IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 20, 2018, accepted September 17, 2018, date of publication September 28, 2018, date of current version October 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872767

Which Targets to Protect in Critical Infrastructures - A Game-Theoretic Solution From a Network Science Perspective

YAPENG LI[1], YU XIAO[1], YONG LI[2], AND JUN WU[1]
[1]College of Systems Engineering, National University of Defense Technology, Changsha 410073, China
[2]School of Economic and Management, Changsha University, Changsha 410022, China

Corresponding author: Yong Li (stoneliyong@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 71371185 and Grant 71871217 and in part by the Program for New Century Excellent Talents in University under Grant NCET-12-0141.

ABSTRACT Modern society is highly dependent on its critical infrastructures. These infrastructures usually suffer intentional attacks, which is a serious threat to social wellbeing, making the protection of them to be a great challenge for the security agencies. Many game models have been proposed to tackle this problem. However, little of them consider the interrelationship of different targets within the infrastructures. In this paper, the protection of critical infrastructures against a malicious attacker is modeled as a simultaneous game, where the payoffs of the players are evaluated on the basis of the topology structure of the infrastructure system. An efficient algorithm is adopted to obtain the Nash equilibrium solution. The experimental results reveal that in the equilibriums, the defender distributes higher probabilities on protecting the targets who are more important, for example, those with large degrees or betweenness, while the attacker prefers attacking targets with medium degrees or betweenness. The effectiveness of the game-theoretic solution is validated, and the experimental results in a real-world network provide us a clear insight on which targets to protect.

INDEX TERMS Critical infrastructures, complex network, game theory, Nash equilibrium.

I. INTRODUCTION

Critical infrastructures, such as transportation, communication and energy transmission, play a vital role in the economic development and social wellbeing of modern societies [1], [2]. In times of war, these infrastructures are important military targets, whose destruction or degradation could have a destructive impact. Moreover, terrorism activities against critical infrastructures have inflicted substantial economic losses and threatened the public health and safety in many countries, for example, in Colombia, India, Pakistan, Turkey, Algeria, and Spain. Therefore, the protection of these infrastructures has received enormous attentions by security agencies and will continue to be paramount in modern society [3].

The attackers are always intentional and intelligent in real-world scenarios, which means that they have the ability to collect the information of the infrastructures and destruct or degrade them in a maximally harmful manner. Game theory offers an appropriate framework to model the confrontations between these intelligent attackers and the defenders who want to maintain the performance of the critical infrastructures as much as possible, and many game models have been proposed [4]–[8]. The applications aiming at the protection of infrastructures based on game-theoretic algorithms have been deployed in airports [9], ports [10], transportations [11] and many other infrastructures [12], [13]. In most previous studies, the components within the infrastructures are treated as independent ones and there is an exact valuation associated with each of them, given by security specialists in advance [13]–[17]. For instance, Guan *et al.* [17] proposed an attacker-defender game with budget constraints, where the valuations of the targets are their monetary values. However, this is not appropriate to depict the infrastructures in real-world scenarios. The Cyber Era has caused the emergence of networks and systems of networks with exponentially increasing complexity, which leads to that the functionalities of networked infrastructures rely heavily on their connectivity and topology structures. The failure of some components may cause devastating effect on the performance of the system. For example, the cascading failure caused by merely two power lines led to the blackouts in

11 states in the U.S. in 1996 [18]. Therefore, it is necessary to evaluate the payoffs of the players in the whole network, rather than to sum the valuations of individual targets up. In our previous study [19], we proposed a simultaneous-move attacker-defender game, which defined the payoffs and the strategies on the basis of the topology structure of the target network. In this game model, we only considered two typical attack and defense strategies, which were the targeted strategy and the random strategy. Nevertheless, the attack and defense approaches in real world are not always selected in such manners.

In this paper, we will take a network science perspective to solve the problem of which targets to protect in critical infrastructures. We model the critical infrastructures as complex networks which depict the fundamental relationships of different targets. To provide a solution on which targets the defender should protect facing the threaten of an intentional attacker, we propose a two-player simultaneous-move game. The valuations of each target are not specified in this game model, but the payoffs of the players are evaluated from the whole network, which is different from the previous studies. Further, we consider all the possible attack and defense strategies and introduce two efficient algorithms to get the payoff matrix and to solve the game model.

II. THE GAME MODEL

An infrastructure system can be easily abstracted as a target network, which is formalized in terms of a simple undirected graph $G(V,\ E)$. Suppose that V is the set of nodes and $E \subseteq V \times V$ is the set of edges. Let $N = |V|$ be the number of nodes in the network. The adjacency matrix of G is denoted by $A(G) = (a_{ij})_{N\times N}$, where $a_{ij} = a_{ji} = 1$ if nodes v_i and v_j are adjacent, and $a_{ij} = a_{ji} = 0$ otherwise.

In this paper, we assume that there is only one attacker who can attack some nodes in the target network to degrade the system's performance, and one defender that aims at maintaining the functionality of the network by protecting a subset of nodes. In other words, the attack and the defense approaches are both against nodes and the attached edges will be removed if one node is removed. It is also assumed that both players can obtain the complete information of the target network and full knowledge about the opponent, namely, the total amount of attack and defense resources. Therefore, they are perfectly informed of all the possible strategies that the opponent may adopt and the payoffs of each other under each strategy profile. Nevertheless, we also assume that the players do not know exactly which nodes the opponent will attack or defend when making their own decisions. Thus, this game is a simultaneous one. One should note that the two players do not have to move at exactly the same time, and it is just required that no players know their adversary's moves before making decisions. Moreover, we assume that the game is played in a single round and it does not repeat for multiple rounds.

Suppose n_A and n_D be the amount of attack and defense resources, respectively, which represent the amount of nodes that the players can attack or defend. Denote by $V^A \subseteq V$ the set of nodes that are attacked, where $\left|V^A\right| = n_A$. We define an attack strategy as $\boldsymbol{X} = [x_1, x_2,\ \ldots\ x_N] \in S_A$, where S_A is the strategy set of the attacker and $x_i = 1$ if $v_i \in V^A$, otherwise $x_i = 0$. Similarly, the defended nodes set V^D and defense strategy $\boldsymbol{Y} = [y_1, y_2,\ \ldots\ y_N] \in S_D$ are defined in the same way as the attacker. We assume that a node v_i is removed only if it is attacked but not protected, that is, if $x_i = 1$ and $y_i = 0$. Conversely, the node will never be removed if it is defended ($y_i = 1$). 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

$$\hat{V} = V^A - V^A \cap V^D. \tag{1}$$

Suppose $U^A : |S_A| \times |S_D|$ be the payoff function of the attacker and $U^A(\boldsymbol{X}, \boldsymbol{Y})$ be the payoff obtained by the attacker when the attacker chooses the strategy $\boldsymbol{X}$ and the defender takes $\boldsymbol{Y}$. The attacker's payoff $U^A(\boldsymbol{X}, \boldsymbol{Y})$ is defined as

$$U^A(\boldsymbol{X}, \boldsymbol{Y}) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0, 1], \tag{2}$$

and the defender's payoff $U^D(\boldsymbol{X}, \boldsymbol{Y})$ is

$$U^D(\boldsymbol{X}, \boldsymbol{Y}) = \frac{\Gamma(\hat{G}) - \Gamma(G)}{\Gamma(G)} \in [-1, 0], \tag{3}$$

where Γ is the measure function of network performance. 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 it is assumed that $\Gamma(G_1) \leq \Gamma(G_2)$. This monotonicity assumption ensures that the network performance declines during the process of nodes removals. The common measure functions can be the size of the largest connected component, the efficiency [20] and so on. Noting that $U^A(\boldsymbol{X}, \boldsymbol{Y}) + U^D(\boldsymbol{X}, \boldsymbol{Y}) = 0$, this game is a two-player zero-sum game. The attacker's aim is to destroy the target network in a maximally harmful way by attacking n_A nodes, which is described by

$$\begin{aligned} &\max_{\boldsymbol{X}\in S_A}\ U^A(\boldsymbol{X}, \boldsymbol{Y}) \\ &s.t.\ \sum_{i=1}^{N} x_i = n_A \\ &\quad x_i = 0, 1. \end{aligned} \tag{4}$$

And the defender's model is

$$\begin{aligned} &\min_{\boldsymbol{Y}\in S_D}\ U^A(\boldsymbol{X}, \boldsymbol{Y}) \\ &s.t.\ \sum_{i=1}^{N} y_i = n_D \\ &\quad y_i = 0, 1. \end{aligned} \tag{5}$$

III. ALGORITHM

For the simultaneous game we have proposed, it is worth mentioning that there does not exist any pure strategy Nash equilibrium. Suppose that a strategy $\boldsymbol{X}^*$ is an attack strategy in a Nash equilibrium, the attacker can obtain a higher payoff when he/she deviates to a strategy $\boldsymbol{X}'$ where more attacked

nodes are not defended, which is a contradiction. Whenever the attacker tries to attack a set of nodes, the defender would protect as many nodes within the attack set V^A as he/she can. Therefore, they can never reach to a pure strategy Nash equilibrium. The proof of this result can be seen in Appendix.

Therefore, our main purpose is to compute and analyze the mixed strategies in Nash equilibriums. To solve the game model, we need to calculate the payoffs of the players in each strategy profile and construct the payoff matrix first. However, the sizes of the attack and defense strategy sets are incredibly large even in a small network. For example, when $N = 100$ and $n_A = 5$, there are more than 7×10^7 different pure attack strategies, making the payoff matrix be incredibly large. It is very time-consuming to calculate the payoffs in each strategy profile one by one. However, for a given attack strategy $\boldsymbol{X}$, the payoffs of the players are only determined by which targets are removed eventually. Thus, the removed nodes set $\hat{V}$ is the subset of attacked nodes set V^A, and there are only $2^{|V^A|}$ outcomes of different payoffs. Therefore, we use an efficient algorithm to construct the payoff matrix as described in Algorithm 1. Because the game is a zero-sum one, we only compute the payoffs of the attacker.

Algorithm 1 An Efficient Algorithm to Construct the Payoff Matrix

Input: n_A, n_D

Output: payoff matrix of the attacker $U^A_{|S_A|\times|S_D|}$;

1: Enumerate all the attack strategies $\boldsymbol{X} \in S_A$ and the defense strategies $\boldsymbol{Y} \in S_D$;
2: **for** $i = 1 : |S_A|$ **do**
3: Enumerate all the subsets $\hat{V}_k \in V^A$ under the attack strategy $\boldsymbol{X}_i$, which represent the nodes that will be removed (the empty set $\emptyset$ means that there are no nodes removed), and calculate the corresponding payoffs of the attacker $U^A(\hat{V}_k)$ as eq. (2);
4: **for** $j = 1 : |S_D|$ **do**
5: $\hat{V}_{ij} \leftarrow find(\boldsymbol{X}_i - \boldsymbol{Y}_j == 1)$;
6: $U^A_{ij} \leftarrow U^A(\hat{V}_k | \hat{V}_k = \hat{V}_{ij})$;
7: **end for**
8: **end for**

As we have pointed out, this game is a two-player zero-sum game. However, solving a game, even in the case of two players, has been known to be intractable [21]. For this game with extremely large strategies sets, typical algorithms such as the linear programming proposed by Tardos and Vazirani [22], the Lemke-Howson method [23] and Porter-Nudelman-Shoham (PNS) algorithm [24], are too time-consuming to be efficiently implemented. In this paper, we adopt the algorithm proposed by Godinho and Dias [25], [26] to obtain the Nash equilibriums, which is also adopted by Zhang *et al.* [7]. This algorithm cannot identify all the Nash equilibrium solutions that exist, but it is guaranteed to find one. The algorithm is described as:

Step 1. Let $t = 1$, start from an pure attack strategy $\boldsymbol{X}^t$ which attacks the nodes with the largest degrees, satisfying the resource constraint. Then, identify the defender's best response to $\boldsymbol{X}^t$, which is a pure strategy $\boldsymbol{Y}^t$.

Step 2. Let $t = t + 1$, identify the attacker's pure strategy best response $\boldsymbol{X}^t$ to $\boldsymbol{Y}^{t-1}$, and then also calculate the defender's pure strategy best response $\boldsymbol{Y}^t$ to $\boldsymbol{X}^t$.

Step 3. If $\boldsymbol{Y}^t = \boldsymbol{Y}^{t-1}$, $(\boldsymbol{X}^t, \boldsymbol{Y}^t)$ is a pure strategy Nash equilibrium, stop. Otherwise, if $\boldsymbol{Y}^t = \boldsymbol{Y}^{t-l}$, for any $l = t - e$ where e is an positive integer and $1 < e < t$, let $\overline{S_A} = \{\boldsymbol{X}^k | l < k \leq t\}$ and let $\overline{S_D} = \{\boldsymbol{Y}^k | l < k \leq t\}$. Otherwise, go to **Step** 2.

Step 4. Compute the Nash equilibrium $(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D})$ ($\overline{\boldsymbol{\sigma}_A} = [p_1, p_2, \ldots, p_i, \ldots, p_{|\overline{S_A}|}]$ and $\overline{\boldsymbol{\sigma}_D} = [q_1, q_2, \ldots, q_j, \ldots, q_{|\overline{S_D}|}]$ are vectors that represent the probability distributions of the two players over each pure strategy) of the restricted game whose attack strategy set is $\overline{S_A}$ and defense strategy set is $\overline{S_D}$. For this restricted game, a linear programming shown in eq.(6) and eq.(7) is adopted in this paper.

Step 5. Calculate a pure strategy best response of the attacker, $\boldsymbol{X}^* \in S_A$, to the mixed defense strategy $\overline{\boldsymbol{\sigma}_D}$, and calculate the best response $\boldsymbol{Y}^* \in S_D$ to $\overline{\boldsymbol{\sigma}_A}$ for the defender as well.

Step 6. If $U^A(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D}) = U^A(\boldsymbol{X}^*, \overline{\boldsymbol{\sigma}_D})$ and $U^A(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D}) = U^A(\overline{\boldsymbol{\sigma}_A}, \boldsymbol{Y}^*)$, then $(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D})$ is a mixed Nash equilibrium for the initial game, stop. Otherwise, if $U^A(\boldsymbol{X}^*, \overline{\boldsymbol{\sigma}_D}) > U^A(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D})$, $\overline{S_A} \leftarrow \overline{S_A} \cup \boldsymbol{X}^*$. And if $U^A(\overline{\boldsymbol{\sigma}_A}, \boldsymbol{Y}^*) > U^A(\overline{\boldsymbol{\sigma}_A}, \overline{\boldsymbol{\sigma}_D})$, $\overline{S_D} \leftarrow \overline{S_D} \cup \boldsymbol{Y}^*$. Go to **Step** 5.

The linear programming to solve the reduced zero-sum game in the algorithm above is

$$\begin{aligned} &min\ z \\ &s.t. \sum_{j\in\overline{S_D}} u_{ij} \cdot q_j \leq z \quad \forall i \in \overline{S_A} \\ &\sum_{j\in\overline{S_D}} q_j = 1 \\ &q_j \geq 0 \quad \forall j \in \overline{S_D}, \end{aligned} \tag{6}$$

and

$$\begin{aligned} &max\ z \\ &s.t. \sum_{i\in\overline{S_A}} u_{ij} \cdot p_i \geq z \quad \forall j \in \overline{S_D} \\ &\sum_{i\in\overline{S_A}} p_i = 1 \\ &p_i \geq 0 \quad \forall i \in \overline{S_A}, \end{aligned} \tag{7}$$

where eq.(6) is the defender's optimization model and eq.(7) is the attacker's. In these equations, z is the expected payoff of the attacker and u_{ij} is the payoff of the attacker under the strategy profile $(\boldsymbol{X}_i, \boldsymbol{Y}_j)$.

In the first step of the algorithm above, the algorithm starts form an attack strategy which attacks the nodes with the largest degrees, which is different from the algorithm described by Godinho and Dias [25], [26]. This improvement can reduce the steps before reaching a pure strategy equilibrium or a cycle, because the selected attack strategy can inflict serious damage on the network and the defender are only

TABLE 1. Probability distributions over pure strategies in the mixed strategy Nash equilibrium. In this experimentation, we set $n_A = n_D = 4$. The strategies shown in this table are in the support set of the mixed strategy Nash equilibrium, which have positive probabilities.

Attack strategy	{1,2,5,8}	{2,6,8,10}	{3,5,10,13}	{4,6,7,12}	{4,6,12,13}	{4,8,12,13}			
Probability	0.1017	0.0508	0.3390	0.3390	0.0932	0.0763			
Defense strategy	{1,3,4,6}	{1,3,4,7}	{1,3,7,13}	{1,4,12,13}	{1,6,7,12}	{2,3,4,12}	{2,4,7,13}	{3,4,6,12}	{3,6,7,12}
Probability	0.1667	0.0021	0.2761	0.1031	0.2189	0.0636	0.0551	0.0438	0.0706

motivated to protect the nodes that may be attacked. When identifying the best pure strategy best response of one player, for example, the attacker, to the opponent's, if there are multiple pure attack strategies with the same payoff which is the largest, we find the defender's second best responses to these pure attack strategies. We then compare the attacker's payoffs under the strategy profiles composed of the pure attack strategies and the pure defense strategies which are second best responses. We choose one pure attack strategy with the highest payoff as the attacker's pure strategy best response. If the payoffs of the second best response strategies are also equal, we choose one of them randomly.

Because the number of pure strategies for the initial game is finite, this algorithm is sure to converge to an equilibrium and the worst case happens when all pure strategies are added into the restricted game. However, in the experiments we have implemented, the size of the pure strategies in the support set of Nash equilibriums is extremely small compared with the size of all pure strategies. Thus, this method is very efficient for our game.

IV. EXPERIMENTAL RESULTS

A. NASH EQUILIBRIUM OF THE GAME MODEL

We first implement an experimentation in a target network, whose topology structure is shown in Fig. 1, to validate our proposed model and algorithm. We use the size of the largest connected component as the measure function Γ in eq.(2). The algorithms proposed in the previous section are coded in Matlab and the linear programming is solved by calling CPLEX.

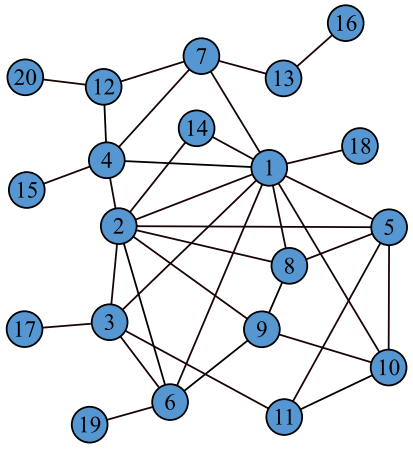


FIGURE 1. Topology structure of the target network with 20 nodes and 35 edges.

We show the mixed strategy Nash equilibrium of the proposed game in Table 1 when both the attacker and the defender can attack or protect 4 nodes. In the attacker's support set of the Nash equilibrium, there are 6 pure strategies in total, and the probabilities distributed on the strategies $\{3, 5, 10, 13\}$ and $\{4, 6, 7, 12\}$ are highest. Likewise, the defender's support set has 9 pure strategies and the defender allocates the highest probability on the strategy $\{1, 3, 7, 13\}$.

From the Nash equilibrium, we find that the attacker's support set is significantly different from that of the defender's. To show which nodes are more preferable for the two players, we map the probabilities over pure strategies to those over each node in the following manner

$$\boldsymbol{\rho}_A = \frac{1}{n_A}\sum_{i=1}^{|S_A|} p_i \cdot \boldsymbol{X}_i = \frac{1}{n_A}\boldsymbol{\sigma}_A \cdot \boldsymbol{X}_{|S_A|\times N}, \tag{8}$$

$$\boldsymbol{\rho}_D = \frac{1}{n_D}\sum_{j=1}^{|S_D|} q_j \cdot \boldsymbol{Y}_j = \frac{1}{n_D}\boldsymbol{\sigma}_D \cdot \boldsymbol{Y}_{|S_D|\times N}, \tag{9}$$

where $\boldsymbol{\rho}_A = [\widetilde{p}_1, \widetilde{p}_2, \ldots, \widetilde{p}_i, \ldots, \widetilde{p}_N]$ and $\boldsymbol{\rho}_D = [\widetilde{q}_1, \widetilde{q}_2, \ldots, \widetilde{q}_j, \ldots, \widetilde{q}_N]$ are the probability distributions over individual nodes of the two players, and $\boldsymbol{\sigma}_A = [p_1, p_2, \ldots, p_i, \ldots, p_{|S_A|}]$ and $\boldsymbol{\sigma}_D = [q_1, q_2, \ldots, q_i, \ldots, q_{|S_D|}]$ are the probability distributions over all the attack and defense strategies. The probability distributions over nodes mapped from the Nash equilibrium in Table 1 are shown in Table 2. The nodes attacked with the largest probabilities are v_4, v_5, v_6, v_{12}, v_{13}, whose degrees and betweenness are neither the largest nor the smallest. However, the defender allocates the largest probability on protecting the node v_1 which has the largest degree and betweenness, and the nodes with larger degree and betweenness are protected in larger probabilities generally. Besides, the nodes whose betweenness are 0 are not appeared in neither the attacker's support set nor the defender's support set. We also visualize this result in Fig. 2, which shows the mapped probabilities over each node in the mixed strategy Nash equilibrium.

B. EFFECTIVENESS OF THE EQUILIBRIUM STRATEGY

To verify the effectiveness of the mixed strategy in Nash equilibrium, we compare the results when both players take the *Nash equilibrium strategy (NS)* and some other typical strategies. The NS means the players choose a pure strategy from the support sets of their mixed strategy Nash equilibrium with a probability proportional to the probability distributions. The typical strategies considered in this paper

TABLE 2. Probability distributions over all the individual nodes. The probabilities are mapped from the mixed strategy Nash equilibrium shown in Table 1.

Node index	1	2	3	4	5	6	7	8	9	10
Degree	10	8	5	5	5	5	4	4	4	4
Betweenness	82.5	27.7	24.1	37.7	5.8	20.1	42.4	1.4	2.3	5.2
$\widetilde{p}_i \in \boldsymbol{\rho}_A$	0.03	0.04	0.08	0.13	0.11	0.12	0.08	0.06	0	0.1
$\widetilde{q}_i \in \boldsymbol{\rho}_D$	0.19	0.03	0.16	0.11	0	0.13	0.16	0	0	0
Node index	11	12	13	14	15	16	17	18	19	20
Degree	3	3	2	2	1	1	1	1	1	1
Betweenness	1.7	18	18	0	0	0	0	0	0	0
$\widetilde{p}_i \in \boldsymbol{\rho}_A$	0	0.13	0.13	0	0	0	0	0	0	0
$\widetilde{q}_i \in \boldsymbol{\rho}_D$	0	0.13	0.11	0	0	0	0	0	0	0

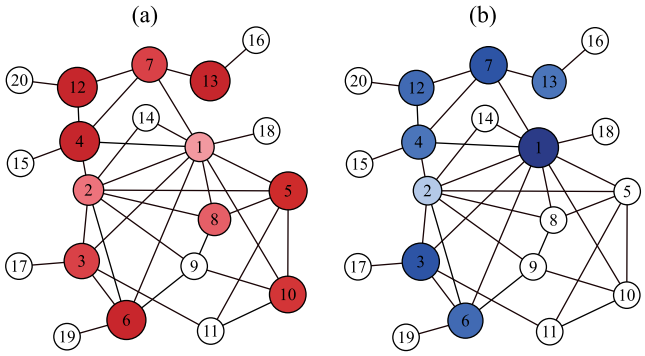


FIGURE 2. Visualization of the probabilities over each node of the attacker (a) and the defender (b). The nodes with larger size and deeper color are attacked or protected with higher probabilities in the Nash equilibrium.

are the *hub nodes strategy (HS)*, which means the players choose the nodes with the largest degrees to attack or defend, the *leaf nodes strategy (LS)*, which represents that the players attack or protect the leaf nodes whose degrees are smallest, and the *random strategy (RS)*, where the players choose their targets randomly. The results are shown in Table 3, where the row is the attacker's strategies and the column represents the defender's strategies. In each realization of the game, the NS and the RS may be different and therefore induce different payoffs. Thus, the payoffs shown in Table 3 are averaged over 5000 independent realizations. The results show that apart from the LS, no matter which strategy the attacker takes, the defender can obtain almost the highest payoff with the NS (the defender's payoff is the opposite of the attacker's). This means the mixed strategy in the Nash equilibrium is efficient for the defender even when the attacker is not strategic.

TABLE 3. The payoffs of the attacker when the two players take different kinds of typical strategies. The NS is the Nash equilibrium strategy. The HS represents the hub nodes strategy. The LS is the leaf nodes strategy and the RS represents the random strategy.

attacker's strategy	defender's strategy			
	NS	HS	LS	RS
NS	0.219	0.267	0.417	0.33
HS	0.211	0	0.65	0.483
LS	0.2	0.2	0	0.161
RS	0.191	0.212	0.253	0.227

Further, if we define a new simultaneous game whose pure strategies are the 4 strategies shown in Table 3, the Nash equilibrium of this new game is also a mixed one, where the attacker's mixed strategy is [0.81, 0.19, 0, 0] and the defender's mixed strategy is [0.9996, 0.0004, 0, 0]. Both the attacker and the defender take the NS with an extremely large probability, which also validates the effectiveness of the Nash equilibrium strategy.

When the attacker and the defender have unsymmetrical attack and defense resources, which means n_A and n_D are not equal, the Nash equilibriums are different. We also implement experiments with different n_A and n_D, and the results are similar with that in the case when $n_A = n_D = 4$, where the attacker prefers nodes which are neither hub nodes nor leaf nodes while the defender protects the hub nodes with larger probabilities. Nevertheless, the nodes contained in the support set of Nash equilibrium are different in these cases and the equilibrium payoffs are also distinct. We show the nodes attacked or protected with a probability larger than 0 in Table 4 and the equilibrium payoffs of the attacker in Fig. 3. In Table 4, we find that the attacker attacks more nodes with positive probabilities when the defender can protect more nodes. In Fig. 3, the equilibrium payoffs of the attacker increase almost linearly with n_A in different cases of n_D.

TABLE 4. Nodes attacked or protected with a positive probability with unequal n_A and n_D. The experiment is implemented in the target network shown in Fig. 1.

	$n_A = 3,\ n_D = 4$	$n_A = 4,\ n_D = 3$
attacker	{1,2,3,4,5,6,7,8,9,10,12,13}	{1,2,3,4,5,6,7,10,12,13}
defender	{1,3,4,6,7,12,13}	{1,3,4,6,7,12,13}

C. EXPERIMENTS IN A REAL-WORLD NETWORK

To consider a more realistic networked infrastructure, we also implement experiments in USAir (http://vlado.fmf.uni-lj.si/pub/networks/data/), which is the network of air transportation system in the US. This network has 332 nodes, thus, the amount of the total strategy profiles will be more than 2.4×10^{17} when $n_A = n_D = 4$. The payoff matrix is too big to construct, not to mention solving it. However, in many real-world scenarios, both the attacker and the defender will only focus on the airports which are the busiest.

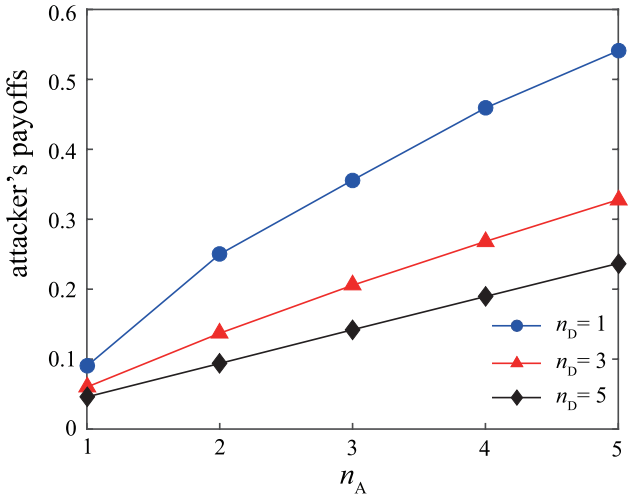


FIGURE 3. Equilibrium payoffs of the attacker versus n_A in different cases of n_D. We only show the payoffs of the attacker because the zero-sum feature of the proposed game.

Besides, the experimental results above indicate that the leaf nodes are neither considered by the attacker nor the defender. Therefore, we define θ_A and θ_D as the attack range and defense range, respectively, and assume that the players only consider attacking or protecting $N \cdot \theta_A$ or $N \cdot \theta_D$ nodes with the largest degrees. When a set of nodes are removed, the players' payoffs are evaluated in the whole network. In this experiment, we use the efficiency as the measure function Γ and we set that $\theta_A = \theta_D = 0.1$ and $n_A = n_D = 3$. We show the probability distributions over pure strategies of the two players in Table 5 and the probability distributions over individual airports mapped from the Nash equilibrium in Table 6. The visualization of this result is shown in Fig.4. It is clear that not all airports within the attack and defense range are attacked or protected with positive probabilities while some

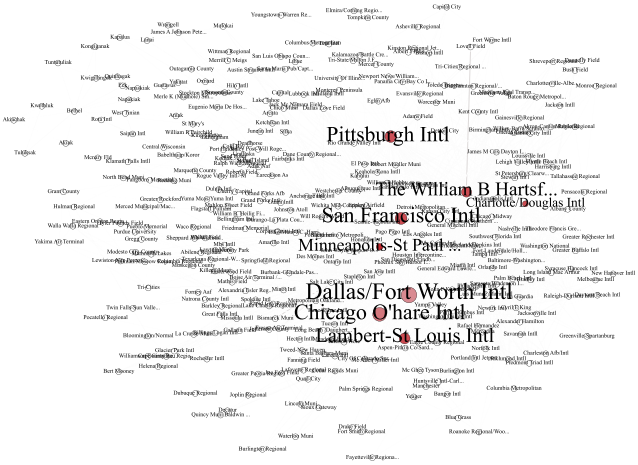


FIGURE 4. Visualization of the attack and defense probabilities over each airport in USAir. The nodes in larger size are defended with larger probabilities and the nodes in deeper color are attacked with larger probabilities.

TABLE 5. Probability distributions over pure strategies in USAir. The indexes of the airports are sorted in the descending order by their degrees.

Attack strategy	{1,4,8}	{1,8,10}	{2,4,10}	{2,8,10}
Probability	0.2195	0.0383	0.0302	0.164
Attack strategy	{3,5,6}	{3,6,10}	{4,8,10}	
Probability		0.3834	0.014	0.1507
Defense strategy	{1,2,3}	{1,2,5}	{1,2,10}	{2,3,10}
Probability	0.0959	0.4477	0.0522	0.0289
Defense strategy	{2,4,10}	{3,4,10}	{4,8,10}	
Probability	0.1165	0.1983	0.065	

TABLE 6. Probability distributions over each airport in USAir. The airports shown in this table are attacked or protected with positive probabilities.

Index	Airport	$\widetilde{p}_i \in \boldsymbol{\rho}_A$	$\widetilde{q}_i \in \boldsymbol{\rho}_D$
1	Chicago O'hare Intl	0.0859	0.1986
2	Dallas/Fort Worth Intl	0.0647	0.2471
3	The William B Hartsfield Atlan	0.1324	0.1077
4	Lambert-St Louis Intl	0.1335	0.1251
5	Pittsburgh Intl	0.1278	0.1492
6	Charlotte/Douglas Intl	0.1324	0
8	Minneapolis-St Paul Intl	0.1908	0.0202
10	San Francisco Intl	0.1324	0.1521

airports are targeted by both players. The airport protected with the largest probability is not attacked with the largest probability. From our results, the security agency should pay more attention to these airports with positive probabilities.

V. CONCLUSION

Deciding which targets to protect in critical infrastructures with limited resources is a key concern of security agencies in many countries. This problem becomes more challenging in this Cyber Era, because the infrastructures usually function as networks and the complexity of these networked systems will increase exponentially with the development of modern society. Therefore, it is not reasonable to only consider the values of individual targets when planning the protection schedules. We should evaluate a target in the whole network and take a network science perspective to tackle the protection of infrastructures. In this paper, we propose a two-player zero-sum simultaneous-move game model. The players' payoffs are defined on the basis of the topology structure of the target network. All the possible attack and defense strategies are considered in this paper. We introduce an efficient algorithm to compute the payoff matrix of the game and adopt an iteration-based algorithm to solve the game. The experimental results in a small size network show that in the mixed Nash equilibrium, the attacker distributes larger probabilities on targets with medium degrees or betweenness while the defender prefers protecting hub targets with the largest degrees. We then validate the effectiveness of the defense strategy. This mixed strategy guarantees the defender much higher payoffs even when the attacker is not strategic. We also implement an experimentation in a real-world network, the USAir, and find similar results. Besides, there are only a limited number of airports appeared in the players'

support set of the mixed strategy Nash equilibrium, which provides the defender useful insights about which targets to protect.

Although we give a game-theoretic solution for defending the critical infrastructures in this paper, there are also some problems to be settled. Because of the extremely large size of the strategy profiles, our algorithm is not applied to the networks with thousands of nodes and to the case when n_A and n_D are large. Besides, our algorithm is guaranteed to get a Nash equilibrium, but we do not know whether this equilibrium provides the defender the highest payoff and which nodes are protected in the optimal equilibrium. In our future work, we will investigate how to construct the payoff matrix in a compact representation and find a more efficient algorithm to solve this game. Besides, the costs to attack or protect different targets are not always equal, which should be considered in our further study. Moreover, in real-world scenarios, the attacker cannot always collect all the information about the target network, which inspires us to explore what the equilibriums will be with incomplete information.

APPENDIX
PROOF OF THE NONEXISTENCE OF PURE STRATEGY NASH EQUILIBRIUM IN THE PROPOSED GAME

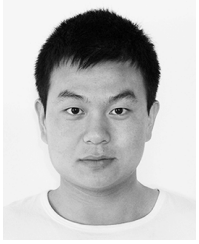
Suppose an arbitrary pair of pure attack and defense strategy to be $(\boldsymbol{X}^*, \boldsymbol{Y}^*)$. Firstly, suppose that $\boldsymbol{Y}^*$ protects at least one node which is attacked by the attacker. In this case, there must exist at least one node not protected whose removal can degrade the network performance. Thus, the attacker prefers the attack strategy $\boldsymbol{X}'$ which contains such nodes and $U^A(\boldsymbol{X}', \boldsymbol{Y}^*) > U^A(\boldsymbol{X}^*, \boldsymbol{Y}^*)$.

Secondly, suppose that the defense strategy $\boldsymbol{Y}^*$ does not protect any nodes within the attack strategy $\boldsymbol{X}^*$. Because of the assumption that the network performance declines monotonically with the removal of nodes, there must exist a defense strategy $\boldsymbol{Y}'$ that can protect at least one node within $\boldsymbol{X}^*$. Thus, $U^D(\boldsymbol{X}^*, \boldsymbol{Y}') > U^D(\boldsymbol{X}^*, \boldsymbol{Y}^*)$.

In all, for every pair of pure strategies, at least one player can obtain a higher payoff by changing their strategies unilaterally. Thus, there does not exist pure-strategy Nash equilibrium in the proposed game. ■

REFERENCES

[1] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.
[2] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Protection*, vol. 8, pp. 53–66, Jan. 2015.
[3] J. E. Ramirez-Marquez, C. M. Rocco, and G. Levitin, "Optimal protection of general source–sink networks via evolutionary techniques," *Rel. Eng. Syst. Saf.*, vol. 94, no. 10, pp. 1676–1684, Oct. 2009.
[4] D. L. Alderson, G. G. Brown, W. M. Carlyle, and R. K. Wood, "Solving defender-attacker-defender models for infrastructure defense," in *Proc. 12th INFORMS Comput. Soc. Conf.*, Monterey, CA, USA, 2011, pp. 28–49.
[5] D. G. Arce, D. Kovenock, and B. Roberson, "Weakest-link attacker-defender games with multiple attack technologies," *Nav. Res. Logistics*, vol. 59, no. 6, pp. 457–469, 2012.
[6] Q. Zhu and T. Basar, "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.*, vol. 35, no. 1, pp. 46–65, Feb. 2015.
[7] C. Zhang, J. E. Ramirez-Marquez, and J. Wang, "Critical infrastructure protection using secrecy—A discrete simultaneous game," *Eur. J. Oper. Res.*, vol. 242, no. 1, pp. 212–221, Apr. 2015.
[8] M. Ouyang, "A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks," *Eur. J. Oper. Res.*, vol. 262, no. 3, pp. 1072–1084, Nov. 2017.
[9] J. Pita *et al.*, "Using game theory for Los Angeles airport security," *AI Mag.*, vol. 30, no. 1, pp. 43–57, 2009.
[10] E. A. Shieh *et al.*, "PROTECT: A deployed game theoretic system to protect the ports of the United States," in *Proc. 11th Int. Conf. Auto. Agents Multiagent Syst.*, Valencia, Spain, 2012, pp. 13–20,.
[11] J. Tsai, C. Kiekintveld, F. Ordóñez, M. Tambe, and S. Rathi, "Iris—A tool for strategic security allocation in transportation networks," in *Proc. 8th Int. Conf. Auto. Agents Multiagent Syst.*, Budapest, Hungary, 2009, pp. 37–44.
[12] Z. Yin *et al.*, "TRUSTS: Scheduling randomized patrols for fare inspection in transit systems," in *Proc. 26th AAAI Conf. Artif. Intell.*, Toronto, ON, Canada, 2012, pp. 1–8.
[13] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proc. 8th Int. Conf. Auto. Agents Multiagent Syst.*, Budapest, Hungary, 2009, pp. 689–696.
[14] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games," in *Proc. 7th Int. Conf. Auto. Agents Multiagent Syst.*, Estoril, Portugal, 2008, pp. 895–902.
[15] A. Nochenson and C. F. L. Heimann, *Simulation and Game-Theoretic Analysis of an Attacker-Defender Game*. Berlin, Germany: Springer, 2012.
[16] N. S. V. Rao, S. W. Poole, C. Y. Ma, F. He, J. Zhuang, and D. K. Yau, "Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models," *Risk Anal.*, vol. 36, no. 4, pp. 694–710, 2016.
[17] P. Guan, M. He, J. Zhuang, and S. C. Hora, "Modeling a multitarget attacker–defender game with budget constraints," *Decision Anal.*, vol. 14, no. 2, pp. 87–107, 2017.
[18] S. H. Strogatz, "Exploring complex networks," *Nature*, vol. 410, pp. 268–276, Mar. 2001.
[19] Y.-P. Li, S.-Y. Tan, Y. Deng, and J. Wu, "Attacker-defender game from a network science perspective," *Chaos*, vol. 28, no. 5, pp. 051102–051109, 2018.
[20] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.*, vol. 87, p. 198701, Oct. 2001.
[21] C. H. Papadimitriou, *The Complexity of Finding Nash Equilibria*. New York, NY, USA: Cambridge Univ. Press, 2007.
[22] E. Tardos and V. V. Vazirani, *Basic Solution Concepts and Computational Issues*. New York, NY, USA: Cambridge Univ. Press, 2007.
[23] C. E. Lemke and J. T. Howson, "Equilibrium points of bimatrix games," *J. Soc. Ind. Appl. Math.*, vol. 12, no. 2, pp. 413–423, 1964.
[24] R. Porter, E. Nudelman, and Y. Shoham, "Simple search methods for finding a Nash equilibrium," *Games Econ. Behav.*, vol. 63, no. 2, pp. 664–669, Jul. 2004.
[25] P. Godinho and J. Dias, "A two-player competitive discrete location model with simultaneous decisions," *Eur. J. Oper. Res.*, vol. 207, no. 3, pp. 1419–1432, Dec. 2010.
[26] P. Godinho and J. Dias, "Two-player simultaneous location game: Preferential rights and overbidding," *Eur. J. Oper. Res.*, vol. 229, no. 3, pp. 663–672, Sep. 2013.



YAPENG LI received the B.S. degree in logistics management from Nankai University, Tianjin, China, in 2016. He is currently pursuing the M.S. degree in management science and engineering from the National University of Defense Technology, Changsha, China.

His research interests include complex networks, game theory, and security game.

YU XIAO received the B.S. degree in communication engineering from Sichuan University, Chengdu, China, in 2014, and the M.S. degree in management science and engineering from the National University of Defense Technology, Changsha, China, in 2016, where he is currently pursuing the Ph.D. degree in management science and engineering.

His current research interests include multicriteria decision analysis, rank aggregation, graph theory, and voting theory.

YONG LI received the B.Eng. degree in electrical and information engineering from Harbin Technical University, China, in 2002, and the Ph.D. degree in management science from the National University of Defense Technology, China, in 2009. In 2008, he joined Changsha University, where he is currently an Associate Professor.

His current research interests are in the areas of complex networks, big data, and analysis of public opinion.

JUN WU received the B.S. degree in management science from Sichuan University, Chengdu, China, in 2002, and the Ph.D. degree in management science from the National University of Defense Technology, Changsha, China, in 2008.

From 2007 to 2008, he was a Visiting Ph.D. Student with the Institute for Mathematical Sciences, Imperial College London, London, U.K. In 2008, he joined the National University of Defense Technology, where he is currently a Professor. From 2016 to 2017, he was an Academic Visitor with the Department of Computer Science, University of California at Davis, Davis, CA, USA. His current research interests include complex networks, especially the structural robustness of complex networks.