Attacker-defender game from a network science perspective

Ya-Peng Li, Suo-Yi Tan, Ye Deng, and Jun Wu[a)]
College of Systems Engineering, National University of Defense Technology, Changsha, Hunan 410073, People's Republic of China

(Received 13 March 2018; accepted 26 April 2018; published online 10 May 2018)

Dealing with the protection of critical infrastructures, many game-theoretic methods have been developed to study the strategic interactions between defenders and attackers. However, most game models ignore the interrelationship between different components within a certain system. In this paper, we propose a simultaneous-move attacker-defender game model, which is a two-player zero-sum static game with complete information. The strategies and payoffs of this game are defined on the basis of the topology structure of the infrastructure system, which is represented by a complex network. Due to the complexity of strategies, the attack and defense strategies are confined by two typical strategies, namely, targeted strategy and random strategy. The simulation results indicate that in a scale-free network, the attacker virtually always attacks randomly in the Nash equilibrium. With a small cost-sensitive parameter, representing the degree to which costs increase with the importance of a target, the defender protects the hub targets with large degrees preferentially. When the cost-sensitive parameter exceeds a threshold, the defender switches to protecting nodes randomly. Our work provides a new theoretical framework to analyze the confrontations between the attacker and the defender on critical infrastructures and deserves further study. *Published by AIP Publishing.* https://doi.org/10.1063/1.5029343

Critical infrastructures play a vital role in modern society. The protection of these complex systems with limited resources is challenging and attracts significant attention by security agencies. The attackers who aim to destruct these critical infrastructures are intelligent decision-makers. As such, the prevention of such attacks requires our protection measures to be strategic. However, the interrelationship nature of components within a system poses great challenge in analyzing and protecting them. Here, we use a game-theoretic framework to analyze this problem and take a network science perspective to understand these systems, in which the idea is new.

I. INTRODUCTION

Modern society is dependent on its critical infrastructures, such as communication, electrical power, rail, and fuel distribution networks.[1,2] This dependence has made critical infrastructures to be the military targets in times of war. For example, in the U.S. Civil War, the rail junction of Chattanooga became a key military objective, and telegraph networks were also attacked. More recently, in the former Yugoslavia, the U.S. Air Force temporarily disabled electrical power stations by dropping conductive fibers. Moreover, critical infrastructures are also targeted by terrorists. Terrorist attacks on electrical power networks, rail networks, and oil pipelines have occurred in Colombia, India, Pakistan, Turkey, Algeria, and Spain. There are enormous public investments in each critical infrastructure system. Thus, even a minor disruption, randomly or deliberately caused, can degrade the systems performance and inflict substantial economic losses.[3] It is essential for us to analyze the vulnerability of such a system facing a set of coordinated terrorist attacks and make informed proposals to reduce its vulnerability.

Probabilistic risk assessment (PRA) is a traditional technique for non-deliberate threats such as natural disasters, technological failures, and accidents. Many researchers and organizations, including the U.S. Department of Homeland Security (DHS), have attempted to use PRA to analyze critical infrastructure investment and protection.[4] PRA models require the probabilities of events to be defined as static inputs. However, growing evidence indicates that static probabilities are inappropriate for modeling the behaviors of an intelligent adversary.[5,6]

Recently, there has been significant research interest in game-theoretic approaches dealing with the protection of infrastructure systems.[7–12] Game theory is the study of mathematical models of conflict and cooperation between intelligent decision-makers and therefore offers a more appropriate framework to model the situations where defenders want to protect critical infrastructures from attack by building defenses, while attackers aim to attack in a maximally harmful manner. Brown *et al.*[3] introduce the general attacker-defender game model, where the defender's object is to minimize the total operating costs obtained by summing the operating costs of individual components, and the attacker's aim is to maximize the costs by attacking some components. Nochenson and Heimann[13] propose an agent-based attacker-defender game in a computer network, in which the value of an individual computer is preassigned randomly in the simulation. In this game, the defender's utility is the total loss of the attacked machines minus the costs of protecting some machines. The attacker's payoff is the total value of the machines that he attacks. This paper also considers some

[a)]Electronic mail: junwu@nudt.edu.cn

typical attack and defense strategies. Guan *et al.*[14] models a multi-target attacker-defender game with budget constraints in both sequential form and simultaneous form. Both the attacker and the defender have different valuations for each target, and the probability that whether a target is successfully attacked is determined by a contest success function. They find that a higher proportion of defense resources should be allocated to the most valuable target if the defender's budget is low while the attacker is less concentrated on attacking the most valuable target as his budget increases. Many applications based on game-theoretic models have also been deployed in airports,[15] ports,[16] transportation,[17] and many other infrastructures.[18,19]

However, most of these game models treat the targets as independent ones[14,20] and evaluate the payoffs of the players by summing up the valuations of individual targets.[13] This means that there is an exact valuation associated with each target, which may be given by security specialists in advance. However, in many critical infrastructure systems where targets are networked, the functionality relies heavily on their connectivity and topology structures, which means that the importance of a target is not only determined by its monetary value but also affected by its neighbors in the network. The failure of some targets individually may make limited difference on the functionality of the network, but it can have a devastating effect when these targets are attacked simultaneously. For example, the cascading failure caused by merely two power lines led to the blackouts in 11 states in the U.S. in 1996.[21] This inspires us to depict critical infrastructures as networked systems and consider a holistic view to tackle this problem. Therefore, different from the previous optimization-based game models, in this paper we will evaluate the effect caused by attack from a network science perspective and explore the equilibrium results between the strategic attacker and the defender. The article is structured as follows. In Sec. II, we introduce the cost model, strategies, payoffs of the game, and define two typical strategies. The simulation pseudocode of the payoff matrix and the solving method in a LP formulation are shown in Sec. III. Sections IV and V show the equilibrium results of the game. Finally, we provide a conclusion in Sec. VI.

II. ATTACKER-DEFENDER GAME MODEL

Consider a target network formalized in terms of a simple undirected graph $G(V, E)$, where V is the set of nodes and $E \subseteq V \times V$ is the set of edges. Suppose $N = |V|$ be the number of nodes in the network. We denote $A(G) = (a_{ij})_{N\times N}$ as the adjacency matrix of G, where $a_{ij} = a_{ji} = 1$ if nodes v_i and v_j are adjacent, and $a_{ij} = a_{ji} = 0$ otherwise. Let $k_i = \sum_{j=1}^{N} a_{ij}$ be the degree of node v_i, which equals the number of edges connected to node v_i. Average degree $\langle k \rangle$ of the whole network is $\langle k \rangle = \frac{1}{N}\sum_{i=1}^{N} k_i$.

We only consider one attacker and one defender in this paper, which are the players of the game model. We assume that both players can obtain the complete information of the target network and full knowledge about the opponent, that is, the available resources of each other and costs of each target, thus they are perfectly informed of the payoffs of the other player for all possible strategy profiles. Moreover, we assume that both players move simultaneously without knowing the decision made by the other player and the game is a single shot one.

In this paper, we assume that the attack as well as the defense approaches are against nodes and the attached edges are removed if one node is removed. Suppose c_i^A and c_i^D be the attack cost and defense cost of node v_i, respectively. We assume that the cost c_i^A or c_i^D is a function of a certain referential property $r_i \geq 0$ of node v_i with the following forms:

$$c_i^A = r_i^{q_A}, \quad c_i^D = r_i^{q_D}, \tag{1}$$

where $q_A \geq 0$ is the *attack-cost-sensitive parameter* and $q_D \geq 0$ is the *defense-cost-sensitive parameter*. Apparently, a target with larger r is costlier for both players, particularly when q_A or q_D is large. In the extreme case where $q_A = 0$, the attack costs toward each target are homogeneous. Besides, the parameters q_A and q_D may have different values in a specific system and are exogenously determined by the system itself, which can be evaluated by security experts with historical data. For instance, the costs to protect different computers in a computer network from attacking by virus are almost equal, while attacking hub stations in a railway network is much costlier. The referential property r_i can be set as the degree, the betweenness, or other structural measures of nodes. Further, the available resources of the attacker and the defender are defined as

$$\hat{C}^A = \theta_A \sum_{i=1}^{N} c_i^A = \theta_A \sum_{i=1}^{N} r_i^{q_A} \tag{2}$$

and

$$\hat{C}^D = \theta_D \sum_{i=1}^{N} c_i^D = \theta_D \sum_{i=1}^{N} r_i^{q_D}, \tag{3}$$

respectively, where $\theta_A \in [0, 1]$ is the *attack-cost-constraint parameter* and $\theta_D \in [0, 1]$ is the *defense-cost-constraint parameter*. The parameters θ_A and θ_D indicate the sufficiency of the budgets for the two players.

Denote by $V^A \subseteq V$ the set of nodes are attacked. We define an attack strategy as $X = [x_1, x_2, \ldots x_N] \in S_A$, where S_A is the strategy set of the attacker and $x_i = 1$ if $v_i \in V^A$, otherwise $x_i = 0$. Let $C_X = \sum_{v_i \in V^A} c_i^A$ be the total cost of the attack strategy X. It is easy to identify that

$$C_X = \sum_{v_i \in V^A} c_i^A = \sum_{i=1}^{N} x_i c_i^A = \sum_{i=1}^{N} x_i r_i^{q_A}. \tag{4}$$

Thus, the budget constraint of the attacker is

$$C_X = \sum_{i=1}^{N} x_i r_i^{q_A} \leq \hat{C}^A = \theta_A \sum_{i=1}^{N} r_i^{q_A}. \tag{5}$$

Any solution X that satisfies Eq. (5) is a feasible attack strategy. Similarly, the defended nodes set V^D and defense strategy $Y = [y_1, y_2, \ldots y_N] \in S_D$ are defined in the same way as the attacker. A feasible defense strategy satisfies

$$C_Y = \sum_{i=1}^{N} y_i r_i^{q_D} \le \hat{C}^D = \theta_D \sum_{i=1}^{N} r_i^{q_D}. \tag{6}$$

We assume that a node v_i will be removed if it is attacked but not defended, that is, if $x_i = 1$ and $y_i = 0$. Conversely, a defended node $(y_i = 1)$ is never removed. We denote the set of nodes that are removed by $\hat{V} \subseteq V$ and denote the network after the removing process by $\hat{G} = (V - \hat{V}, \hat{E})$. It is easy to identify that

$$\hat{V} = V^A - V^A \cap V^D. \tag{7}$$

The measure function of network performance is denoted by Γ. We assume that if $G_1 = (V_1, E_1)$ is a subgraph of $G_2 = (V_2, E_2)$, i.e., $V_1 \subseteq V_2$ and $E_1 \subseteq E_2$, then $\Gamma(G_1) \le \Gamma(G_2)$. This monotonicity assumption ensures that the network performance declines during the process of nodes removals. The common measure functions include the size of the largest connected component, the efficiency,[22] and so on. Suppose $U^A : S_A \times S_D$ be the payoff function of the attacker and $U^A(X, Y)$ be the payoff received by the attacker when the attacker chooses the strategy X and the defender adopts Y. Thus, the payoff of the attacker is

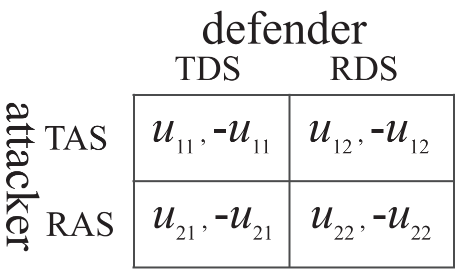
$$U^A(X, Y) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0, 1]. \tag{8}$$

Similarly, the payoff of the defender is defined as

$$U^D(X, Y) = \frac{\Gamma(\hat{G}) - \Gamma(G)}{\Gamma(G)} \in [-1, 0]. \tag{9}$$

Noting that $U^A(X, Y) + U^D(X, Y) = 0$, this attacker-defender game is a two-player zero-sum game.

According to Eqs. (5) and (6), the strategy space of the players will be extremely large for large network size N. For example, when $\theta_A = \theta_D = 1$, $|S_A| = |S_D| = 2^N \approx 10^{30}$ with $N = 100$. Thus, the total number of strategy profiles $|S_A \times S_D|$ is more than 10^{60}, where few techniques are available to solve this game model using brute force. Besides, the payoff function of the game model has a non-explicit formulation, where decomposition methods and compact representation used in the previous studies are not executable.[19,23] However, with limited decision-support information and computing power, decision-makers in most real-world scenarios generally choose a better one from several options. We assume that the attacker follows some simple criterion to decide which targets to attack and so does the defender. Thus, for the convenience of analysis, we only consider two typical attack and defense strategies, which were first suggested by Albert *et al.*[24] and well-investigated by subsequent research. We define the attack strategies as the *targeted attack strategy* (*TAS*) (corresponding to "intentional attack") and the *random attack strategy* (*RAS*) (corresponding to "random failure"). The TAS prescribes the attacker to allocate all the resource toward targets with the largest referential properties r_i, while the RAS is attacking some targets randomly. We also consider the defense strategies to be the two typical defense strategies, namely, the *targeted defense strategy* (*TDS*) and the *random defense strategy* (*RDS*). Therefore, the payoff matrix under all strategy profiles is shown in Fig. 1, where u_{ij} is the payoff of the attacker when the attacker chooses strategy i and the defender takes strategy j. The row player is the attacker and the column is the defender.



		defender	
		TDS	RDS
attacker	TAS	u_{11}, -u_{11}	u_{12}, -u_{12}
	RAS	u_{21}, -u_{21}	u_{22}, -u_{22}

FIG. 1. Payoff matrix of the attacker-defender game.

Now, we use an example to illustrate how the game is played. The target network is shown in Fig. 2. We set that $q_A = q_D = 1$ and $\theta_A = \theta_D = 0.5$. Besides, we choose degree k_i as the referential property r_i in Eq. (1) and the size of the largest connected component as a measure function Γ in Eq. (8). Thus, the budgets of the two players are both 12. When the attacker chooses the TAS, $X_1 = [1100010000]$. One possible RAS is $X_2 = [1000101101]$. Similarly, $Y_1 = [1100010000]$ and $Y_2 = [0101101011]$. The payoff matrix is shown in Fig. 3, which indicates that the TDS is a dominant strategy for the defender, and the RAS is dominant as well. Therefore, a pure-strategy Nash equilibrium is obtained, where the attacker chooses the RAS and the defender takes the TDS. It is worth mentioning that the random strategy in another realization may induce different payoffs and equilibrium. Therefore, the analysis should be based on the averaged payoffs over many independent realizations.

III. SOLVING THE GAME MODEL

Although the random strategy may not be exactly the same in each independent game, the averaged payoffs over adequate realizations can reveal the most probable case and provide us useful insights. The algorithm pseudocode to obtain the averaged payoff matrix is shown in Algorithm 1.

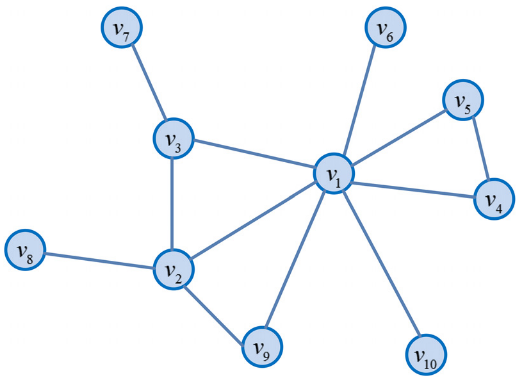
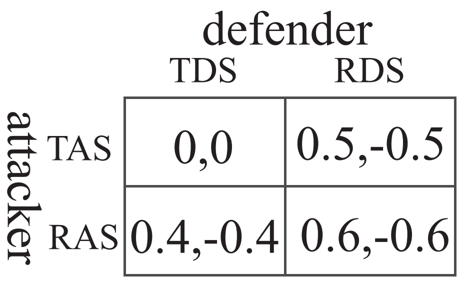


FIG. 2. Topology structure of a target network.



		defender	
		TDS	RDS
attacker	TAS	0,0	0.5,-0.5
	RAS	0.4,-0.4	0.6,-0.6

FIG. 3. Payoff matrix of the example whose target network is shown in Fig. 2.

ALGORITHM 1: Algorithm pseudocode for obtaining the payoff matrix.

```
Input: A target network $G(V,E)$ whose $N=|V|$, $r_i$, $q_A$, $q_D$, $\theta_A$, $\theta_D$,
       number of independent realizations $N_r$;
Output: payoffs of the attacker $u_{11}$, $u_{12}$, $u_{21}$, and $u_{22}$;
Calculate $r_i$ of $N$ nodes, resort their indexes, denoted by $I_i$, in descending
  order by $r_i$;
Calculate the available resources of the two players:
  $\hat{C}_A=\theta_A\sum_{i=1}^{N} r_i^{q_A}, \hat{C}_D=\theta_D\sum_{i=1}^{N} r_i^{q_D}$.
Initialization: $C_{TAS}^A \leftarrow 0$, $C_{RAS}^A \leftarrow 0$, $C_{TDS}^D \leftarrow 0$, $C_{RDS}^D \leftarrow 0$, $u_{11} \leftarrow 0$,
  $u_{12} \leftarrow 0$, $u_{21} \leftarrow 0$, $u_{22} \leftarrow 0$, $V_{TAS}^A \leftarrow \emptyset$, $V_{RAS}^A \leftarrow \emptyset$, $V_{TDS}^D \leftarrow \emptyset$, $V_{RDS}^D \leftarrow \emptyset$,
  $del_{11} \leftarrow \emptyset$, $del_{12} \leftarrow \emptyset$, $del_{21} \leftarrow \emptyset$, $del_{22} \leftarrow \emptyset$;
for $i=1:N$ do
  if $C_{TAS}^A + r_{I_i}^{q_A} \le \hat{C}_A$ then
    $V_{TAS}^A \leftarrow V_{TAS}^A \cup I_i$, $C_{TAS}^A \leftarrow C_{TAS}^A + r_{I_i}^{q_A}$;
  end if
  if $C_{TDS}^D + r_{I_i}^{q_D} \le \hat{C}_D$ then
    $V_{TDS}^D \leftarrow V_{TDS}^D \cup I_i$, $C_{TDS}^D \leftarrow C_{TDS}^D + r_{I_i}^{q_D}$;
  end if
end for
$X_1 \leftarrow zeros(1,N)$, $X_1(V_{TAS}^A) \leftarrow 1$, $Y_1 \leftarrow zeros(1,N)$, $Y_1(V_{TDS}^D) \leftarrow 1$;
loop $N_r$ times
    $ra \leftarrow randperm(1:N)$, $rd \leftarrow randperm(1:N)$;
    for $i=1:N$ do
      if $C_{RAS}^A + r_{ra_i}^{q_A} \le \hat{C}_A$ then
        $V_{RAS}^A \leftarrow V_{RAS}^A \cup ra_i$, $C_{RAS}^A \leftarrow C_{RAS}^A + r_{ra_i}^{q_A}$;
      end if
      if $C_{RDS}^D + r_{rd_i}^{q_D} \le \hat{C}_D$ then
        $V_{RDS}^D \leftarrow V_{RDS}^D \cup rd_i$, $C_{RDS}^D \leftarrow C_{RDS}^D + r_{rd_i}^{q_D}$;
      end if
    end for
    $X_2 \leftarrow zeros(1,N), X_2(V_{RAS}^A) \leftarrow 1, Y_2 \leftarrow zeros(1,N), Y_2(V_{RDS}^D) \leftarrow 1$;
$del_{11} \leftarrow find(X_1 - Y_1 == 1)$, $del_{12} \leftarrow find(X_1 - Y_2 == 1)$,
  $del_{21} \leftarrow find(X_2 - Y_1 == 1)$, $del_{22} \leftarrow find(X_2 - Y_2 == 1)$;
$pay_{11} \leftarrow \frac{\Gamma(G)-\Gamma(G-del_{11})}{\Gamma(G)}$, $pay_{12} \leftarrow \frac{\Gamma(G)-\Gamma(G-del_{12})}{\Gamma(G)}$, $pay_{21} \leftarrow \frac{\Gamma(G)-\Gamma(G-del_{21})}{\Gamma(G)}$,
  $pay_{22} \leftarrow \frac{\Gamma(G)-\Gamma(G-del_{22})}{\Gamma(G)}$, $u_{11} \leftarrow u_{11} + pay_{11}$, $u_{12} \leftarrow u_{12} + pay_{12}$,
  $u_{21} \leftarrow u_{21} + pay_{21}$, $u_{22} \leftarrow u_{22} + pay_{22}$, $V_{RAS}^A \leftarrow \emptyset$, $V_{RDS}^D \leftarrow \emptyset$;
end loop
$u_{11} \leftarrow u_{11}/N_r$, $u_{12} \leftarrow u_{12}/N_r$, $u_{21} \leftarrow u_{21}/N_r$, $u_{22} \leftarrow u_{22}/N_r$.
```

After the payoff matrix is obtained, we use a linear programming to solve this zero-sum game and find its Nash equilibrium. Suppose z is the expected payoff for the attacker and $U=(u_{ij})$ is the payoff matrix of the attacker. The probability that the attacker and defender adopt strategy i is denoted by p_i^A and p_i^D, respectively. The optimization model of the defender is defined as follows:

$$\begin{aligned} & min\, z \\ & s.t. \sum_{j\in S_D} u_{ij}\cdot p_j^D \le z \qquad \forall i \in S_A \\ & \quad \sum_{j\in S_D} p_j^D = 1 \\ & \quad p_j^D \ge 0 \qquad \forall j \in S_D. \end{aligned} \tag{10}$$

In the first constraint, for every pure strategy i of the attacker, the expected payoff for playing any strategy $i\in S_A$ given the mixed strategy p^D of the defender is at most z, and these pure strategies for which the expected utility is exactly z will be in the best response set of the attacker. The optimization model of the attacker is

$$\begin{aligned} & max\, z \\ & s.t. \sum_{i\in S_A} u_{ij}\cdot p_i^A \ge z \qquad \forall j \in S_D \\ & \quad \sum_{i\in S_A} p_i^A = 1 \\ & \quad p_i^A \ge 0 \qquad \forall i \in S_A. \end{aligned} \tag{11}$$

By solving this linear programming, a Nash equilibrium (p^{A*}, p^{D*}) is obtained and the equilibrium payoff of the attacker is $z = p^{A*T}\cdot U \cdot p^{D*}$ and that of the defender is $-z$.

IV. ATTACK AND DEFENSE STRATEGIES IN NASH EQUILIBRIUMS

For the ubiquity of scale-free networks in natural and man-made systems, we consider the target networks to be scale-free networks in this paper, whose degree distributions follow $P(k)\sim k^{-\lambda}$, where λ is the degree exponent. We also use degree k_i as the referential property r_i and the size of the largest connected component as a measure function Γ, similar to the above example. First, we set $q_A = q_D \equiv q$ and $\theta_A = \theta_D \equiv \theta = 0.5$. For each parameter configuration, the payoffs are averaged over 5000 independent realizations to obtain Nash equilibriums.

We show in Fig. 4 the equilibrium strategies of the two players with different values of q. When $q=0.1$, the attacker takes the RAS with a probability of 1 and the defender always chooses the TDS. This pure-strategy equilibrium is denoted by (RAS, TDS). When $q=0.5$, both players take mixed strategies in equilibrium where the probability of the RAS is approximately 0.9 and the defender chooses the RDS with a probability of approximately 1. In the case of $q=0.9$, both players take the random strategy in equilibrium, which is (RAS, RDS). It is easy to observe that the attacker always takes the RAS with an extremely large probability regardless of q, while the defender prefers the TDS when q is small and shifts to the RDS when q increases.

To investigate the equilibrium strategies in depth, we show the payoffs of the attacker as a function of q under all strategy profiles in Fig. 5. Owing to the zero-sum feature of the game, the payoffs of the defender are negations of the attacker's and not shown. There are two thresholds of q in this figure, namely, $q_1^* = 0.25$ which makes $u_{21}=u_{22}$ and $q_2^* = 0.55$ where $u_{12}=u_{22}$. When $q<q_1^*$, the TDS is

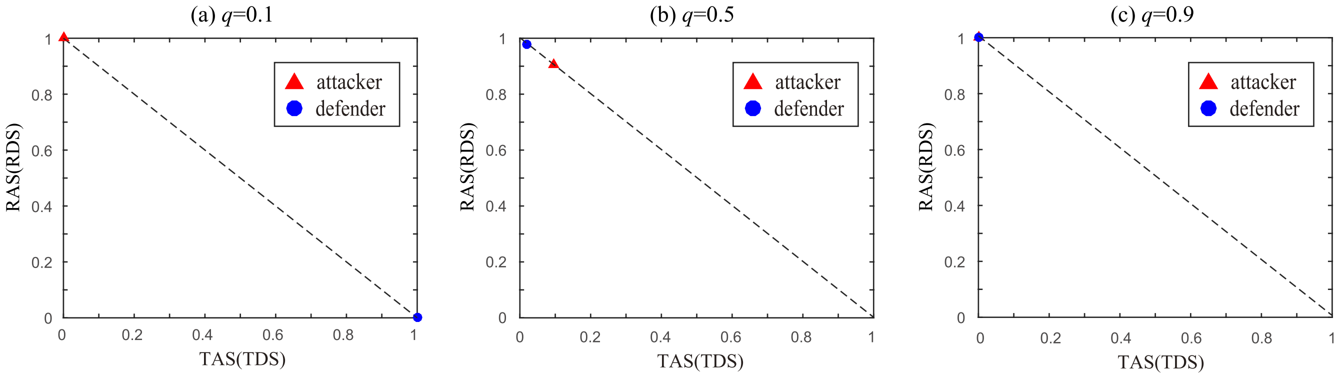


FIG. 4. Equilibrium strategies of the players when $q = 0.1$ (a), $q = 0.5$ (b), and $q = 0.9$ (c). The target network is a random scale-free network whose $N = 1000$, $\lambda = 3$, and $\langle k \rangle = 4$. The probability of the attacker to take the TAS in Nash equilibrium is shown on the horizontal axis and that of the RAS corresponds with the vertical axis. Therefore, the equilibrium points are at all times on the dashed line, whose two ends represent pure-strategy equilibriums.

dominant for the defender as $u_{12} > u_{11}$ and $u_{22} > u_{21}$. Thus, the Nash equilibrium is (RAS, TDS). When $q > q_2^*$, the RAS becomes strictly dominant ($u_{21} > u_{11}$ and $u_{22} > u_{12}$) and the equilibrium is (RAS, RDS). When $q_1^* < q < q_2^*$, there are no dominant strategy for both players, which means the equilibriums are mixed ones, where both the attacker and defender adopt the random strategy with a far higher probability.

This result is rooted in the change of cost-sensitive parameters and high heterogeneity of the degree distributions in scale-free networks. As $q_A = q_D$ and $\theta_A = \theta_D$, the attacker's best response to the TDS is always the RAS. When q is small, the number of targets defended with the TDS is almost equal to that with the RDS. However, the targets with larger degrees contribute more to the connectivity of the network, making the TDS more preferable for the defender. Thus, the equilibrium is (RAS, TDS) when $q < q_1^*$. With an increase in q, due to the degree distribution of scale-free networks, the costs of attacking targets with large degrees become much higher, leading to less targets being attacked with the TAS. However, with the RAS, there are many nodes with small degrees removed, whose number is rather large, providing the attacker a considerable payoff. Thus, the attacker's best response to the RDS is the random attack strategy in this case. Therefore, the attacker prefers choosing the RAS regardless of the defender's choice. The defender's best response to the RAS is the RDS in this case, as targets with large degrees are also too costly to defend. Thus, the equilibrium becomes (RAS, RDS). Moreover, the mixed strategies indicate that both players take the random strategy in most cases because the random strategies have much higher probabilities in the equilibriums when $q_1^* < q < q_2^*$. When the attacker allocates a higher probability on the TAS, a much lower payoff will be obtained, because $u_{11} = 0$ and the defender will adopt the TDS to get a higher payoff in this case. Therefore, the probability of the RAS will be far higher in the attacker's mixed equilibrium strategy, making the defender be indifferent between the two defense strategies. Besides, the defender will also choose the RDS with a higher probability in equilibrium because $u_{21} > u_{22}$.

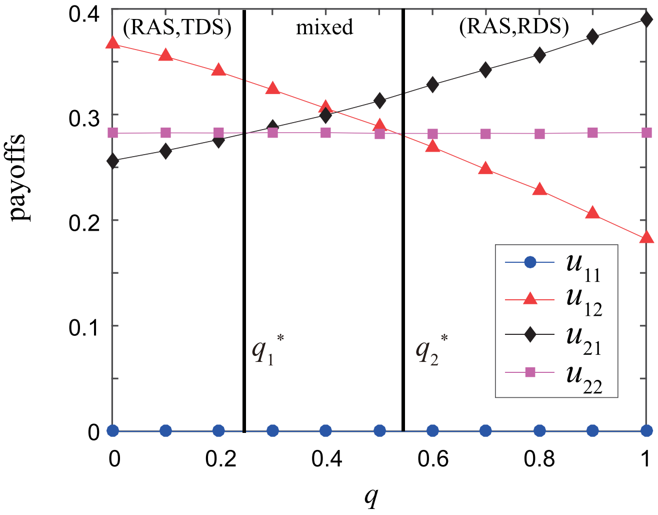


FIG. 5. Payoffs of the attacker in the payoff matrix versus q. The target network is the same as that used in Fig. 4.

To validate our methods and results, we investigate the equilibrium strategies with various parameters. First, we implement simulations when $q_A \neq q_D$ and find that the result is quite similar to our previous one, particularly when the difference between q_A and q_D is very minor. Further, we use efficiency as the measure function, which is different from the size of the largest connected component that mainly indicates the reachability of pair-wise nodes in the network. The result exhibits similar pattern, where the only difference lies in the values of q_1^* and q_2^*. Finally, we also investigate the cases with different θ and find similar equilibrium strategies, but it is worth mentioning that the differences among the payoffs in different strategy profiles are not so significant as those when $\theta = 0.5$.

V. INFLUENCE OF TARGET NETWORKS ON EQUILIBRIUM RESULTS

When the topology structure of the target network changes, the payoffs under each strategy profile may be different in comparison to the previous results, which may lead to different equilibrium results. As we have assumed the target networks to be scale-free networks, two parameters, that is, average degree $\langle k \rangle$ and degree exponent λ, may make

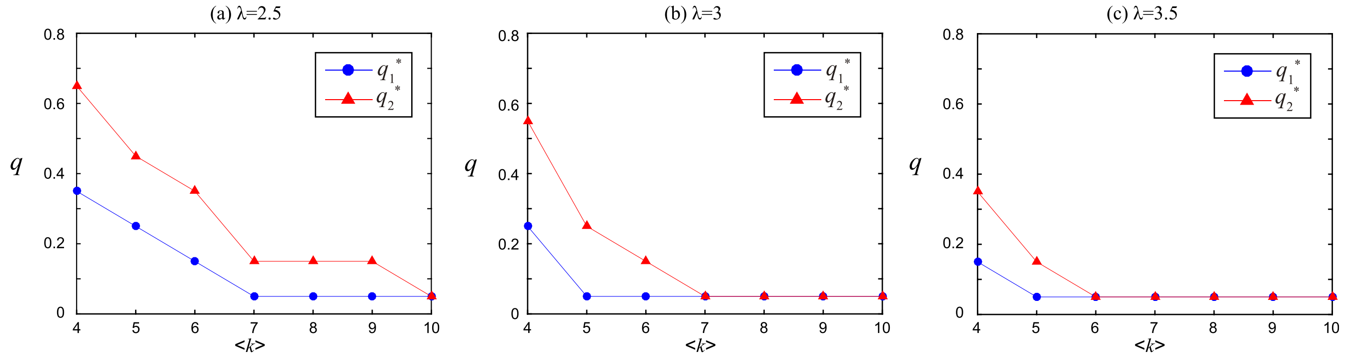


FIG. 6. Thresholds of q versus average degree $\langle k \rangle$ in random scale-free networks with different degree exponents λ. The value of q_1^* and q_2^* is approximated, such as, if $0.3 < q_1^* < 0.4$, $q_1^* = 0.35$.

a difference on equilibrium results. To investigate this influence, we alter these two parameters and obtain the corresponding Nash equilibriums. The equilibriums are similar to the previous results where the equilibrium strategies are (RAS, TDS) when $q < q_1^*$ and (RAS, RDS) when $q > q_2^*$. When $q_1^* < q < q_2^*$, both players take mixed strategies. Additionally, the values of q_1^* and q_2^* are influenced by the topology structure of the target network, shown in Fig. 6. We find that q_1^* and q_2^* both decrease monotonically with an increase in average degree $\langle k \rangle$ regardless of λ. Besides, when $\langle k \rangle$ exceeds a certain value which is larger with a smaller λ, $q_1^* = q_2^*$ and they approximate 0, indicating that the players adopt (RAS, TDS) as equilibrium strategies only when the costs of different targets are extremely homogeneous. Moreover, it is also evident that the networks with a smaller λ have larger q_1^* and q_2^* with the same $\langle k \rangle$.

This result can be explained by the disintegration effectiveness of hub targets with largest degrees. In a less connected network, the TAS will have a superior disintegration effectiveness because the removal of hub targets will generate more small components, which is the case when $\langle k \rangle$ is smaller. This can be seen in Fig. 7(a), where larger $\langle k \rangle$ makes the payoffs u_{12} decrease dramatically. Besides, a network with higher heterogeneity of the degree distribution (smaller λ) is more vulnerable under the TAS, which provides the attacker a higher payoff, as can be seen in Fig. 7(b). However, the disintegration effectiveness of the RAS is mainly determined by the number of targets attacked, which is scarcely affected by $\langle k \rangle$ and λ (Fig. 7). Thus, with increasing $\langle k \rangle$ and λ, q_1^* and q_2^* become smaller.

VI. CONCLUSIONS AND DISCUSSIONS

Defending critical infrastructures in modern society has attracted significant attention of researchers and organizations. Many methods have been proposed to tackle this problem, such as PRA and game-theoretic methods. However, little research considers the interrelationship between the targets to be protected. Different from the previous studies, we think that the value of a target is not only determined by its monetary value but also by the role it plays in the network. Therefore, we evaluate the payoffs of the players in a holistic view.

In this paper, we focus on the interconnection within a certain infrastructure system which is represented by a complex network. An attacker-defender game model is proposed,

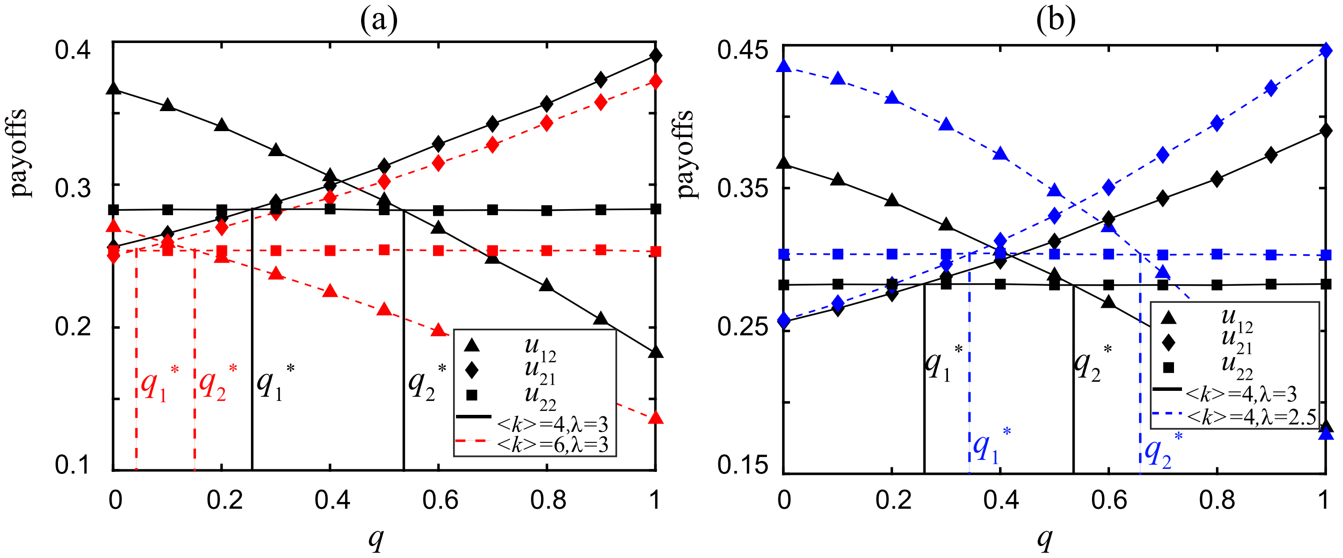


FIG. 7. The payoffs of the attacker versus q with different $\langle k \rangle$ and λ. The payoff u_{11} is always equal to 0 when $q_A = q_D$ and $\theta_A = \theta_D$, which is not shown. The black lines in (a) and (b) are the payoffs of the attacker in a scale-free network whose $N = 1000$, $\lambda = 3$, and $\langle k \rangle = 4$. The red lines in (a) and the blue lines in (b) are the results in scale-free networks with $\langle k \rangle = 6$ and $\lambda = 2.5$, respectively. The two thresholds q_1^* and q_2^* of these three cases are also shown.

which is a two-player zero-sum static game with complete information. The payoffs of the two players are defined as the reduction of network performance. Due to the complexity of the strategies involved, we only consider two typical strategies, namely, targeted strategy and random strategy. We mainly investigate the equilibrium strategies when $\theta_A = \theta_D$ and $q_A = q_D$ in random scale-free networks. The simulation results show that there are two thresholds of q, denoted by q_1^* and q_2^*. The equilibrium is (RAS, TDS) when $q < q_1^*$, which means that the attacker attacks a set of targets randomly and the defender protects the hub targets with large degrees preferentially. When $q > q_2^*$, both players take random strategy. Besides, they both adopt a mixed strategy when $q_1^* < q < q_2^*$. The influence of target networks on the equilibriums is also investigated and explained, which indicates that the larger average degree $\langle k \rangle$ or degree exponent λ are, the smaller q_1^* and q_2^* are.

To the best of our knowledge, the game in this paper is the first one to model the confrontations of the attacker and defender from a network science perspective. It is rather counterintuitive that the attacker virtually always attacks randomly, but this result is confined to the framework where only two strategies are considered. However, the problem of defending critical infrastructures which are networks considering strategic attackers is far from being solved. A more elaborate cost model which depicts more realistic features of the system, larger strategy sets covering more strategies and the sequence of player's moves will be considered in our future work. Moreover, in the real-world, complete information about the target network is not always available for the attacker, which inspires us to explore what the equilibriums will be with incomplete information.

ACKNOWLEDGMENTS

We acknowledge the National Natural Science Foundation of China under Grant No. 71371185 and the Program for New Century Excellent Talents in University under Grant No. NCET-12-0141. We thank Dr. Dong-Mei Fan and Yu Bai for their linguistic assistance during the preparation of this manuscript.

[1] A. H. Dekker, in *Proceedings of 28th Australasian Conference on Computer Science* (Australian Computer Society, 2005), pp. 59–68.
[2] C. Alcaraz and S. Zeadally, Int. J. Crit. Infrastruct. Prot. **8**, 53 (2015).
[3] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, Interfaces **36**, 530 (2006).
[4] B. C. Ezell, S. P. Bennett, D. Von Winterfeldt, J. Sokolowski, and A. J. Collins, Risk Anal. **30**, 575 (2010).
[5] G. G. Brown and L. A. T. Cox, Jr., Risk Anal. **31**, 196 (2011).
[6] B. Golany, E. H. Kaplan, A. Marmur, and U. G. Rothblum, Eur. J. Oper. Res. **192**, 198 (2009).
[7] D. G. Arce, D. Kovenock, and B. Roberson, Nav. Res. Logist. **59**, 457 (2012).
[8] M. P. Scaparra and R. L. Church, Comput. Oper. Res. **35**, 1905 (2008).
[9] J. Salmeron, K. Wood, and R. Baldick, IEEE Trans. Power Syst. **24**, 96 (2009).
[10] D. L. Alderson, G. G. Brown, W. M. Carlyle, and R. K. Wood, in *Proceedings of 12th INFORMS Computing Society Conference* (INFORMS, 2011), pp. 28–49.
[11] Q. Zhu and T. Basar, IEEE Control. Syst. **35**, 46 (2015).
[12] M. Ouyang, Eur. J. Oper. Res. **262**, 1072 (2017).
[13] A. Nochenson and C. F. L. Heimann, in *International Conference on Decision and Game Theory for Security* (Springer, 2012), pp. 138–151.
[14] P. Guan, M. He, J. Zhuang, and S. C. Hora, Decis. Anal. **14**, 87 (2017).
[15] J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, AI Mag. **30**, 43 (2009).
[16] E. Shieh, B. An, R. Yang, M. Tambe, C. Baldwin, J. DiRenzo, B. Maule, and G. Meyer, in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems* (IFAAMAS, 2012), Vol. 1, pp. 13–20.
[17] J. Tsai, C. Kiekintveld, F. Ordóñez, M. Tambe, and S. Rathi, in *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (IFAAMAS, 2009), pp. 37–44.
[18] Z. Yin, A. X. Jiang, M. P. Johnson, M. Tambe, C. Kiekintveld, K. Leyton-Brown, T. Sandholm, and J. P. Sullivan, in *Proceedings of the 26th AAAI Conference on Artificial Intelligence* (AAAI, 2012), pp. 2348–2355.
[19] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, in *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (IFAAMAS, 2009), Vol. 1, pp. 689–696.
[20] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, in *Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems* (IFAAMAS, 2008), Vol. 2, pp. 895–902.
[21] S. H. Strogatz, Nature **410**, 268 (2001).
[22] V. Latora and M. Marchiori, Phys. Rev. Lett. **87**, 198701 (2001).
[23] P. Paruchuri, J. P. Pearce, M. Tambe, F. Ordonez, and S. Kraus in *Proceedings of the 6th International Conference on Autonomous Agents and Multiagent Systems* (IFAAMAS, 2007), pp. 181–189.
[24] R. Albert, H. Jeong, and A. L. Barabási, Nature **406**, 378 (2000).