker attacks the HCE nodes with the available resources of proportion Θ_A, and the defender has a $(1 - \Theta_D)$proportion of available resources for defending the HCE nodes. $\overline{C}_{HCE}$is the average cost of all the HCE nodes, and $\overline{B}^D_{HCE}$ is the average payoff obtained by the defender when the attacked HCE nodes are all defended.

The payoff of the attacker can be expressed as:

$$\begin{aligned} B^{A} &= R_{\Theta_A\Theta_D}\left[(1-\Theta_A)TC_A - \overline{C}_{ECE}\frac{\Theta_D TC_D}{\overline{C}_{ECE}}*\frac{1}{N-D}*\left(A-\frac{\Theta_A TC_A}{\overline{C}_{ECE}}\right)\right] \\ &\quad + R_{\Theta_D\Theta_A}\Theta_D{}^*\Theta_A TC_A + \mathrm{Z} \\ &= R_{\Theta_A\Theta_D}P^*TC(1-\Theta_A) - R_{\Theta_A\Theta_D}\Theta_D P^*\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}*\frac{P^*TC}{\overline{C}_{ECE}}*(1-\Theta_A) \\ &\quad + R_{\Theta_D\Theta_A}\Theta_D{}^*\Theta_A P^*TC + \mathrm{Z} \\ &= R_{\Theta_A\Theta_D}P^*TC(1-\Theta_A)\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}*\frac{\Theta_D{}^*P}{\overline{C}_{ECE}}\right) + R_{\Theta_D\Theta_A}\Theta_D{}^*\Theta_A P^*TC + \mathrm{Z}(\Theta_A,\Theta_D) \end{aligned} \quad . \qquad (3)$$

The first item is the attacker's payoff from the ECE nodes. It contains two parts. One part is $(1-\Theta_A)TC_A$, which is the payoff obtained by the attacker using the$(1-\Theta_A)$ proportion of available resources to attack the ECE nodes. The other part is the loss of the attacker's payoff after the defender protects the ECE nodes with $\Theta_D{}^*TC_D$ resources. The loss represented by the second part of Eq. (3) corresponds to the payoff represented by the first term of Eq. (2). $R_{\Theta_A\Theta_D} \geq 1$ is the parameter of overflow benefits caused by isolated ECE nodes. The second term is the payoff of the attacker successfully attacking the HCE nodes. $R_{\Theta_D\Theta_A} \geq 1$ reflects the additional benefits of the HCE nodes that have not been attacked but rather have failed due to cascading effects and isolated HCE nodes, as shown in Eq. (4).

$$R_{\theta_A\theta_D} = \frac{B^A_{ECE}}{C^A_{ECE}} \text{ and } R_{\theta_D\theta_A} = \frac{B^A_{ECE}}{C^A_{ECE}}. \qquad (4)$$

where B^A_{ECE} and B^A_{HCE} are the payoffs obtained by the attacker when the ECE and HCE nodes fail, respectively. It is worth noting that the attacker's payoffs come from three types of failed nodes: (1) Successfully attacked nodes; (2) nodes that are not attacked but cascade fail; (3) nodes that lose the connection to the network. C^A_{ECE} and C^A_{HCE} are the costs when the attacker successfully attacks the HCE node and the ECE node, respectively, that is, the effective attack costs. Essentially, both $R_{\Theta_A\Theta_D}$and $R_{\Theta_D\Theta_A}$are functions of $\Theta_A$and Θ_D. Special attention is paid to the variable $\mathrm{Z}(\Theta_A,\Theta_D)$. When $\Theta_A = 0$, $\mathrm{Z}(0,\Theta_D)$ represents the attacker's payoff generated when the HCE node is isolated, and $R_{\theta_D,0} = 1$; when $\Theta_A = 1$, $\mathrm{Z}(1,\Theta_D)$ represents the payoff generated by the ECE node, and $R_{1,D} = 1$. In other cases, $\mathrm{Z}(\Theta_A,\Theta_D) = 0$.

Obviously, the attacker-defender game for the network model is an adversarial non-cooperative game.

1 Optimization: $Atta\text{cker} : \min B^D$, $Defender : \max B^D$

It is assumed that the defender decides to transfer the available resources of proportion $\Theta_D$to protect the ECE nodes. The value of Θ_A depends on the attacker's purpose.

$$\begin{aligned} B^D &= \frac{\Theta_D P^*\overline{B}^D_{ECE}}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*(1-\Theta_A)\frac{P^*TC}{\overline{C}_{ECE}} + \Theta_A P^*TC(1-\Theta_D)\frac{\overline{B}^D_{HCE}}{\overline{C}_{HCE}} \\ &= \overline{B}^D_{ECE}{}^*\frac{\Theta_D{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*\frac{P^2{}^*TC}{\overline{C}^2_{ECE}} \\ &\quad + \Theta_A P^*TC\left[(1-\Theta_D)\frac{\overline{B}^D_{HCE}}{\overline{C}_{HCE}} - \frac{\Theta_D P^*\overline{B}^D_{ECE}}{\overline{C}^2_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right] \end{aligned} \quad . \qquad (5)$$

Here, $\overline{B}^D_{HCE} = \overline{C}_{HCE}$ and $\overline{B}^D_{ECE} = \overline{C}_{ECE}$. Therefore, Eq. (5) can be rewritten as:

$$B^D = \frac{\Theta_D{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*\frac{P^2{}^*TC}{\overline{C}_{ECE}} + \Theta_A P^*TC\left[(1-\Theta_D) - \frac{\Theta_D P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right]. \qquad (6)$$

For a specific network, parameters $\overline{C}_T$, $\overline{C}_{HCE}$, $\overline{C}_{ECE}$, TC, and P are definite values. When the defender decides to transfer the available resources of proportion Θ_D to protect the ECE nodes, the only variable in Eq. (6) is the parameter Θ_A. In order to facilitate analysis and expression, Eq. (6) can be written as:

$$\begin{aligned} B^D &= \frac{\Theta_D{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*\frac{P^2{}^*TC}{\overline{C}_{ECE}} + \Theta_A P^*TC\left[(1-\Theta_D) - \frac{\Theta_D P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right]. \\ &= Con(1) + \Theta_A P^*TC^*[Con(2) - Con(3)] \end{aligned} \qquad (7)$$

$$\begin{aligned} Con(1) &= \frac{\Theta_D{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*\frac{P^2{}^*TC}{\overline{C}_{ECE}};\ Con(2) = (1-\Theta_D);\ Con(3) \\ &= \frac{\Theta_D P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}] \end{aligned}$$

Here, $Con(i)$ represents a constant variable symbol whose value is a constant corresponding to the function.

The attacker's strategy is to minimize the defender's benefit. Therefore, the variable Θ_A must satisfy the following relationship.

$$\begin{aligned} &\min B^D = Con(1) + \Theta_A P^*TC^*(Con(2) - Con(3)) \\ &\quad if \quad \begin{cases} Con(2) - Con(3) < 0 & \Theta_A = 1 \\ Con(2) - Con(3) > 0 & \Theta_A = 0 \end{cases} \end{aligned} \quad . \qquad (8)$$

As shown in Eq. (8), if $Con(2) - Con(3) < 0$, to minimize the defender's gain B^D, the attacker will allocate all resources to attack the HCE nodes, that is, $\Theta_A = 1$. If $Con(2) - Con(3) > 0$, the attacker's strategy is $\Theta_A = 0$. Eq. (8) is rewritten in combination with the attacker's strategy.

$$\begin{cases} Con(2) - Com(3) < 0 \\ 1 - \Theta_D - \dfrac{\Theta_D P}{\overline{C}_{ECE}}*\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T} < 0 \Rightarrow \Theta_D > \Theta_D^* \end{cases} . \qquad (9)$$

$$\begin{cases} Con(2) - Com(3) > 0 \\ 1 - \Theta_D - \dfrac{\Theta_D P}{\overline{C}_{ECE}}*\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T} > 0 \Rightarrow \Theta_D < \Theta_D^* \end{cases} . \qquad (10)$$

$$\Theta_D^* = \frac{\overline{C}_{ECE}*\left(\overline{C}_{HCE} - P*\overline{C}_T\right)}{\overline{C}_{ECE}*\left(\overline{C}_{HCE} - P*\overline{C}_T\right) + P*\overline{C}_T*\overline{C}_{HCE}}$$

If and only $\Theta_D > \Theta_D^*$, Eq. (9) is satisfied, and the result of Eq. (10) is $\Theta_D < \Theta_D^*$. As $\Theta_D$increases from 0 to 1, there is a critical point Θ_D^*that causes $\Theta_A$to mutate from 0 to 1. Therefore, in the face of a mixed strategy of defenders, attackers can adopt a pure strategy to minimize the defender's benefits.

Assuming that $\Theta_A = 0$, Eq. (6) can be written as:

$$\begin{aligned} B^D &= \frac{\Theta_D*\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}*\frac{P^2*TC}{\overline{C}_{ECE}} + \Theta_A P*TC\left[(1-\Theta_D) - \frac{\Theta_D P}{\overline{C}_{ECE}}*\frac{\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}\right]. \\ &= \frac{\Theta_D*\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}*\frac{P^2*TC}{\overline{C}_{ECE}} \end{aligned} \tag{11}$$

To get the results of $\max B^D$, the defender hopes that the larger the Θ_D, the better. However, by combining Eq. (8), Eq. (9), and Eq. (10), as Θ_D improves, the attacker's strategy mutates to $\Theta_A = 1$ when the parameter $\Theta_D > \Theta_D^*$. Therefore, under the premise that the attacker still adopts the strategy of $\Theta_A = 0$, the best strategy of the defender is $\Theta_D = \Theta_D^*$.

If $\Theta_A = 1$, Eq. (6) can be written as:

$$\begin{aligned} B^D &= \frac{\Theta_D*\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}*\frac{P^2*TC}{\overline{C}_{ECE}} + \Theta_A P*TC\left[(1-\Theta_D) - \frac{\Theta_D P}{\overline{C}_{ECE}}*\frac{\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}\right]. \\ &= P*TC*(1-\Theta_D) \end{aligned} \tag{12}$$

The analysis of Eq. (12) shows that the smaller the Θ_D, the better the defender's payoff. Therefore, under the premise that the attacker still adopts the strategy of $\Theta_A = 1$, the best strategy of the defender is $\Theta_D = \Theta_D^*$. Combining Eq. (11) and Eq. (12), the solution of the optimization problem $A : \min B^D$, $D : \max B^D$ is:

$$\underset{\Theta_A}{min}\ \underset{\Theta_D}{max} B^D = \min\begin{cases} B_1^D = \frac{\Theta_D*\overline{C}_T*\overline{C}_{HCE}}{\overline{C}_{HCE} - P*\overline{C}_T}*\frac{P^2*TC}{\overline{C}_{ECE}} & \begin{cases}\Theta_A = 0 \\ \Theta_D = \Theta_D^*\end{cases} \\ B_2^D = P*TC*(1-\Theta_D) & \begin{cases}\Theta_A = 1 \\ \Theta_D = \Theta_D^*\end{cases} \end{cases}. \tag{13}$$

According to Eq. (9) and Eq. (10), we obtain the expression for Θ_D^*. The result is $B_1^D = B_2^D$ by substituting Θ_D^* into the two relationships of Eq. (13). As shown in Eq. (14):

$$\underset{\Theta_A}{min}\ \underset{\Theta_D}{max} B^D = \frac{\overline{C}_T*\overline{C}_{HCE}*P^2*TC}{\overline{C}_{ECE}*\left(\overline{C}_{HCE} - P*\overline{C}_T\right) + \overline{C}_T*\overline{C}_{HCE}*P} \begin{cases}\Theta_A = 0\ or\ 1 \\ \Theta_D = \Theta_D^*\end{cases}. \tag{14}$$

1 Optimization: *Attac*ker : $\min B^D$, *Defender* : $\min B^A$

To minimize the payoff of the defender, according to Eq. (8), Eq. (9), and Eq. (10), it is known that there are only two strategies for the attacker: $\Theta_A = 0$when $\Theta_D < \Theta_D^*$, and $\Theta_A = 1$when $\Theta_D > \Theta_D^*$. Therefore, the behaviors of the defender for these two strategies of the attacker are analyzed.

When the defender tries to reduce the attacker's payoff and $\Theta_D < \Theta_D^*$ under the condition of $\Theta_A = 0$, the attacker's payoff is expressed as:

$$\begin{aligned} B^A &= R_{\Theta_A\Theta_D}P*TC(1-\Theta_A)\left(1 - \frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE} - P\overline{C}_T}*\frac{\Theta_D*P}{\overline{C}_{ECE}}\right) + R_{\Theta_D\Theta_A}\Theta_D*\Theta_A P*TC + Z(\Theta_A,\Theta_D) \\ &= R_{\Theta_A\Theta_D}P*TC*\left(1 - \frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE} - P\overline{C}_T}*\frac{\Theta_D*P}{\overline{C}_{ECE}}\right) + Z(0,\Theta_D) \end{aligned}. \tag{15}$$

$R_{\Theta_A\Theta_D}$ and $Z(0,\Theta_D)$ depend on the number of ECE nodes successfully attacked. Therefore, both $R_{\Theta_A\Theta_D}$and $Z(0,\Theta_D)$ decrease as Θ_D increases.

When Θ_D continues to increase to meet the condition of $\Theta_D > \Theta_D^*$, $\Theta_A = 1$, the attacker's payoff is expressed as:

$$\begin{aligned} B^A &= R_{\Theta_A\Theta_D}P*TC(1-\Theta_A)\left(1 - \frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE} - P\overline{C}_T}*\frac{\Theta_D*P}{\overline{C}_{ECE}}\right) + R_{\Theta_D\Theta_A}\Theta_D*\Theta_A P*TC + Z(\Theta_A,\Theta_D) \\ &= R_{\Theta_D\Theta_A}\Theta_D P*TC + Z(1,\Theta_D) \end{aligned}. \tag{16}$$

As Θ_D increases, the value of $R_{\Theta_D\Theta_A}$ decreases to 1, but $Z(1,\Theta_D)$ increases. In a scale-free network, under this condition, $R_{\Theta_D\Theta_A} \approx 1$ and $Z(1,\Theta_D)$ has a larger value [15]. Therefore, for the condition of $\Theta_A = 1$, the smaller the Θ_D, the better.

After combining Eq. (15) and Eq. (16), the solution of the optimization problem $A : \min B^D$, $D : \min B^A$ is:

$$\mathrm{Attacker}:\ \min B^D, \mathit{Defender}:\min B^A$$

$$B^D = \frac{\overline{C}_T*\overline{C}_{HCE}*P^2*TC}{\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)+\overline{C}_T*\overline{C}_{HCE}*P} \qquad \begin{cases}\Theta_A=0\,or\,\Theta_A=1\\ \Theta_D=\Theta_D^*\end{cases}$$

$$B^A=\min\begin{cases} R_{\Theta_A\Theta_D^*}P*TC*\left(1-\frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}*\frac{\Theta_D^**P}{\overline{C}_{ECE}}\right)+Z(0,\Theta_D) & \begin{cases}\Theta_A=0\\ \Theta_D=\Theta_D^*\end{cases} \\ R_{\Theta_D^*\Theta_A}\Theta_D^*P*TC+Z(1,\Theta_D) & \begin{cases}\Theta_A=1\\ \Theta_D=\Theta_D^*\end{cases}\end{cases}. \tag{17}$$

the defense resources of the ECE nodes, the attacker's benefit decreases. The reduction of the attacker's benefit comes from two aspects: one is that the defender successfully defends the attacked node, and the other is the protection of the network structure brought about by the successful defense, which reduces the number of isolated nodes. When the attacker transfers his/her resources to attack the HCE nodes, the changes in his/her benefits are mainly affected by the relationship between the benefit generated by the transferred resources Θ_A in the ECE nodes and the benefit obtained in the HCE nodes. However, the cascading impact caused by the destruction of the HCE nodes and the additional benefits generated by the destruction of the network structure (isolated nodes) are also very important aspects.

There are three main situations in which the attacker obtains the most benefit:

$$\max B^A=\begin{cases} R_{\Theta_A\Theta_D}P*TC\left(1-\frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}*\frac{\Theta_D*P}{\overline{C}_{ECE}}\right)+Z(0,\Theta_D) & \begin{cases}\Theta_A=0\\ \Theta_D<\Theta_D^1\end{cases} \\ \left[R_{\Theta_A^*\Theta_D}\left(1-\Theta_A^*\right)\left(1-\frac{\overline{C}_{HCE}*\overline{C}_T*\Theta_D*P}{\overline{C}_{ECE}\left(\overline{C}_{HCE}-P\overline{C}_T\right)}\right)+R_{\Theta_D\Theta_A^*}\Theta_D*\Theta_A^*\right]P*TC & \begin{cases}\Theta_A=\Theta_A^*\\ \Theta_D^1\le\Theta_D<\Theta_D^2\end{cases} \\ R_{\Theta_D\Theta_A^*}\Theta_D*\Theta_A^**P*TC+Z(1,\Theta_D) & \begin{cases}\Theta_A=1\\ \Theta_D\ge\Theta_D^2\end{cases}\end{cases}. \tag{19}$$

After substituting the expression for Θ_D^* into the two relationships of Eq. (17), Eq. (17) can be expressed as:

$$\mathrm{Attacker}:\ \min B^D, \mathit{Defender}:\min B^A$$

$$B^D = \frac{\overline{C}_T*\overline{C}_{HCE}*P^2*TC}{\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)+\overline{C}_T*\overline{C}_{HCE}*P} \qquad \begin{cases}\Theta_A=0\,or\,\Theta_A=1\\ \Theta_D=\Theta_D^*\end{cases}$$

$$B^A=\min\begin{cases} \frac{R_{\Theta_A\Theta_D^*}*\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)*P*TC}{\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)+P*\overline{C}_T*\overline{C}_{HCE}}+Z\left(0,\Theta_D^*\right) & \begin{cases}\Theta_A=0\\ \Theta_D=\Theta_D^*\end{cases} \\ \frac{R_{\Theta_D^*\Theta_A}*\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)*P*TC}{\overline{C}_{ECE}*\left(\overline{C}_{HCE}-P*\overline{C}_T\right)+P*\overline{C}_T*\overline{C}_{HCE}}+Z\left(1,\Theta_D^*\right) & \begin{cases}\Theta_A=1\\ \Theta_D=\Theta_D^*\end{cases}\end{cases}. \tag{18}$$

The scale-free network is vulnerable to the failure of the large-value nodes. Therefore, the equilibrium solution is usually $\Theta_A = 0$, $\Theta_D = \Theta_D^*$.

1 Optimization: *Attac*ker : max B^A , *Defender* : min B^A

In the initial state $\Theta_A = 0$, $\Theta_D = 0$, and when the defender increases

Assuming that the defender allocates resources Θ_D to protect the ECE node, the benefits of the attacker's resource $\Theta_A P*TC$ used to attack the ECE and HCE nodes are as follows.

(1) Profit from destroying the ECE nodes:

$$B^A_{ECE}(\Theta_D,\Theta_A)=R_{\Theta_A\Theta_D}\left(1-\frac{\overline{C}_{HCE}*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}*\frac{\Theta_D*P}{\overline{C}_{ECE}}\right)*\Theta_A P*TC+Z_{HCE}. \tag{20}$$

where Z_{HCE}represents the profit generated by the failure of the HCE nodes due to isolation. In a scale-free network, $Z_{HCE}\approx 0$.

(1) Profit from destroying the HCE nodes:

$$B^A_{HCE}(\Theta_D,\Theta_A)=R_{\Theta_D\Theta_A}\Theta_D*\Theta_A P*TC+Z_{ECE}. \tag{21}$$

where Z_{ECE} represents the profit generated by the failure of the ECE nodes due to cascade or isolation. Z_{ECE} increases as the number of failed HCE nodes increases.

In the analysis from the structural characteristics, the HCE nodes

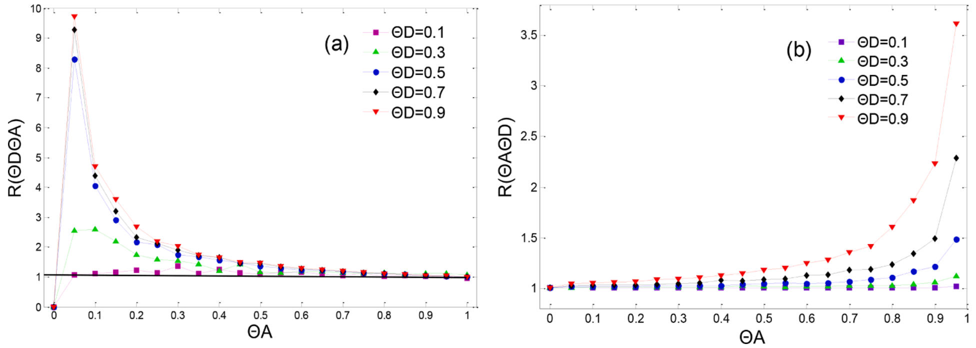


FIG. 6. Function relationship between parameters $R_{\Theta_A\Theta_D}(R_{\Theta_D\Theta_A})$ vs. Θ_A.

require that the degree value distribution of its neighboring nodes be heterogeneous. The condition for a node v_i with the degree k_i to become an HCE node is that at least one neighbor node $v_j$satisfies the relationship$\alpha + \ (\beta - \ 1)k_j^\theta < k_i^\theta k_j^\theta / \left(\sum_{h\in\Gamma_i} k_h^\theta\right)$. Therefore, large degree nodes are more likely to become HCE nodes, and the HCE nodes have excellent connectivity. We mark the giant cluster formed by all HCE nodes (removing ECE nodes) as the HCE-network. However, when Θ_D is small, there are fewer unprotected HCE nodes at this time, and the HCE nodes are dispersed from each other in terms of structure, so they cannot produce cascading effects, and the structure of the network is not damaged. Under this condition, $R_{\Theta_D\Theta_A} \approx 1$, $R_{\Theta_A\Theta_D} \approx 1$, and $Z_{ECE}$and $Z_{HCE}$are both small. Therefore, Eq. (20) and Eq. (21) can be approximated as:

$$B_{ECE}^A(\Theta_D, \Theta_A) = \left(1 - \frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE} - P\overline{C}_T}{}^*\frac{\Theta_D{}^*P}{\overline{C}_{ECE}}\right){}^*\Theta_A P^*TC \qquad (22)$$

$$B_{HCE}^A(\Theta_D, \Theta_A) = \Theta_D{}^*\Theta_A P^*TC$$

The attacker's benefit at this time is a linear function, and the attacker's strategy depends on the following relationships:

$$\begin{aligned}
&if\ \Theta_D{}^*\left[\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right) + \overline{C}_{HCE}{}^*\overline{C}_T{}^*P\right]\Big\rangle\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right)\\
&\quad \Theta_D > \Theta_D^c\ and\ \ \Theta_A = 1\\
&else\\
&\quad \Theta_D{}^*\left[\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right) + \overline{C}_{HCE}{}^*\overline{C}_T{}^*P\right]\Big\langle\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right)\\
&\quad \Theta_D < \Theta_D^c\ and\ \ \Theta_A = 0
\end{aligned} \qquad (23)$$

According to Eq. (23), a critical value can be obtained:

$$\Theta_D^c = \frac{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right)}{\left[\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE} - P\overline{C}_T\right) + \overline{C}_{HCE}{}^*\overline{C}_T{}^*P\right]}. \qquad (24)$$

In this case, the problem is similar to the first type of optimization problem, and $\Theta_D^C = \Theta_D^*$. Therefore, $\Theta_A = 0$ when $\Theta_D < \Theta_D^c$is satisfied; otherwise, $\Theta_A = 1$.

If the mixed strategy is $\Theta_A = 0, \Theta_D < \Theta_D^c$. According to Eq. (3), the attacker's profit is:

$$B^A = P^*TC\left(1 - \frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE} - P\overline{C}_T}{}^*\frac{\Theta_D{}^*P}{\overline{C}_{ECE}}\right) + Z(0, \Theta_D). \qquad (25)$$

To reduce the attacker's profit, the defender increases Θ_D. Therefore, the optimal solution is $(\Theta_A = 0, \Theta_D = \Theta_D^c)$.

If the mixed strategy is $\Theta_A = 1, \Theta_D \geq \Theta_D^c$, the attacker's profit is:

$$B^A = \Theta_D{}^*P^*TC + Z(1, \Theta_D). \qquad (26)$$

To reduce the attacker's profit, the defender decreases Θ_D. Therefore, the optimal solution is $(\Theta_A = 1, \Theta_D = \Theta_D^c)$.

However, the above analysis must meet a prerequisite. Θ_D must be less than another critical value Θ_D^Λ. When the transferred defense resources exceed the critical valueΘ_D^Λ, the unprotected nodes in the HCE nodes form a structurally connected graph. Therefore, the cascading effect between HCE nodes can be spread. Reference [50] analyzes the critical occupation probability for the arbitrary degree distribution to satisfy $p_c = \langle k\rangle/(\langle k^2\rangle - \langle k\rangle)$. Therefore, Θ_D^Λ should satisfy the relationship $\langle k\rangle/(\langle k^2\rangle - \langle k\rangle) = (\Theta_D^\Lambda)^2$, and $\langle k\rangle$ and $\langle k^2\rangle$ are the average degree of the HCE-network and the average degree of the second moment, respectively.

Scale-free networks are very robust against random attacks, but they are very vulnerable to the destruction of large value nodes. In other words, as the number of failed HCE nodes increases, the destruction of the network structure increases the value of $R_{\Theta_A\Theta_D}$in Eq. (3). An increase in Θ_A increases the numerator and decreases the denominator. $R_{\Theta_D\Theta_A}$ is mainly affected by the cascading effect, and it decreases when a HCE node fails due to the cascading effect and is attacked at the same time. Therefore, as shown in Fig. 6, all the data in Fig. 6 comes from the simulation calculation in Section 5. The change of $R_{\Theta_D\Theta_A}$ is a parabola with $\Theta_A$as a function. The range of change for both $R_{\Theta_A\Theta_D}$and $R_{\Theta_D\Theta_A}$increases with the increase of Θ_D.

If $\Theta_D^\Lambda \leq \Theta_D$, the benefit of the attacker is greater than the benefit of a successful attack due to the cascading impact. Therefore, $\Theta_D^1 \geq \Theta_D^\Lambda$ is a

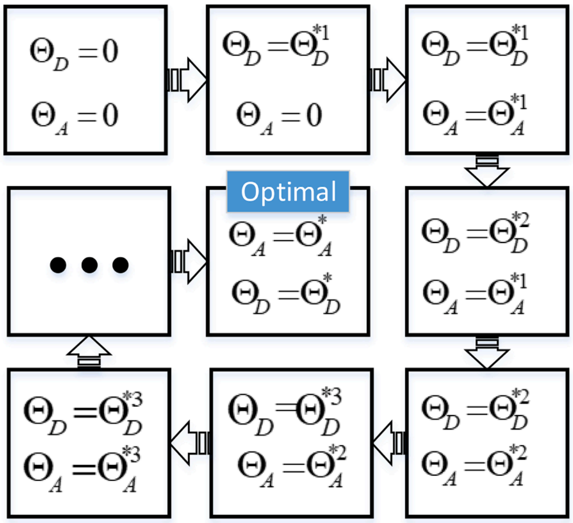

$\Theta_D = 0$
$\Theta_A = 0$
$\Theta_D = \Theta_D^{*1}$
$\Theta_A = 0$
$\Theta_D = \Theta_D^{*1}$
$\Theta_A = \Theta_A^{*1}$
Optimal
$\Theta_A = \Theta_A^*$
$\Theta_D = \Theta_D^*$
$\Theta_D = \Theta_D^{*2}$
$\Theta_A = \Theta_A^{*1}$
$\Theta_D = \Theta_D^{*3}$
$\Theta_A = \Theta_A^{*3}$
$\Theta_D = \Theta_D^{*3}$
$\Theta_A = \Theta_A^{*2}$
$\Theta_D = \Theta_D^{*2}$
$\Theta_A = \Theta_A^{*2}$

FIG. 7. Schematic diagram of optimization process decomposition.

necessary condition. Additionally, there is a critical point Θ_A^* at which the resource used by the attacker to attack the HCE nodes exceeds Θ_A^*, the benefit of the cascading impact is reduced, and the resource used to attack the HCE node is not as effective as attacking the ECE nodes. If $\Theta_D^1 \le \Theta_D < \Theta_D^2$,$\Theta_A^*$ is determined by the HCE-network. However, due to the self-similar properties of complex networks, the mutation of Θ_A^* is inevitable and stable. For a certain Θ_D, the following relationship is satisfied.

$$\begin{aligned} B^A\left(\Theta_D,\Theta_A^*\right) &= B_{HCE}^A\left(\Theta_D,\Theta_A^*\right)+B_{ECE}^A\left(\Theta_D,1-\Theta_A^*\right) \\ &> B_{ECE}^A\left(\Theta_D,\Theta_A^*\right)+B_{ECE}^A\left(\Theta_D,1-\Theta_A^*\right) \quad . \\ &= B^A\left(\Theta_D,0\right) \end{aligned} \tag{27}$$

According to Eq. (20) and Eq. (21), for a certainΘ_A, the larger the Θ_D, the greater the profit of B^A.

$$\begin{aligned} &if \;\; \Theta_{D1} > \Theta_{D2} \\ &B_{HCE}^A(\Theta_{D1},\Theta_A)\rangle B_{HCE}^A(\Theta_{D2},\Theta_A)\rangle B_{ECE}^A(\Theta_{D2},\Theta_A)\rangle B_{ECE}^A(\Theta_{D1},\Theta_A) \end{aligned} . \tag{28}$$

Therefore, Eq. (27) and Eq. (28) are combined to minimize the attacker's profits, and the defender's strategy is $\Theta_D = \Theta_D^\Lambda$.

In summary, the equilibrium solution of the optimization problem ($A:\max B^A\;,\;D:\min B^A$) can have the following two situations.

(i) If $\Theta_D^c < \Theta_D^\Lambda$

$$\underset{\Theta_A\;\;\Theta_D}{maxmin}B^A = \max\begin{cases} P^*TC\left(1-\dfrac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\dfrac{\Theta_D^c{}^*P}{\overline{C}_{ECE}}\right)+Z\left(0,\Theta_D^c\right) & \begin{cases}\Theta_A=0\\ \Theta_D=\Theta_D^c\end{cases} \\ \Theta_D^c{}^*P^*TC+Z\left(1,\Theta_D^c\right) & \begin{cases}\Theta_A=1\\ \Theta_D=\Theta_D^c\end{cases} \end{cases} . \tag{29}$$

Combined with Eq. (24), Eq. (29) can be expressed as:

$$\underset{\Theta_A\;\;\Theta_D}{maxmin}B^A = \max\begin{cases} \dfrac{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right){}^*P^*TC}{\left[\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right)+\overline{C}_{HCE}{}^*\overline{C}_T{}^*P\right]}+Z\left(0,\Theta_D^c\right) \\ \dfrac{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right){}^*P^*TC}{\left[\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right)+\overline{C}_{HCE}{}^*\overline{C}_T{}^*P\right]}+Z\left(1,\Theta_D^c\right) \end{cases} . \tag{30}$$

(i) If $\Theta_D^c > \Theta_D^\Lambda$, the optimal result is as shown in Eq. (31).

$$\begin{aligned} \underset{\Theta_A\;\;\Theta_D}{maxmin}B^A &= P^*TC\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^{\Lambda}{}^*P}{\overline{C}_{ECE}}\right) \\ &\quad +Z\left(0,\Theta_D^\Lambda\right)\;\begin{cases}\Theta_A=0\\ \Theta_D=\Theta_D^\Lambda\end{cases} . \end{aligned} \tag{31}$$

$\langle k\rangle/(\langle k^2\rangle-\langle k\rangle) = (\Theta_D^\Lambda)^2$ is combined to rewrite Eq. (31).

$$\begin{aligned} \underset{\Theta_A\;\;\Theta_D}{maxmin}B^A &= P^*TC\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\left[\langle k\rangle/\left(\left\langle k^2\right\rangle-\langle k\rangle\right)\right]^{1/2}{}^*P}{\overline{C}_{ECE}}\right) \\ &\quad +Z\left(0,\Theta_D^\Lambda\right) . \end{aligned} \tag{32}$$

1 Optimization: *Attac*ker : max B^A , *Defender* : max B^D

As analyzed in a previous section, the defender will first take action to increase his/her profit. Therefore, combined with the idea of dynamic programming, the game process is decomposed into steps, as shown in Fig. 7. The attacker and the defender act alternately. The actor at each step makes a strategic choice based on the opponent's action result in the previous step and finally achieves a balanced solution. The specific solution steps are as follows.

The first step: We set $\Theta_D = \Theta_D^*$. With this condition, the attacker's strategy does not affect the defender's payoff. This means that the attacker's attack success rate between HCE nodes and ECE nodes is the same, and the attacker's strategy choice depends on the additional payoffs brought by isolated nodes or cascading failed nodes. The analysis from the attacker's payoff shows: max B^A.

$$\begin{aligned} \max B^A \; &= R_{\Theta_A\Theta_D^*}P^*TC(1-\Theta_A)\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^*{}^*P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^*\Theta_A}\Theta_D^*{}^*\Theta_AP^*TC+Z(\Theta_A,\Theta_D) \\ &= R_{\Theta_A\Theta_D^*}P^*TC(1-\Theta_A)(1-Con(4))\;+R_{\Theta_D^*\Theta_A}\Theta_D^*{}^*\Theta_AP^*TC+Z(\Theta_A,\Theta_D) \\ &= P^*TC^*\left[R_{\Theta_A\Theta_D^*}(1-\Theta_A)(1-Con(4))\;+R_{\Theta_D^*\Theta_A}\Theta_D^*{}^*\Theta_A\right]+Z(\Theta_A,\Theta_D) \end{aligned} \tag{33}$$

Table 2
Network parameter value list.

Parameter\Network	θ	α	β	p	$\overline{C}_{HCE}$	$\overline{C}_{ECE}$	$\overline{C}_{T}$	TC
Scale-free Network	1	1.01	3.5	0.342	18.24	4.44	6.01	6000
Email Network	1	1.01	2.2	0.272	17.77	8.213	9.622	10,902

$$=\max\begin{cases} P^*TC^*R_{\Theta_A,\Theta_D^*}(1-Con(4))+\mathrm{Z}(0,\Theta_D) & \Theta_A=0 \\ P^*TC^*\left[R_{\Theta_A\Theta_D^*}(1-\Theta_A)(1-Con(4))+R_{\Theta_D\Theta_A}\Theta_D^{*}{}^*\Theta_A\right] & \Theta_A=\Theta_A^* \\ P^*TC^*R_{\Theta_D^*\Theta_A}\Theta_D^*+Z(1,\Theta_D) & \Theta_A=1 \end{cases}$$

The second step: If the optimal solution of Eq. (19) is $(\Theta_A=0,\Theta_D=\Theta_D^*)$ or $(\Theta_A=1,\Theta_D=\Theta_D^*)$, then combined with Eq. (14), the optimization $(A:\max B^A, D:\max B^D)$ obtains a balanced solution. Otherwise, an optimal value can be found that satisfies $\Theta_A^*\in(0,\ 1)$to maximize the attacker's profits. Based on Eq. (6), in order to maximize their own profits, the defender changes the value of $\Theta_D$according to the following three possible relationships:

$$\max B^D=\frac{\Theta_D^{*}{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}+\Theta_A^*P^*TC\left[\left(1-\Theta_D^*\right)-\frac{\Theta_D^*P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right]$$

$$\text{(i)}\ \ if\ \frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}<\Theta_A^*P^*TC\left(1+\frac{P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right)$$

$$\max B^D=\Theta_A^*P^*TC\ \ \left(\Theta_A=\Theta_A^*,\ \Theta_D=0\right). \tag{34}$$

$$\text{(ii)}\ \ if\ \frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}=\Theta_A^*P^*TC\left(1+\frac{P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right)$$

$$\max B^D=\frac{\Theta_D^{*}{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}+\Theta_A^*P^*TC\left[\left(1-\Theta_D^*\right)-\frac{\Theta_D^*P}{\overline{C}_{ECE}}{}^*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right]\ \left(\Theta_A=\Theta_A^*,\Theta_D=\Theta_D^*\right). \tag{35}$$

$$\text{(iii)}\ \ if\ \frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}>\Theta_A^*P^*TC\left(1+\frac{P}{\overline{C}_{ECE}}*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right)$$

$$\max B^D=\left(1-\Theta_A^*\right)\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}\qquad\left(\Theta_A=\Theta_A^*,\ \Theta_D=1\right). \tag{36}$$

If Eq. (35) is satisfied, the defender change strategy does not produce greater benefits, and the optimization $(A:\max B^A\ ,\ D:\max B^D)$ can obtain the optimal value. Otherwise, Θ_D tends towards two extremes according to Eq. (34) and Eq. (36). Here, we record the relationship for which $\Theta_A^\#$ satisfies Eq. (35). For the case of the attacker adopting strategy $\Theta_A^\#$, any strategy of the defender does not change his/her benefit.

The third step: Consider two cases based on step 2.

1 For the situation of Eq. (34), the strategic tendency of the defender tends towards $\Theta_D=0$. However, when $\Theta_D=0$, the optimal strategy of the attacker must be $\Theta_A=0$. At this time, the relationship of Eq. (34) is no longer satisfied, and the relationship of Eq. (36) is satisfied, which makes the defender's strategic tendency tend towards $\Theta_D=1$. Therefore, according to Eq. (19), Θ_D^Λ is the turning point, and when $\Theta_D<\Theta_D^\Lambda$, the relationship between Eq. (34) and Eq. (36) changes suddenly, and the equilibrium solution is $(\Theta_D^\Lambda,\ \Theta_A^*)$.

$$\begin{cases}\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}*\dfrac{P^2{}^*TC}{\overline{C}_{ECE}}<\Theta_A^*P*TC\left(1+\dfrac{P}{\overline{C}_{ECE}}*\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right) & \Theta_D\end{cases}\geq\Theta_D^\Lambda \tag{37}$$

$$\begin{cases}\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\dfrac{P^2{}^*TC}{\overline{C}_{ECE}}\geq\Theta_A^*P^*TC\left(1+\dfrac{P}{\overline{C}_{ECE}}{}^*\dfrac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right) & \Theta_D<\Theta_D^\Lambda\end{cases} \tag{38}$$

2 If the value of Θ_A^* satisfies Eq. (36), the strategic tendency of the defender tends toward $\Theta_D=1$. According to Eq. (19), if there is a value Θ_D^2 for which the attacker's strategy to achieve the most benefit is $\Theta_A=1$, then the equilibrium solution is $(\Theta_D^2,\ \Theta_A^*)$ if and only if the following relationship is satisfied.

$$\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}\leq P^*TC\left(1+\frac{P}{\overline{C}_{ECE}}{}^*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right). \tag{39}$$

When $\Theta_D=\Theta_D^2$, as $\Theta_A$increases from $\Theta_A^*$to 1, the effect of the cascading influence is reduced, and the increase of B_A is based on a linear relationship. Therefore, Θ_D^2 can be obtained based on the following relationship:

$$if\quad\Theta_A\geq\Theta_A^*$$

$$P^*TC^*\left[R_{\Theta_A\Theta_D^2}(1-\Theta_A)\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^2{}^*P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^2\Theta_A}\Theta_D^2{}^*\Theta_A\right]=P^*TC^*\Theta_D^2+\mathrm{Z}_{\Theta_A=1} \tag{40}$$

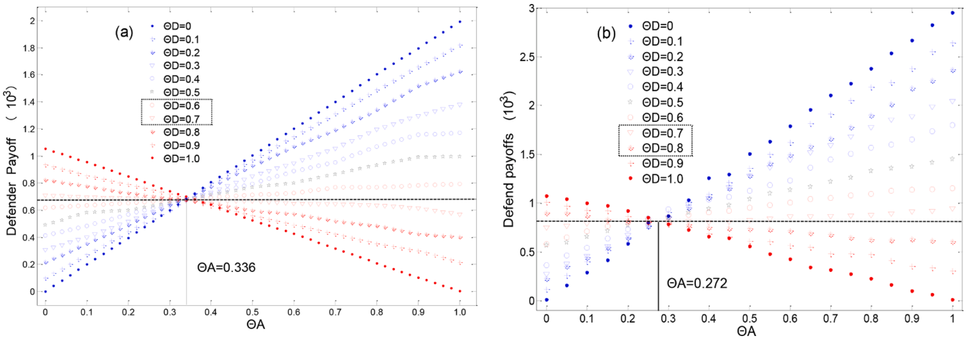


FIG. 8. Simulation results of optimization problems $A:\min B^D, D:\max B^D$((a) shows the simulation results of the scale-free network, and (b) shows the simulation results of the email network.).

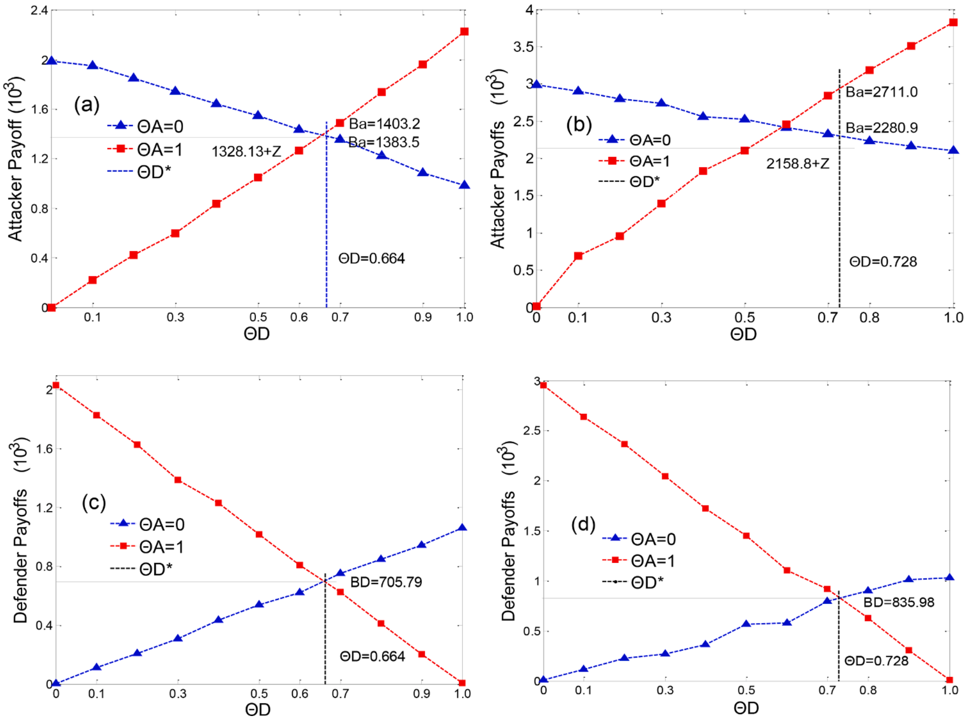


FIG. 9. Simulation results of the optimization problems $A:\min B^D$, $D:\min B^A$((a) and (c) are the simulation results of the scale-free network, and (b) and (d) are the simulation results of the email network.).

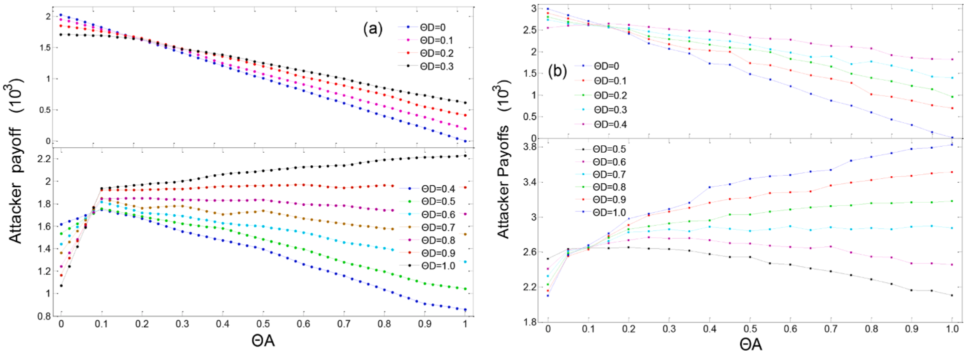


FIG. 10. Simulation results of the optimization problems $A:\max B^A$, $D:\min B^A$((a) shows the simulation results of the scale-free network, and (b) shows the simulation results of the email network.).

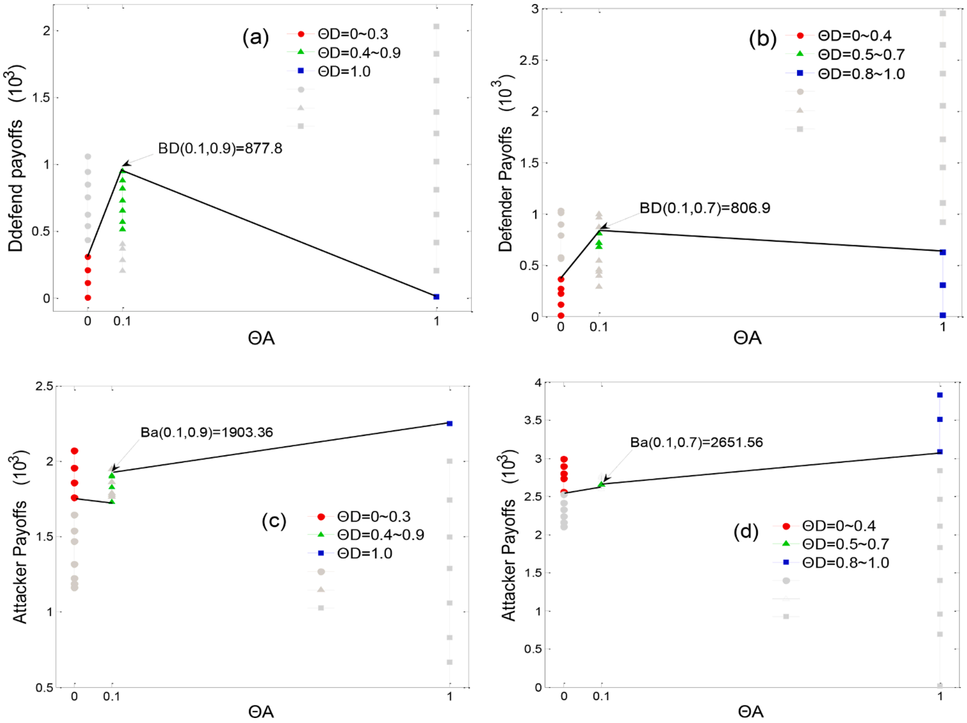


FIG. 11. Simulation results of the optimization problems $A : \max B^A, D : \min B^A$((a) and (c) show the simulation results of the scale-free network, and (b) and (d) show the simulation results of the email network.).

Table 3
Attacker's payoffs under different combinations of strategies in the email network.

$\Theta_D \backslash \Theta_A$	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0	2.9879	2.8957	2.7995	2.7339	2.5544	2.5222	2.4082	2.3245	2.2321	2.1593	2.1
0.1	2.7096	2.6481	2.6182	2.6088	2.6222	2.649	2.652	2.6516	2.6499	2.6295	2.6759
0.2	2.4148	2.4549	2.514	2.5419	2.6185	2.6512	2.7361	2.8272	2.8582	2.907	2.9795
0.3	2.0678	2.1722	2.2907	2.3883	2.5253	2.6342	2.7553	2.8591	2.9257	3.0634	3.0899
0.4	1.7295	2.0297	2.1626	2.2815	2.4696	2.5774	2.7354	2.8863	2.9604	3.1605	3.3389
0.5	1.4852	1.7394	2.0587	2.1601	2.323	2.5404	2.6949	2.8412	3.0276	3.2184	3.436
0.6	1.1976	1.5666	1.8329	1.9759	2.2748	2.454	2.6593	2.8922	3.0864	3.2826	3.4779
0.7	0.874	1.3738	1.6564	1.8898	2.1303	2.3771	2.6644	2.8858	3.1241	3.3606	3.535
0.8	0.5996	1.0118	1.3898	1.7776	2.071	2.2885	2.5488	2.8735	3.1599	3.4215	3.6873
0.9	0.3044	0.8654	1.2088	1.5676	1.8616	2.1641	2.4701	2.8884	3.1683	3.4708	3.7781
1.0	0.0146	0.6913	0.9585	1.3958	1.826	2.1067	2.4563	2.8733	3.1817	3.5114	3.8275

If any Θ_D does not satisfy Eq. (40), then Θ_D^2 does not exist. Therefore,

Table 4
Defender's payoffs under different combinations of strategies in the email network.

$\Theta_D \backslash \Theta_A$	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0	0.0079	0.115	0.2249	0.2692	0.3609	0.5652	0.5766	0.7925	0.8991	1.0097	1.0329
0.1	0.2883	0.3965	0.4376	0.456	0.5416	0.6753	0.7171	0.8069	0.8697	0.9646	0.999
0.2	0.5802	0.6335	0.6134	0.6731	0.7312	0.732	0.828	0.7676	0.8175	0.8582	0.9403
0.3	0.9245	0.9017	0.9133	0.9452	0.9333	0.8486	0.8748	0.8053	0.7964	0.7823	0.7827
0.4	1.2542	1.0861	1.0576	1.1105	1.0316	0.9684	0.931	0.8133	0.7476	0.6832	0.6528
0.5	1.5012	1.437	1.2801	1.2274	1.1223	1.0704	0.9309	0.8081	0.7241	0.6086	0.5536
0.6	1.7844	1.6167	1.4934	1.3659	1.228	1.112	1.0105	0.8581	0.7138	0.5581	0.4237
0.7	2.1032	1.9091	1.778	1.5903	1.3752	1.1433	1.0523	0.8235	0.6445	0.4758	0.3127
0.8	2.3743	2.1853	1.9674	1.6741	1.5082	1.3619	1.082	0.8506	0.6445	0.4688	0.2229
0.9	2.6667	2.3777	2.1749	1.8881	1.5926	1.3578	1.1141	0.8583	0.6051	0.3518	0.0977
1.0	2.9525	2.6401	2.3648	2.0471	1.7248	1.4522	1.1014	0.9174	0.6266	0.3034	0.0068

Table 5
Attacker's payoffs under different combinations of strategies in the scale-free network.

$\Theta_D \backslash \Theta_A$	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0	2.0691	1.9547	1.8563	1.7579	1.6447	1.5366	1.4654	1.3153	1.2212	1.1862	1.1587
0.1	1.8582	1.7871	1.7727	1.7605	1.7286	1.7657	1.7879	1.8275	1.8954	1.9033	1.9463
0.2	1.6434	1.6208	1.6227	1.6293	1.6671	1.6957	1.7697	1.7785	1.8865	1.9108	1.9962
0.3	1.4426	1.4487	1.4993	1.5259	1.5852	1.6327	1.7038	1.7368	1.8733	1.9371	2.0166
0.4	1.2382	1.2746	1.3393	1.3748	1.5006	1.5846	1.6548	1.7763	1.8817	1.9515	2.0495
0.5	1.0278	1.104	1.1769	1.2554	1.4326	1.5104	1.5880	1.7083	1.8476	1.9758	2.1060
0.6	0.8372	0.9256	1.0387	1.1697	1.2682	1.3886	1.5358	1.7035	1.7858	1.9837	2.1241
0.7	0.6284	0.7415	0.8736	1.0318	1.1707	1.3179	1.5217	1.6543	1.7875	1.9777	2.1455
0.8	0.4110	0.5620	0.7295	0.8865	1.0511	1.2499	1.4090	1.5768	1.7711	2.0121	2.1960
0.9	0.2101	0.3822	0.5425	0.7394	0.9667	1.1333	1.3386	1.5401	1.7564	1.9760	2.2134
1.0	0.0125	0.2193	0.4247	0.6675	0.8300	1.0564	1.2881	1.4942	1.7398	1.9974	2.2473

Table 6
Defender's payoffs under different combinations of strategies in the scale-free network.

$\Theta_D \backslash \Theta_A$	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0	0.0005	0.1111	0.2076	0.3082	0.4353	0.5372	0.6225	0.7526	0.8477	0.9450	1.0614
0.1	0.2043	0.2831	0.3661	0.4017	0.5138	0.5703	0.6517	0.7285	0.8194	0.8778	0.9490
0.2	0.4166	0.4548	0.5177	0.5336	0.5913	0.6157	0.6695	0.6874	0.7533	0.8009	0.8466
0.3	0.6145	0.6297	0.6320	0.6553	0.6545	0.6638	0.6794	0.7042	0.7085	0.7359	0.7516
0.4	0.8168	0.7976	0.7752	0.7637	0.7351	0.7157	0.6968	0.6940	0.6772	0.6534	0.6414
0.5	1.0252	0.9674	0.9258	0.8765	0.8097	0.7569	0.7166	0.7038	0.6216	0.5866	0.5277
0.6	1.2144	1.1450	1.0631	0.9771	0.8921	0.8225	0.7491	0.6480	0.6026	0.4979	0.4255
0.7	1.4226	1.3244	1.2155	1.0896	0.9874	0.8827	0.7459	0.6441	0.5434	0.4373	0.3229
0.8	1.6391	1.4958	1.3496	1.2265	1.0825	0.9171	0.7974	0.6527	0.5084	0.3372	0.2098
0.9	1.8401	1.6719	1.5203	1.3446	1.1343	0.9883	0.8081	0.6381	0.4604	0.2857	0.1135
1.0	2.0307	1.8291	1.6256	1.3888	1.2299	1.0183	0.8080	0.6239	0.4120	0.2015	0.0064

the attacker's strategy to obtain the most profit is Θ_A^*, and the equilibrium solution is $(1,\ \Theta_A^*)$.

In summary, the equilibrium solution of the optimization problem $(A: \max B^A\ ,\ D: \max B^D)$ can have the following situations.

$$\mathit{Attacker}:\ \max B^A,\ \mathit{Defender}:\ \max B^D$$

$$\mathit{If}\ \Theta_A^* > \Theta_A^\#,\quad \left(\Theta_D = \Theta_D^\Lambda, \Theta_A = \Theta_A^*\right)$$

$$\begin{cases} B^A = P{*}TC{*}\left[R_{\Theta_A^*\Theta_D^\Lambda}\left(1-\Theta_A^*\right)\left(1-\dfrac{\overline{C}_{HCE}{*}\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{*}\dfrac{\Theta_D^*{*}P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^\Lambda\Theta_A^*}\Theta_D^\Lambda{*}\Theta_A^*\right] \\ B^D = \dfrac{\Theta_D^\Lambda{*}\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}{*}\dfrac{P^2{*}TC}{\overline{C}_{ECE}}+\Theta_A^*P{*}TC\left[\left(1-\Theta_D^\Lambda\right)-\dfrac{\Theta_D^\Lambda P}{\overline{C}_{ECE}}{*}\dfrac{\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}\right] \end{cases}. \tag{41}$$

$$\mathit{Attacker}:\ \max B^A,\ \mathit{Defender}:\ \max B^D$$

$$\mathit{If}\ \Theta_A^* = \Theta_A^\#,\quad \left(\Theta_D = \Theta_D^*, \Theta_A = \Theta_A^* = \Theta_A^\#\right)$$

$$\begin{cases} B^A = P{*}TC{*}\left[R_{\Theta_A^*\Theta_D^*}\left(1-\Theta_A^*\right)\left(1-\dfrac{\overline{C}_{HCE}{*}\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{*}\dfrac{\Theta_D^*{*}P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^*\Theta_A^*}\Theta_D^*{*}\Theta_A^*\right] \\ B^D = \dfrac{\Theta_D^*{*}\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}{*}\dfrac{P^2{*}TC}{\overline{C}_{ECE}}+\Theta_A^*P{*}TC\left[\left(1-\Theta_D^*\right)-\dfrac{\Theta_D^*P}{\overline{C}_{ECE}}{*}\dfrac{\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}\right] \end{cases}. \tag{42}$$

$$\mathit{Attacker}:\ \max B^A,\ \mathit{Defender}:\ \max B^D$$

$$\mathit{If}\ \Theta_A^* < \Theta_A^\#$$

i) $\left(\Theta_D = 1,\ \Theta_A = \Theta_A^*\right)$

$$\begin{cases} B^A = P{*}TC{*}\left[R_{\Theta_A^*\Theta_D}\left(1-\Theta_A^*\right)\left(1-\dfrac{\overline{C}_{HCE}{*}\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{*}\dfrac{P}{\overline{C}_{ECE}}\right)+R_{\Theta_D\Theta_A^*}{*}\Theta_A^*\right] \\ B^D = \dfrac{\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}{*}\dfrac{P^2{*}TC}{\overline{C}_{ECE}}-\Theta_A^*P{*}TC\dfrac{P}{\overline{C}_{ECE}}{*}\dfrac{\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T} \end{cases}. \tag{43}$$

ii) $\left(\Theta_D = \Theta_D^2, \Theta_A = \Theta_A^*\right)$

$$\begin{cases} B^A = P{*}TC{*}\left[R_{\Theta_A^*\Theta_D^2}\left(1-\Theta_A^*\right)\left(1-\dfrac{\overline{C}_{HCE}{*}\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{*}\dfrac{\Theta_D^2{*}P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^2\Theta_A^*}{*}\Theta_D^2{*}\Theta_A^*\right] \\ B^D = \dfrac{\Theta_D^2{*}\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}{*}\dfrac{P^2{*}TC}{\overline{C}_{ECE}}+\Theta_A^*P{*}TC\left[\left(1-\Theta_D^2\right)-\dfrac{\Theta_D^2P}{\overline{C}_{ECE}}{*}\dfrac{\overline{C}_T{*}\overline{C}_{HCE}}{\overline{C}_{HCE}-P{*}\overline{C}_T}\right] \end{cases}. \tag{44}$$

5. Simulation verification analysis

In order to verify the correctness of the above analysis with a mixed strategy, we construct a scale-free network that satisfies the following properties: total number of nodes $N = 1000$, average connectivity degree $\langle k \rangle \approx 6$, degree distributions following$p(k) \sim k^{-2.45}$, and a real network: The email network [51] with$N = 1133$nodes and $E = 4567$ edges is also used for analysis and verification. In order to facilitate analysis, we choose the appropriate parameter set, as shown in Table 2.

The simulation results are shown in Figs. 8–11, and the theoretical results are as follows. Each value is obtained through 50 independent simulations, and the random effects are processed by averaging. Tables 3–6 show the data calculated by the simulation.

1 Optimization: *Attac*ker : min B^D, ***Defender*** : max B^D

Scale-Free Network:

$$\underset{\Theta^D\quad\Theta^A}{minmax}B^D = \frac{\overline{C}_T{}^*\overline{C}_{HCE}{}^*P^2{}^*TC}{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P^*\overline{C}_T\right)+\overline{C}_T{}^*\overline{C}_{HCE}{}^*P} = 671.94$$

$$\Theta_D^* = \frac{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P^*\overline{C}_T\right)}{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P^*\overline{C}_T\right)+P^*\overline{C}_T{}^*\overline{C}_{HCE}} = 0.664 \quad . \qquad (45)$$

The equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.664)$.
Email Network:

$$\underset{\Theta^D\quad\Theta^A}{minmax}B^D = 806.69 \qquad \Theta_D^* = 0.728 \qquad (46)$$

The equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.728)$.
The simulation results are shown in Fig. 8.

1 Optimization: *Attac*ker : min B^D, ***Defender*** : min B^A

Scale-Free Network:

$$B^D = \frac{\overline{C}_T{}^*\overline{C}_{HCE}{}^*P^2{}^*TC}{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P^*\overline{C}_T\right)+\overline{C}_T{}^*\overline{C}_{HCE}{}^*P} = 671.94 \qquad (47)$$

$$B^A = \min\begin{cases} R_{\Theta_A\Theta_D^*}P^*TC^*\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^*{}^*P}{\overline{C}_{ECE}}\right)+\mathrm{Z}\left(0,\Theta_D^*\right) & \begin{cases}\Theta_A = 0\\ \Theta_D = \Theta_D^*\end{cases} \\ R_{\Theta_D^*\Theta_A}\Theta_D^*P^*TC+\mathrm{Z}\left(1,\Theta_D^*\right) & \begin{cases}\Theta_A = 1\\ \Theta_D = \Theta_D^*\end{cases}\end{cases} .$$

$$= \min\begin{cases} 1328.13+\mathrm{Z}\left(0,\Theta_D^*\right) & \begin{cases}\Theta_A = 0\\ \Theta_D = \Theta_D^*\end{cases} \\ 1328.13+\mathrm{Z}\left(1,\Theta_D^*\right) & \begin{cases}\Theta_A = 1\\ \Theta_D = \Theta_D^*\end{cases}\end{cases} \qquad (48)$$

Usually, in a scale-free network, the equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.664)$.
Email Network:

$$B^D = 806.69 \qquad B^A = \min\begin{cases} 2158.8+\mathrm{Z}\left(0,\Theta_D^*\right) & \left(\begin{cases}\Theta_A = 0\\ \Theta_D = \Theta_D^*\end{cases}\right) \\ 2158.8+\mathrm{Z}\left(1,\Theta_D^*\right) & \left(\begin{cases}\Theta_A = 1\\ \Theta_D = \Theta_D^*\end{cases}\right)\end{cases} . \qquad (49)$$

The simulation shows that $\mathrm{Z}(1,\Theta_D^*)$is much larger than $\mathrm{Z}(0,\Theta_D^*)$, and the equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.728)$.
The simulation results are shown in Fig. 9.

1 Optimization: *Attac*ker : max B^A , ***Defender*** : min B^A

Scale-Free Network:

$$\Theta_D^c = \frac{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right)}{\overline{C}_{ECE}{}^*\left(\overline{C}_{HCE}-P\overline{C}_T\right)+\overline{C}_{HCE}{}^*\overline{C}_T{}^*P} = 0.664 \quad . \qquad (50)$$

$$\Theta_D^\Lambda = \left[\langle k\rangle/\left(\langle k^2\rangle-\langle k\rangle\right)\right]^{\frac{1}{2}} = 0.3163$$

Since $\Theta_D^\Lambda < \Theta_D^c$, according to Eq. (32), the optimal solution is:

$$\underset{\Theta_A\quad\Theta_D}{maxmin}B^A = P^*TC\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^\Lambda{}^*P}{\overline{C}_{ECE}}\right)+\mathrm{Z}\left(0,\Theta_D^\Lambda\right)$$
$$= 1682.68+\mathrm{Z}\left(0,\Theta_D^\Lambda\right). \qquad (51)$$

The equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.3163)$.
Email Network:

$$\Theta_D^c = 0.728 \qquad \Theta_D^\Lambda = 0.4334 \qquad (52)$$

Since $\Theta_D^\Lambda < \Theta_D^c$, according to Eq. (32), the optimal solution is:

$$\underset{\Theta_A\quad\Theta_D}{maxmin}B^A = P^*TC\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^\Lambda{}^*P}{\overline{C}_{ECE}}\right)+\mathrm{Z}\left(0,\Theta_D^\Lambda\right)$$
$$= 2485+\mathrm{Z}\left(0,\Theta_D^\Lambda\right). \qquad (53)$$

The equilibrium solution is $(\Theta_A = 0, \Theta_D = 0.4334)$.
The simulation results are shown in Fig. 10.

1 Optimization: *Attac*ker : max B^A , ***Defender*** : max B^D

The previous analysis knows that $\Theta_D^\Lambda < \Theta_D^*$. Therefore, there is Θ_A^* that maximizes the benefit of the attacker. Then, according to Eq. (41), Eq. (42), Eq. (43), and Eq. (44), we need to judge whether Θ_A^* satisfies the following relationship.

$$\mathrm{Scale-FreeNetwork}: \begin{cases}\Theta_A^* > 0.336 & \Theta_D \to 0\\ \Theta_A^{*1} = 0.336 & \Theta_D = \Theta_D^*\\ \Theta_A^* < 0.336 & \Theta_D \to 1\end{cases} . \qquad (53a)$$

$$\mathrm{EmailNetwork}: \begin{cases}\Theta_A^* > 0.272 & \Theta_D \to 0\\ \Theta_A^{*1} = 0.272 & \Theta_D = \Theta_D^*\\ \Theta_A^* < 0.272 & \Theta_D \to 1\end{cases} . \qquad (54)$$

The simulation results of the scale-free network show that$\Theta_A^{*1} \approx 0.1$. Additionally, according to Eq. (40), there is $\Theta_D^2 \approx 0.9$.

$$B^A = P^*TC^*\left[R_{\Theta_A^*\Theta_D^2}\left(1-\Theta_A^*\right)\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^2{}^*P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^2\Theta_A^*}{}^*\Theta_D^2{}^*\Theta_A^*\right].$$
$$= R_{\Theta_A^*\Theta_D^2}{}^*979.6+184.68^*R_{\Theta_D^2\Theta_A^*} \qquad (55)$$

$$B^D = \frac{\Theta_D^2{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}+\Theta_A^*P^*TC\left[\left(1-\Theta_D^2\right)-\frac{\Theta_D^2P}{\overline{C}_{ECE}}{}^*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right].$$
$$= 839.59 \qquad (56)$$

Therefore, the equilibrium solution is $(\Theta_D = 0.9, \quad \Theta_A = 0.1)$.
The results of the email network satisfy the fact that $\Theta_A^{*1} \approx 0.1$ and $\Theta_D^2 \approx 0.7$.

$$\begin{aligned} B^A &= P^*TC^*\left[R_{\Theta_A^*\Theta_D^2}\left(1-\Theta_A^*\right)\left(1-\frac{\overline{C}_{HCE}{}^*\overline{C}_T}{\overline{C}_{HCE}-P\overline{C}_T}{}^*\frac{\Theta_D^2{}^*P}{\overline{C}_{ECE}}\right)+R_{\Theta_D^2\Theta_A^*}{}^*\Theta_D^2{}^*\Theta_A^*\right]. \\ &= R_{\Theta_A^*\Theta_D^2}{}^*1970.67+207.57^*R_{\Theta_D^2\Theta_A^*} \end{aligned} \tag{57}$$

$$\begin{aligned} B^D &= \frac{\Theta_D^2{}^*\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}{}^*\frac{P^2{}^*TC}{\overline{C}_{ECE}}+\Theta_A^*P^*TC\left[\left(1-\Theta_D^2\right)-\frac{\Theta_D^2P}{\overline{C}_{ECE}}{}^*\frac{\overline{C}_T{}^*\overline{C}_{HCE}}{\overline{C}_{HCE}-P^*\overline{C}_T}\right]. \\ &= 764.32 \end{aligned} \tag{58}$$

The equilibrium solution is $(\Theta_D = 0.7, \quad \Theta_A = 0.1)$.

The simulation results are shown in Fig. 11.

6. Conclusions and discussions

Critical infrastructure plays an important role in modern society. Game theory provides a proper framework to model confrontations in critical infrastructure between strategic attackers and defenders. Recent studies have analyzed the influence of the fault relationship between the components of a system from the perspective of the network structure. However, cascading failure is a network failure propagation phenomenon that has more destructive effects than structural failures. In this article, we analyze the game equilibrium of network offensive and defensive strategies under the influence of the cascade effect.

We study a simultaneous-move attacker-defender game model, which is a two-player static game with complete information. First, the nodes are divided into two types according to the cascading influence, and the focus of the game is transformed into the resource allocation of the two types of nodes, which greatly simplifies the calculation space for an offensive and defensive network game. The purpose of the attacker is to destroy the network, and his/her profit is determined by the failed nodes and isolated nodes; the defender's profit depends on how many attacked nodes are successfully protected. Since the resources are limited, when a pure strategy is adopted, defenders will tend to protect High Cost-Efficient ratio nodes (HCE nodes), while attackers will choose to attack Equal Cost-Effective ratio nodes (ECE nodes). This result is in line with normal cognition. In the mixed strategy model, in order to obtain greater benefits, the defender will first take action to transfer resources from the HCE nodes to the ECE nodes. Additionally, the attacker will take different actions according to different purposes. Four kinds of optimization problems are studied, and their stability conditions are analyzed. For different optimization goals, the defender and the attacker will adopt different strategies. Therefore, the decision of the strategy first needs to clarify the goals of both parties. Especially from the perspective of the attacker's payoffs, compared with the result that does not consider the cascading influence, the attacker adds a new stable strategy with the cascading effect, and the equilibrium solution of the strategy is related to the structural properties of the network, which has a significant impact on the equilibrium solution of the game.

Our research is intended to examine the local cascading impact model with a single network, but in reality, the attributes and relationships of a network are more diverse. Intermediate failures and partial failures are more realistic models, and an attack and defense game with interdependent networks and a time-dependent network has greater challenges. Next, we will study the impact of network attacks and defense games with structural coupling, for which intermediate failure and partial failure are some of the important issues. There are different cascade propagation rules, incomplete network information, the sequence of attack and defense, etc. Any changes will have a great impact on the balance of an offense and defense game. In summary, there are many problems in network offense and defense that are worth exploring.

Author statement

All the authors who have made substantial contributions to the manuscript "Attack-Defense Game for Critical Infrastructure Considering the Cascade Effect" are following:

Fu Chaoqi: Conceptualization, Methodology, Software, Formal analysis, Writing - Original Draft.

Gao Yangjun: Software, Formal analysis, Validation.

Zhong Jilong: Formal analysis, Validation, Writing - Review & Editing.

Sun Yun: Data Curation, Writing- Reviewing and Editing, Visualization.

Zhang Pengtao: Resources, Writing- Reviewing and Editing.

Wu Tao: Investigation, Writing- Reviewing and Editing.

All persons who have made substantial contributions to the work reported in the manuscript, including those who provided editing and writing assistance but who are not authors, are named in the Acknowledgments section of the manuscript and have given their written permission to be named. If the manuscript dose not include Acknowledgments, it is because the authors have not received substantial contributions from nonauthors.

CRediT authorship contribution statement

Fu Chaoqi: Conceptualization, Methodology, Software, Formal analysis, Writing – original draft. **Gao Yangjun:** Software, Formal analysis, Validation. **Zhong Jilong:** Formal analysis, Validation, Writing – review & editing. **Sun Yun:** Data curation, Writing – review & editing, Visualization. **Zhang Pengtao:** Resources, Writing – review & editing. **Wu Tao:** Investigation, Writing – review & editing.

Declaration of Competing Interest

We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled "Attack-Defense Game for Critical Infrastructure Considering the Cascade Effect".

Acknowledgments

This work was supported by the National Natural Science Foundations of China under Grant No. 72001213 and the Basic research program of Natural Science in Shaanxi Province of China (No. 2021JQ-369). We thank LetPub (www.letpub.com) for its linguistic assistance during the preparation of this manuscript.

References

[1] Brown GG, Carlyle WM, Salmeron J, et al. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses; 2005.

[2] Alcaraz C, Zeadally S. Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 2015.

[3] Ezell BC, Bennett SP, Winterfeldt DV, et al. Probabilistic risk analysis and terrorism risk. Risk Anal 2010;30(4):575–89.

[4] Golany B, Kaplan EH, Marmur A, et al. Nature plays with dice – terrorists do not: allocating resources to counter strategic versus probabilistic risks. Eur J Oper Res 2009;192(1):198–208.

[5] Brown GG, Cox LA. How probabilistic risk assessment can mislead terrorism risk analysts. Risk Anal 2011;31(2):196–204.

[6] Shieh E, An B, Yang R, et al. PROTECT: a deployed game theoretic system to protect the ports of the United States. In: International Conference on Autonomous Agents & Multiagent Systems; 2012.

[7] Tsai J, Kiekintveld C, Ordóñez F, et al. Iris-a tool for strategic security allocation in transportation networks. In: Proc.the 8th International Conference on Autonomous Agents and Multiagent Systems; 2009. p. 37–44.

[8] Guan P, He M, Zhuang J, et al. Modeling a Multitarget Attacker–Defender game with budget constraints. Decision Analysis 2017;14(2):87–107.

[9] Task-Force UCPSO. Final report on the August 14, 2003 blackout in the United States and Canada: causes and Recommendations. 2004; [Online]. Available: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFina L-Web. pdf.

[10] Rao NS, Poole SW, Ma CY, et al. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. Risk Anal 2016;36(4):694–710.

[11] Li D, Fu B, Wang Y, et al. Percolation transition in dynamical traffic network with evolving critical bottlenecks. Proc Natl Acad Sci USA 2015;112:669–72.

[12] Albert R, Barabasi AL. Statistical mechanics of complex networks. Rev Mod Phys 2002;26(1):xii.

[13] Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. Risk Anal 2011;31:1196.

[14] Li YF, Sansavini G, Zio E. Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. Reliab Eng Syst Saf 2013;111:195–205.

[15] Albert R, Jeong H, Barabasi AL. Error and attack tolerance of complex networks. Nature 2000;406(6794):378–82.

[16] Camerer CF, Ho TH, Chong JK. Behavioural game theory: thinking, learning and teaching. Advances in Understanding Strategic Behavior. Palgrave Macmillan UK; 2004.

[17] Arce DG, Kovenock D, Roberson B. Weakest-link attacker-defender games with multiple attack technologies. Naval Res Logs 2012;59(6):457–69.

[18] Salmeron J, Wood K, Baldick R. Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst 2015;19(2):905–12.

[19] Zhu Q, Basar T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Syst 2015;35(1):46–65.

[20] Nystrom JK, Robbins MJ, Deckro RF, et al. Simulating attacker and defender strategies within a dynamic game on network topology. J Simulat 2018;12(4): 307–31.

[21] Hausken K, Levitin G. Review of systems defense and attack models. Int J Performab Eng 2012;8(4):355–66.

[22] Zhang J, Zhuang J. Modeling a multi-target attacker-defender game with multiple attack types. Reliab Eng Syst Saf 2019;185(may):465–75.

[23] Jing Z, Zhuang J, Jose V. The role of risk preferences in a multi-target defender-attacker resource allocation game. Reliab Eng Syst Saf 2018:169.

[24] Zhang J, Wang Y, Zhuang J. Modeling multi-target defender-attacker games with quantal response attack strategies. Reliab Eng Syst Saf 2021:205.

[25] Lin C, Xiao H, Peng R, et al. Optimal defense-attack strategies between M defenders and N attackers: a method based on cumulative prospect theory. Reliab Eng Syst Saf 2021:210.

[26] Nochenson A, Heimann CFL. Simulation and game-theoretic analysis of an attacker-defender game. In: International Conference on Decision & Game Theory for Security. Springer; 2012.

[27] Pita James, Jain, et al. Using game theory for los angeles airport security. Ai Magazine 2009.

[28] Paruchuri P, Pearce JP, Marecki J, et al. Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games. In: International Joint Conference on Autonomous Agents & Multiagent Systems. DBLP; 2008.

[29] Nochenson Alan, Heimann CFLarry. Simulation and game-theoretic analysis of an attacker-defender game, decision and game theory for security. Berlin Heidelberg: Springer; 2012.

[30] Rao NS, Poole SW, Ma CY, et al. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. Risk Anal 2016;36(4):694–710.

[31] Kjell Hausken. Defense and attack for interdependent systems. Eur J Oper Res 2017.

[32] Hausken K, Levitin G. Minmax defense strategy for complex multi-state systems. Reliab Eng Syst Saf 2009;94(2):577–87.

[33] Zhang X, Ding S, Ge B, et al. Resource allocation among multiple targets for a defender-attacker game with false targets consideration. Reliab Eng Syst Saf 2021: 211.

[34] Zhuang J, Bier VM, Gupta A. Subsidies in interdependent security with heterogeneous discount rates. Eng. Econ 2007;52(1):1–19.

[35] Zhuang J. Impacts of subsidized security on stability and total social costs of equilibrium solutions in an N-Player game with errors. Eng Econ 2010;55(2): 131–49.

[36] Li Ya-Peng, Tan Suo-Yi, et al. Attacker-defender game from a network science perspective. Chaos 2018;28(5):051102.

[37] Li Y, Xiao Y, Li Y, et al. Which targets to protect in critical infrastructures - A game-theoretic solution from a network science perspective. IEEE Access 2018:1. -1.

[38] Li Y, Qiao S, Deng Y, et al. Stackelberg game in critical infrastructures from a network science perspective. Physica A: Statal Mech Appl 2019.

[39] Zeng C, Ren B, Li M, et al. Stackelberg game under asymmetric information in critical infrastructure system: from a complex network perspective. Chaos 2019;29 (8):083129.

[40] Yw Zc A, Hg A, et al. Defender-attacker-operater: tri-level game-theoretic interdiction analysis of urban water distribution networks. Reliab Eng Syst Saf 2021.

[41] X.J. Shan, J. Zhuang. A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. Reliab Eng Syst Saf, 195.

[42] Motter AE, Lai Y-C. Cascade-based attacks on complex networks. Phys Rev E 2002; 66:065102.

[43] Zhong J, Sanhedrai H, Zhang FM, et al. Network endurance against cascading overload failure. Reliability Engineering? Syst. Saf. 2020;201:106916.

[44] Buldyrev SV, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks. Nature 2010;464(7291):1025.

[45] Tas S, Bier VM. Addressing vulnerability to cascading failure against intelligent adversaries in power networks. Energy Syst 2016;7(2):193–213.

[46] Chaoqi F, Ying W, Kun Z, et al. Complex networks under dynamic repair model. Phys. A Statal Mech. Appl. 2017;490:323–30.

[47] Wu BC, Tang AP, Wu J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliab Eng Syst Saf 2016;147:1–8.

[48] Khanna V. Interconnectedness and Interdependencies of Critical Infrastructures: implications for Resilience in the U.S. Economy. Physica A Statal Mech Appl 2015; 436:865–77.

[49] Barabá Si A. Emergence of scaling in random networks. Science 1999;286(5439): 509–12.

[50] Newman MEJ, Strogatz SH, Watts DJ. Random graphs with arbitrary degree distributions and their applications. The Structure and Dynamics of Networks; 2011.

[51] Wikipedia editor 2014 https://github.com/gephi/gephi/wiki/Datasets. [2016.10.15].