Physica A 521 (2019) 705–714

Contents lists available at ScienceDirect

Physica A

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

Stackelberg game in critical infrastructures from a network science perspective

Yapeng Li, Shun Qiao, Ye Deng, Jun Wu *

College of Systems Engineering, National University of Defense Technology, Changsha, Hunan 410073, PR China

HIGHLIGHTS

- We propose a Stackelberg game model to depict the confrontations between the strategic attacker and defender in critical infrastructures.
- We define the strategies and payoffs of the game on the basis of the topology structure of the network.
- We explore the Strong Stackelberg Equilibriums of the game in different kinds of networks.
- We find that the cost sensitivity is the main factor influencing the equilibrium results.

ARTICLE INFO

Article history:
Received 6 June 2018
Received in revised form 28 September 2018
Available online 1 February 2019

Keywords:
Complex networks
Stackelberg game
Strong Stackelberg Equilibrium
Heterogeneous cost

ABSTRACT

Defending critical infrastructures has received enormous attentions by security agencies. Many infrastructures function as networks such as transportation and communication systems. It is necessary for us to protect them from a network science perspective. In many real-world scenarios, the attacker can observe the defender's action and then choose its best strategy accordingly. Therefore, we propose a Stackelberg game where the defender commits to a strategy, either a pure strategy or a mixed one, and the attacker makes its choice after knowing the defender's action. The strategies and payoffs in this game are defined on the basis of the topology structure of the network. For the convenience of analysis, only two attack and defense strategies, namely, targeted strategy and random strategy, are considered in this paper. The simulation results reveal that in infrastructures with a small cost-sensitive parameter, representing the degree to which costs increase with the importance of a target, the defender commits to a mixed strategy and the attacker's best response is to attack hub nodes with the largest degrees. When the cost-sensitive parameter exceeds a threshold, both the defender and the attacker switch to the random strategy. We also implement experiments with different cost-sensitive parameters and find that the attack-cost-sensitive parameter is the key factor influencing the equilibrium strategies. Our work is a rudimentary attempt to analyze the Stackelberg game in protecting networked infrastructures and it is worth further study.

1. Introduction

Security at critical infrastructures, such as communication, electrical power, rail, and fuel distribution networks, is a key concern and a challenging task for security agencies all over the world. These critical infrastructures play a vital role in modern society, which makes them to be the military targets in times of war. Besides, the threat of terrorism exacerbates the

* Corresponding author.
E-mail address: junwu@nudt.edu.cn (J. Wu).

https://doi.org/10.1016/j.physa.2019.01.119
0378-4371/

		attacker c	attacker d
defender	a	2, 1	5, 0
	b	1, 0	3, 2

Fig. 1. Payoff matrix of a normal form game.

vulnerability of these infrastructures. For example, Colombia, India, Pakistan, Spain and Turkey have encountered terrorist attacks on electrical power networks, rail networks, and oil pipelines. Moreover, the components of these systems are always networked, where the connectivity as well as the topology structures of these networks have tremendous impact on their functionalities. There are always enormous public investments in each infrastructure system, thus, even a minor disruption caused randomly or deliberately, will inflict substantial economic losses [1]. The interrelationship among the components within a certain system and among different systems poses an even larger challenge on protecting these infrastructures.

In the past few years, many methods have been proposed to deal with the protection of infrastructure systems, such as Probabilistic Risk Assessment (PRA) [2] and game-theoretic approaches [3–9]. Due to the limitations of PRA that it requires static probabilities as inputs [10], the game-theoretic methods have been accumulating significant research interest. Nochenson and Heimann [11] propose an agent-based network security game to protect the computer networks. This game is a simultaneous-move and repeated game, where the utilities of the players are determined by the values of individual computers which are preassigned randomly in the simulation. Rao et al. [12] investigate the game in infrastructures consisting of a network of systems, where the costs of players are in sum-form, product-form and composite utility functions. Many other studies also investigate these interactive situations between the attacker and defender on defending critical infrastructures [13–18]. However, most studies do not consider the connectivity of different components within a system and they only evaluate the payoffs of the players by summing up the valuations of individual targets. This evaluation is not reasonable in networked systems, because the importance of a target is not only determined by its monetary value, but is also affected by its neighbors. Li et al. [19] propose an attacker–defender game, which defines the payoffs and the strategies on the basis of the topology structure of the target network. This game is simultaneous-move and both players have complete information about the opponent. Keeping the protection resource allocation secret is common in real-world and is studied by many researches [20,21].

However, in many real-world scenarios, strategies are not always selected in such a simultaneous manner. Oftentimes, the leader is able to commit to a strategy before the follower chooses its own strategy, which is a Stackelberg game. Stackelberg games are commonly used to model attacker–defender scenarios in security domains [1]. In many security problems, a motivated attacker can gather historical information about security measures by surveillance. Although the follower in a Stackelberg game is allowed to observe the leader's strategy before making its own action, there is often an advantage for the leader over the simultaneous-move case. This first-mover advantage in a defender–attacker sequential games is discussed as a theorem in [22]. To illustrate the advantage of being the leader, consider the game with the payoff matrix as shown in Fig. 1, which is adapted from [23]. The only pure-strategy Nash equilibrium for this game is that the leader chooses the strategy a which is a dominant strategy and thus the follower plays c, ensuring the leader a payoff of 2. However, when the leader commits to the strategy b, the follower's best response is d and the leader obtains a higher payoff of 3. When the leader commits to a mixed strategy of playing a and b with equal probability, the follower's best strategy is still d and the leader gets a even higher payoff of 4. Conitzer and Sandholm [23] firstly investigates this kind of Stackelberg game and studies how to compute optimal strategies to commit to in both normal-form and Bayesian form. Paruchuri et al. [24] study the Bayesian Stackelberg games in the domain of patrolling and propose an efficient algorithm DOBSS for finding the optimal strategy for the defender to commit to, which is at the heart of the ARMOR system that aims at protecting the Los Angeles International Airport. There are many other algorithms for these Bayesian Stackelberg games, such as ASAP [25] and ERASER [26]. Many applications based on these algorithms have been deployed in airports [27], ports [28], transportations [29] and many other infrastructures [26,30–33].

In this paper, we will propose a Stackelberg game where the valuation of a target is evaluated in the whole network. The rest of this paper is organized as follows. In Section 2, we introduce the cost model, strategies, payoffs of the game, and introduce the Stackelberg game with two typical defense and attack strategies. The solution method is shown in Section 3. The experimental results in scale-free networks are shown in Section 4. We also implement simulations in various networks in Section 5. Finally, we make a conclusion and introduce future work in Section 6.

2. Stackelberg game model

A networked infrastructure system can be 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. The number of nodes $|V|$ is denoted by N. Suppose $A(G) = (a_{ij})_{N\times N}$ be 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. The degree of node v_i is $k_i = \sum_{j=1}^{N} a_{ij}$, which equals the number of edges connected to it.

In this paper, we consider the situation where one defender can commit to a strategy, either a pure strategy or a mixed one, to obtain a higher payoff, and one attacker can observe the strategy that the defender has committed to with historical information and then choose its own strategy. Thus, in this Stackelberg game, the defender is the leader and the attacker is the follower. It is assumed that both the defender and the attacker can obtain the complete information of the target network and potential strategies of the opponent. Besides, the available resources of each other and costs of each target are also known by both players before they play the game.

2.1. Cost model

We assume that both the attack and the defense approaches are against nodes because the attack against nodes may induce more serious consequences. If one node is removed, the attached edges are also removed from the network. Denote by c_i^A and c_i^D the attack cost and defense cost of node v_i, respectively, with the following forms

$$c_i^A = {r_i}^p, c_i^D = {r_i}^q, \tag{1}$$

where $r_i \geq 0$ is a certain referential property of node v_i and $p \geq 0$ ($q \geq 0$) is the *attack (defense)-cost-sensitive parameter*. In this equation, it is clear that the cost is determined by the referential property of v_i as well as the cost-sensitive parameters of the players. The referential property r_i can be the degree, the betweenness or some other structural measures of nodes. In the extreme case where $p = 0$ ($q = 0$), the attack (defense) costs toward each target are completely equal, regardless of the referential property. When p and q are large, the removal or defense of the node whose referential property is larger costs the players more resources. Besides, the parameters p and q are exogenously determined by the specific systems. For example, the protection costs among different computers in a computer network are almost identical. However, the hub stations in a railway network are much costlier for the attacker to attack and also requires more resources to defend. In real-world scenarios, the maximal available resources of the attacker and defender are always limited, which are defined as

$$\hat{C}^A = \alpha \sum_{i=1}^{N} c_i^A = \alpha \sum_{i=1}^{N} {r_i}^p, \tag{2}$$

and

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

respectively, where $\alpha \in [0, 1]$ is the *attack-cost-constraint parameter* and $\beta \in [0, 1]$ is the *defense-cost-constraint parameter*. The parameters α and β reveal how many resources the players can devote to their actions. With the increase of α, there are more targets that the attacker can attack when taking the same attack strategy. In the extreme case that $\alpha = 1$, all the targets can be attacked by the attacker.

2.2. Strategies

Suppose $V^A \subseteq V$ be the set of nodes that are attacked. An attack strategy is defined 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 the node v_i is attacked, namely, $v_i \in V^A$, otherwise $x_i = 0$. Let C_X be the total cost of the attack strategy X, which is defined as

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

Therefore, the budget constraint of the attacker is

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

Any solution X that satisfies this constraint is a feasible attack strategy. Similarly, a feasible defense strategy also satisfies

$$C_Y = \sum_{i=1}^{N} y_i {r_i}^q \leq \hat{C}^D = \beta \sum_{i=1}^{N} {r_i}^q, \tag{6}$$

where $Y = [y_1, y_2, \ldots y_N] \in S_D$ is a defense strategy defined in the same way as the attack strategy.

		attacker: TAS	attacker: RAS
defender	TDS	u_{11}^{D}, u_{11}^{A}	u_{12}^{D}, u_{12}^{A}
	RDS	u_{21}^{D}, u_{21}^{A}	u_{22}^{D}, u_{22}^{A}

Fig. 2. Payoff matrix of the security game.

2.3. Payoffs

We assume that if a node v_i is defended ($y_i = 1$), it will not be removed when the attacker attacks it. However, a node with no defense will be removed from the network when it is attacked, that is, $x_i = 1$ and $y_i = 0$. Suppose the set of nodes that are removed be $\hat{V} \subseteq V$. Thus, the network after the removing process is $\hat{G} = (V - \hat{V}, \hat{E})$. It is easy to identify that

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

Suppose $U^A : S_D \times S_A \to \mathbb{R}$ be the payoff function of the attacker and $U^A(Y, X)$ be the payoff received by the attacker when the defender commits to the strategy Y and the attacker chooses the strategy X. Thus, the payoff of the attacker is defined as

$$U^A(Y, X) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)}, \tag{8}$$

where Γ is the measure function of network performance. We assume that the network performance declines during the process of nodes removals, which means $\Gamma(G_1) \leq \Gamma(G_2)$ if $G_1 = (V_1, E_1)$ is a subgraph of $G_2 = (V_2, E_2)$. The common measure functions include the size of the largest connected component and the efficiency. The attacker's payoff function means that the attacker can obtain a higher payoff when the network performance declines to a larger extent. Let $\widetilde{G} = (V - V^A, \widetilde{E})$ be the network when all the attacked nodes are removed with no defense. We define the payoff of the defender as

$$U^D(Y, X) = \frac{\Gamma(\hat{G})}{\Gamma(G)} \exp \frac{\Gamma(\hat{G}) - \Gamma(\widetilde{G})}{2\Gamma(G)}. \tag{9}$$

In this equation, the first factor $\Gamma(\hat{G})/\Gamma(G)$ represents the network performance after the attacked nodes are removed. It is apparent that the defender will obtain higher payoffs when the target network maintains higher performance. Besides, the second factor shows the effectiveness of defense, which means that the more attacked nodes are defended, the higher payoff that the defender will obtain. It needs to be emphasized that the network performance is the principal factor affecting the defender's payoff.

2.4. Security game with typical attack and defense strategies

The attack and defense strategies defined in Eqs. (5) and (6) have extremely large strategy space with large network size N. For example, in a network with $N = 100$, $| S_A | = 2^N \approx 10^{30}$ when $\alpha = 1$ and $p = 0$. The size of strategy profiles $| S_D \times S_A |$ is even larger and few techniques are available to solve this game model using brute force. Moreover, the payoff functions defined above do not have explicit formulations. Thus, the efficient methods to solve Stackelberg games with decomposition process and compact representation adopted in previous studies are not executable in our game model [25,26]. It is intuitive that many decision-makers in real-world scenarios generally follow some simple criterion to make their decisions. Thus, for the convenience of analysis, we consider two typical attack and defense strategies in this paper. The typical attack strategies are the *targeted attack strategy (TAS)* (corresponding to "intentional attack") and the *random attack strategy (RAS)* (corresponding to "random failure") [34]. The TAS means that the attacker devotes all its resources toward the targets with the largest referential properties r_i. While the RAS indicates that the attacker selects as many targets as possible to attack randomly. We also consider the defense strategies to be the *targeted defense strategy (TDS)* and the *random defense strategy (RDS)*. To obtain a targeted strategy, we first sort the nodes by their referential property in the descending order. Then we add the targets to the attack (defense) set in this order one by one and check whether the budget constraint is violated. This process is terminated until the constraint is violated when adding one more node into the set. Therefore, the payoff matrix with 4 strategy profiles are shown in Fig. 2, where $u_{ij}^D(u_{ij}^A)$ is the payoff of the defender (attacker) when the defender chooses strategy i and the attacker takes strategy j. The row player is the defender, which is the leader, and the column player is the attacker.

3. Methods

As the Stackelberg game we have proposed, the defender is the leader and first commits to a pure strategy or a mixed strategy. The attacker is the follower and can observe the action made by the defender and makes its own optimal strategy

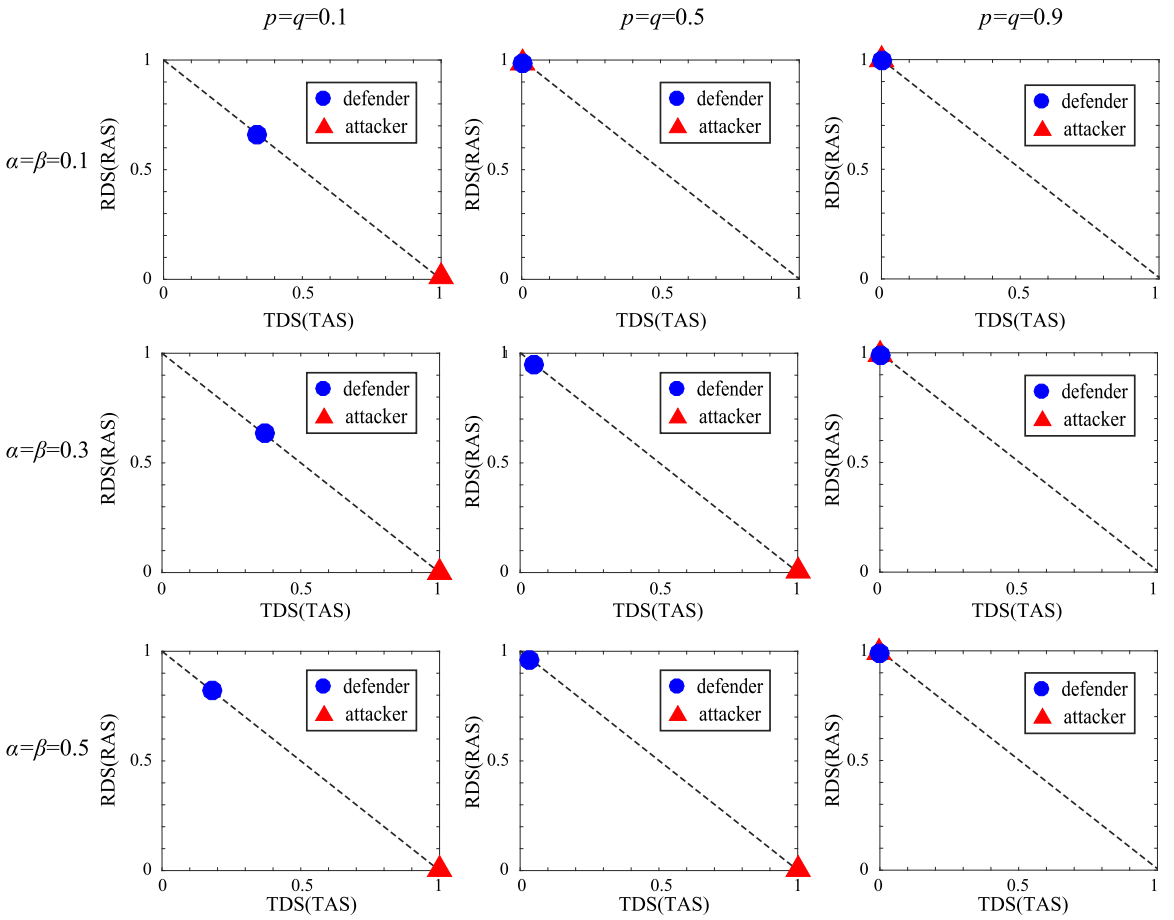

Fig. 3. SSE strategies with different p ($p = q$) and α ($\alpha = \beta$). The target network is a random scale-free network whose $N = 1000$, $\lambda = 3$ and $\langle k \rangle = 4$. The probability of the defender (attacker) to take the TDS (TAS) in SSEs corresponds with the horizontal axis, and that of the RDS (RAS) is shown on the vertical axis. Because we only consider two defense and attack strategies, the equilibrium points are at all times on the dashed lines, and pure-strategy equilibriums are at the two ends of the lines.

accordingly. Thus, the defender's goal is to find a best strategy to commit to, which guarantees it a best payoff. In this Stackelberg game model, we use Strong Stackelberg Equilibrium (SSE) as the solution concept, because a SSE exists in all Stackelberg games [35]. A SSE is a subgame perfect equilibrium where the follower will always choose the optimal strategy in the leader's favor in cases of indifference. This solution concept is the most commonly adopted concept in Stackelberg games [23,24,26]. It is worth mentioning that the random strategy may induce different payoffs in each realization, making the equilibriums be quite different. Therefore, we analyze the equilibriums based on the payoffs which are averaged over many independent realizations.

After the payoff matrix shown in Fig. 2 is obtained, we use the Multiple-LPs methods proposed by Conitzer and Sandholm [23] to calculate the SSE. Suppose p_i be the probability that the defender commits to the defense strategy $i \in S^D$. The defender's best strategy is computed as

$$\begin{aligned} max \quad & \sum_{i \in S_D} p_i u^D_{ij^*} \\ s.t. \quad & \sum_{i \in S_D} p_i u^A_{ij^*} \geq \sum_{i \in S_D} p_i u^A_{ij} \qquad \forall j \in S_A \\ & \sum_{i \in S_D} p_i = 1 \\ & p_i \in [0, 1] \qquad \forall i \in S_D. \end{aligned} \tag{10}$$

In Eq. (10), j^* is the attacker's best response given the defender's (mixed) strategy.

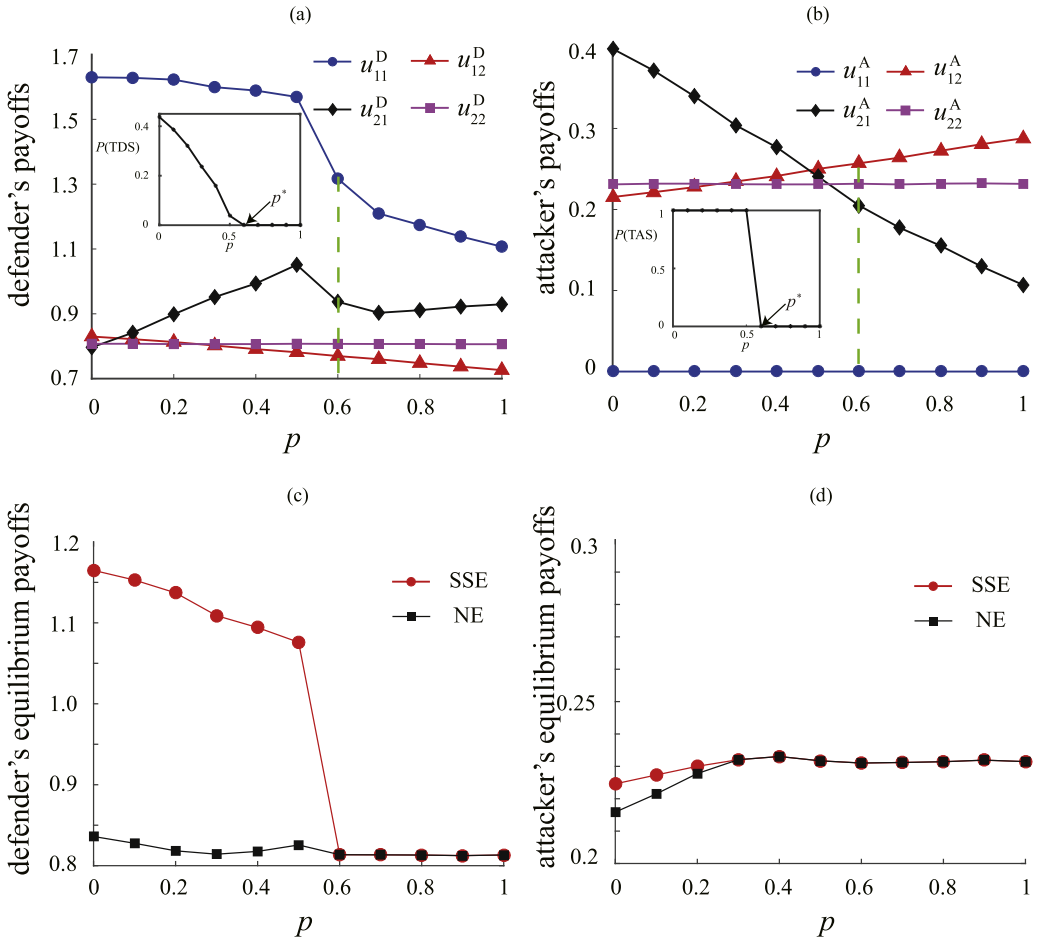

Fig. 4. Payoffs in each strategy profile of the defender (a) and the attacker (b) and equilibrium payoffs in SSE and Nash equilibrium (NE) of the defender (c) and the attacker (d) versus p ($q = p$) when $\alpha = \beta = 0.3$. The target network is the same one as that in Fig. 3. The probabilities that the defender and the attacker take the targeted strategy in SSEs are also shown in (a) and (b), respectively. There is a threshold p^* where the defender takes the RDS which is a pure-strategy SSE and the attacker shifts to the RAS at the same time when $p \geq p^*$. Apart from the equilibrium payoffs in the SSEs, we also compute the equilibrium payoffs when the two players act simultaneously and show them in (c) and (d).

4. Equilibrium strategies in scale-free networks

For the ubiquity of scale-free networks in natural and man-made systems, we first explore the equilibrium results in scale-free networks, whose degree distributions follow $P(k) \sim k^{-\lambda}$, where λ is the degree exponent. We adopt the degree k_i as the referential property r_i and the size of the largest connected component as the measure function Γ. For the convenience of analysis, we first assume that $p = q$ and $\alpha = \beta$. For each parameter configuration, the payoffs are averaged over 1000 independent realizations.

The SSE strategies of the two players with 3 different cases of p and α are shown in Fig. 3. When $p = q = 0.1$, the defender takes the mixed defense strategy, and the attacker adopts the TAS as the best response to the defender's mixed strategy. When the cost-sensitive parameters become larger ($p = q = 0.5$), the equilibriums are different with different cost-constraint parameters. With loose resource constraints ($\alpha = \beta = 0.1$), both players take the random strategy in SSE. With more available resources ($\alpha = \beta = 0.3$ and $\alpha = \beta = 0.5$), the defender still chooses the mixed strategy, where the probabilities of the TDS are approximate to 0, and the attacker takes the TAS. In the third case that $p = q = 0.9$, the SSEs are all identical, where the defender commits to the RDS and the attacker's best strategy is also the RAS.

It seems that the cost-sensitive parameter is the main factor which influences the equilibrium results. To investigate this influence in depth, we show in Fig. 4 the payoffs in each strategy profile of the two players and their equilibrium payoffs as a function of p ($p = q$) when $\alpha = \beta = 0.3$. In Fig. 4(a), we show the probability that the defender chooses the TDS in equilibriums. This probability decreases with p and equals 0 when $p \geq 0.6$. Likewise, the attacker changes its strategy from the TAS to the RAS when $p \geq 0.6$, which can be seen in Fig. 4(b). We denote this threshold where the defender's SSE becomes the RDS and the attacker's best strategy becomes the RAS by p^*. This result can be explained by the change of payoffs with p.

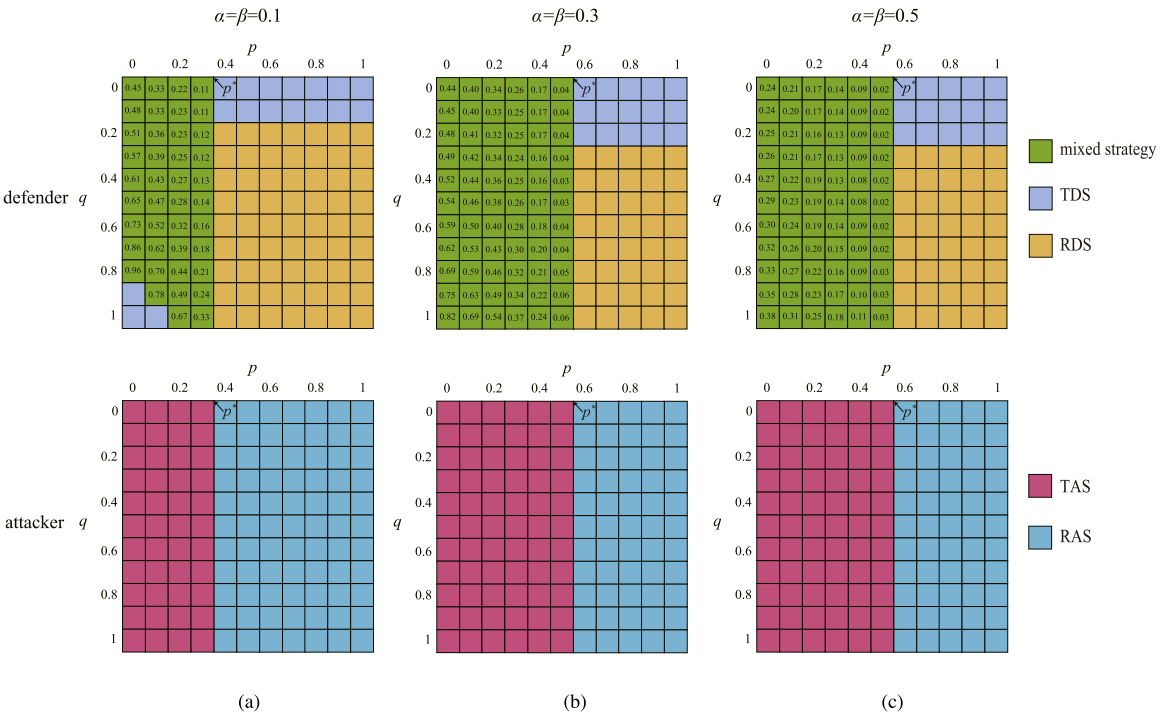

Fig. 5. Equilibrium strategies of the two players when p and q are different with $\alpha = \beta = 0.1$ (a), $\alpha = \beta = 0.3$ (b) and $\alpha = \beta = 0.5$ (c). We use the same target network as that in Fig. 3. The numbers in the blocks represent the probabilities of the TDS in the defender's mixed-SSEs. The blocks in different colors show the different equilibrium strategies.

When $p = 0.6$, as shown by the dashed line in (b), the attacker's payoff u^A_{22} becomes larger than u^A_{21}. Besides, u^A_{12} is also larger than u^A_{11} in this case. Therefore, the RAS becomes the dominant strategy for the attacker, which means that no matter what the defender does, the attacker will always chooses the RAS. Thus, the defender's best strategy is the RDS because $u^D_{22} > u^D_{12}$, as can be seen in (a). When $p < p^*$, the defender commits to mixed strategies where the RDS has a larger probability to make the TAS be more preferable for the attacker ($p_{TDS} \cdot u^A_{11} + p_{RDS} \cdot u^A_{21} > p_{TDS} \cdot u^A_{12} + p_{RDS} \cdot u^A_{22}$), because this can guarantee the defender a higher payoff ($p_{TDS} \cdot u^D_{11} + p_{RDS} \cdot u^D_{21} > p_{TDS} \cdot u^D_{12} + p_{RDS} \cdot u^D_{22}$). This SSE means that when the probability of the TDS is larger than that in SSE, the attacker will no longer take the TAS and the defender loses the chance to ruin all the attacker's efforts, which leads to a lower payoff for the defender. With the increase of p, u^A_{21} decreases, which requires the defender allocates larger probability on the RDS to make the TAS be more preferable for the attacker.

In Fig. 4(c), we find that the defender's equilibrium payoffs are much larger than that in the simultaneous game when $p < p^*$. When $p \geq p^*$, the payoffs in the two games are equal. This is because the equilibrium strategies are identical in this case, which leads to the same payoffs. As for the attacker, the change of its equilibrium payoffs is not obvious with different p (in Fig. 4(d)). Besides, the attacker can obtain higher payoffs in SSE than in Nash equilibrium with small p. But this improvement is less attracting compared with that of the defender, which proves the first-mover advantage and the merit of the mixed strategy for the defender in this Stackelberg game.

When p and q are different, the SSEs are shown in Fig. 5. In this figure, we find a similar pattern in the players' SSEs with different α (β). For example, when $\alpha = \beta = 0.3$, the defender commits to mixed strategies where the probabilities of the TDS increase with q and decrease with p when $p < p^* = 0.6$. This result can be explained by Fig. 6.

In Fig. 6(b), the payoff u^A_{21} decreases monotonically with p but is still larger than u^A_{22} when $p < p^*$. Therefore, as we have analyzed, the defender commits to mixed strategies and allocates larger probability on the RDS with larger p to make the attacker choose the TAS and thus gets higher payoffs. When p is fixed, consider a special case that $\alpha = \beta = 0.3$ and $p = 0$, which can be seen in Fig. 6(c) and (d). It is clear that u^A_{11} increases significantly with q because the hub targets with large degrees are so costly to defend that more hub nodes are removed when q is larger. Therefore, the defender allocates higher probabilities on the TDS with the increasing q. Besides, When $\alpha = \beta = 0.3$ and $p \geq 0.6$, the defender takes the TDS which is a pure-strategy equilibrium in the case when $q \leq 0.2$ and shifts to the RDS when $q > 0.3$. This is because when $p \geq p^*$, as we have analyzed, the attacker's dominant strategy is the RAS. Thus, the defender's best strategy to commit to is determined by the payoffs u^D_{12} and u^D_{22}. When q is small, the defender can protect many hub targets with large degrees and get a higher payoff ($u^D_{12} > u^D_{22}$), leading to the defender's best strategy to be the TDS. However, when q becomes larger, the defender defends less targets with the TDS and $u^D_{12} < u^D_{22}$. Thus, the defender's equilibrium strategy becomes the RDS. As for

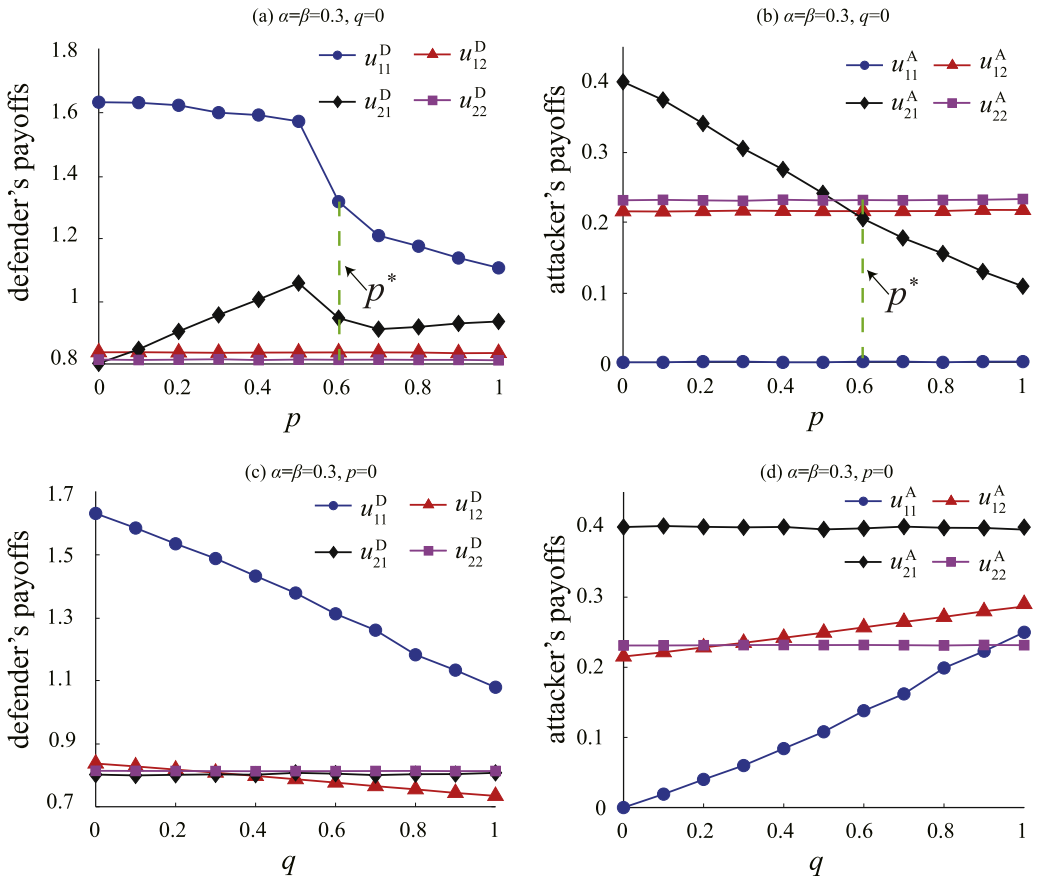

Fig. 6. Payoffs in each strategy profile versus p of the defender (a) and the attacker (b) when $\alpha = \beta = 0.3$, $q = 0$ and that versus q when $\alpha = \beta = 0.3$, $p = 0$ (c, d). The target network is the same one as that in Fig. 3.

the attacker, when $p < p^*$, it takes the TAS at all times, which is the best response to the defender's mixed strategy. When $p \geq p^*$, the attacker adopts the RAS regardless of q because this is the dominant strategy. In Fig. 5, a special result occurs when $\alpha = \beta = 0.1$, that the defender commits to the TDS when q is extremely large and p is quite small. In this case, u_{11}^A exceeds u_{12}^A and the TAS becomes the dominant strategy for the attacker, making the defender's best response be the TDS.

5. Equilibrium results in different networks

As we have analyzed, the threshold p^* is a critical indicator of our game model which indicates the equilibrium results. When the topology structure of the target network changes, the equilibriums will be different and this difference can be revealed by p^*. To show the equilibrium results in different target networks, we implement simulations in various networks and show the change of p^* in Fig. 7. It is clear that p^* is larger in all networks with more sufficient resources but remains unchanged when α exceeds a certain value. In scale-free networks (see Fig. 7(a)), p^* is always larger with a smaller λ and smaller $\langle k \rangle$. In ER networks (see Fig. 7(b)), p^* is equal to 0.1 regardless of α when $\langle k \rangle = 6$. Besides, it seems that p^* is always smaller in ER networks than in scale-free networks with equal $\langle k \rangle$. As we have analyzed, when $p \geq p^*$ ($p = q$), both the players shift to the random strategy and the defender's equilibrium payoff decreases dramatically. So, a network with a very small p^* means that the defender can only obtain relatively higher payoffs when the costs among different targets are quite homogeneous.

6. Conclusions and discussions

Game theory provides a proper framework to model the confrontations in critical infrastructures between the strategic attackers and defenders. In some real-world scenarios, the attacker can observe the defender's moves and then make its best response. This game is known as Stackelberg game, where the defender commits to a (mixed) strategy first. Strong Stackelberg Equilibrium (SSE) is the most commonly adopted solution concept in these games. Although many Stackelberg games have been proposed, little of them consider the infrastructures as networked systems. We believe that the topology

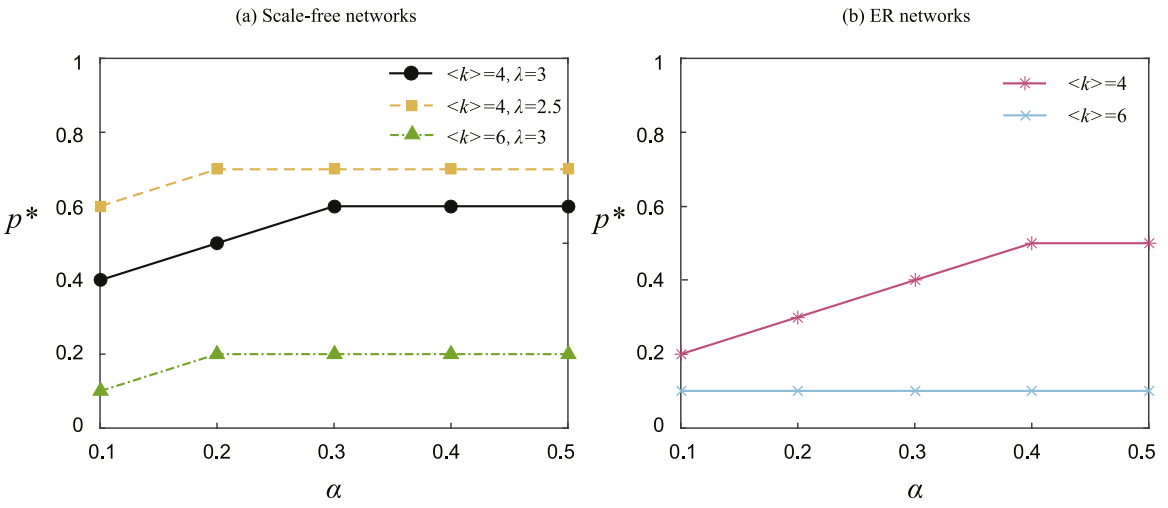

Fig. 7. The thresholds p^* versus α when $\alpha = \beta$ in scale-free networks (a) and in ER networks (b) with various parameters. The solid line in (a) shows the result in the same target network as in Fig. 3. The size of the networks shown are all $N = 1000$.

structure of these systems also plays a vital role in maintaining their functionalities and we should take a network science perspective to protect them. In this paper, we study this sequential-move game and evaluate the payoffs of the players on the basis of the topology structure. For the convenience of analysis, we only consider two typical defense and attack strategies, namely, targeted strategy and random strategy. We investigate the SSEs of the game in networks with different cost-sensitive parameters ($p = q$) or cost-constraint parameters ($\alpha = \beta$) in a random scale-free network. We find that there is a threshold p^* where both the players adopt the random strategy when $p \geq p^*$. By analyzing the results when p and q are different, we find that the cost-sensitive parameters are the key factors that affect the equilibrium strategies and p^* is a critical indicator of the equilibrium results. Therefore, we further study how p^* changes versus available resources in various target networks and find that p^* is larger in networks with more heterogeneous degree distributions and less connections.

This paper studies a Stackelberg game with complete information in critical infrastructures between one defender who is the leader and one attacker who is the follower, which only considers two typical attack and defense strategies. In our future work, we will enlarge the strategy sets and investigate more efficient algorithms to solve the Stackelberg games in networks. Moreover, there are many different kinds of attackers who have different goals and they can attack both the nodes and the arcs in real-world scenarios. So, we will focus on Bayesian Stackelberg games and make the game model more practical in the future.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 71371185 and 71871217, and the Program for New Century Excellent Talents in University, China under Grant No NCET-12-0141.

References

[1] G. Brown, M. Carlyle, J. Salmerón, K. Wood, Defending critical infrastructure, Interfaces 36 (6) (2006) 530–544.
[2] B.C. Ezell, S.P. Bennett, D. Von Winterfeldt, J. Sokolowski, A.J. Collins, Probabilistic risk analysis and terrorism risk, Risk Anal. 30 (4) (2010) 575–589.
[3] M.P. Scaparra, R.L. Church, A bilevel mixed-integer program for critical infrastructure protection planning, Comput. Oper. Res. 35 (6) (2008) 1905–1923.
[4] J. Salmeron, K. Wood, R. Baldick, Worst-case interdiction analysis of large-scale electric power grids, IEEE T. Power Syst. 24 (1) (2009) 96–104.
[5] D.L. Alderson, G.G. Brown, W.M. Carlyle, R.K. Wood, Solving defender-attacker-defender models for infrastructure defense, in: 12th INFORMS Computing Society Conference, INFORMS, 2011, pp. 28–49.
[6] D.G. Arce, D. Kovenock, B. Roberson, Weakest-link attacker-defender games with multiple attack technologies, Naval Res. Logist. 59 (6) (2012) 457–469.
[7] Q. Zhu, 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. 35 (1) (2015) 46–65.
[8] M. Ouyang, A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks, European J. Oper. Res. 262 (3) (2017) 1072–1084.
[9] S. Bao, C. Zhang, M. Ouyang, L. Miao, An integrated tri-level model for enhancing the resilience of facilities against intentional attacks, Ann. Oper. Res. (3) (2017) 1–31.
[10] G.G. Brown, L.A.T. Cox Jr, How probabilistic risk assessment can mislead terrorism risk analysts, Risk Anal. 31 (2) (2011) 196–204.
[11] A. Nochenson, C.F.L. Heimann, Simulation and Game-Theoretic Analysis of an Attacker-Defender Game, Springer Berlin Heidelberg, 2012.
[12] N. Rao, C. Ma, K. Hausken, F. He, D. Yau, J. Zhuang, Defense strategies for asymmetric networked systems with discrete components, Sensors 18 (5) (2018) 1421.

[13] C. Zhang, J. Ramirez-Marquez, C. Rocco, A holistic method for reliability performance assessment and critical components detection in complex networks, IIE Trans. 43 (9) (2011) 661–675.
[14] C. Zhang, J. Ramirez-Marquez, Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information, IIE Trans. 45 (3) (2013) 244–258.
[15] N.S. Rao, S.W. Poole, C.Y. Ma, F. He, J. Zhuang, D.K. Yau, Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models, Risk Anal. 36 (4) (2016) 694–710.
[16] P. Guan, M. He, J. Zhuang, S.C. Hora, Modeling a multitarget attacker–defender game with budget constraints, Decis. Anal. 14 (2) (2017) 87–107.
[17] J. Zhang, J. Zhuang, B. Behlendorf, Stochastic shortest path network interdiction with a case study of Arizona-Mexico border, Reliab. Eng. Syst. Saf. (179) (2018) 62–73.
[18] M. Ouyang, M. Xu, C. Zhang, S. Huang, Mitigating electric power system vulnerability to worst-case spatially localized attacks, Reliab. Eng. Syst. Saf. 165 (2017) 144–154.
[19] Y.P. Li, S.Y. Tan, Y. Deng, J. Wu, Attacker-defender game from a network science perspective, Chaos 28 (5) (2018) 051102–051109.
[20] C. Zhang, J. Ramirez-Marquez, J. Wang, Critical infrastructure protection using secrecy a discrete simultaneous game, European J. Oper. Res. 242 (1) (2015) 212–221.
[21] C. Zhang, J.E. Ramirez-Marquez, Q. Li, Locating and protecting facilities from intentional attacks using secrecy, Reliab. Eng. Syst. Saf. 169 (2018) 51–62.
[22] J. Zhuang, V.M. Bier, Balancing terrorism and natural disasters–defensive strategy with endogenous attacker effort, Oper. Res. 55 (5) (2007) 976–991.
[23] V. Conitzer, T. Sandholm, Computing the optimal strategy to commit to, in: Proceedings of the 7th ACM Conference on Electronic Commerce, 2006, pp. 82–90.
[24] P. Paruchuri, J.P. Pearce, J. Marecki, M. Tambe, F. Ordonez, S. and Kraus, Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games, in: Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems, vol. 2, IFAAMAS, 2008, pp. 895–902.
[25] P. Paruchuri, J.P. Pearce, M. Tambe, F. Ordonez, S. Kraus, An efficient heuristic approach for security against multiple adversaries, in: Proceedings of the 6th International Conference on Autonomous Agents and Multiagent Systems, IFAAMAS, 2007, pp. 118–189.
[26] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, M. and Tambe, Computing optimal randomized resource allocations for massive security games, in: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems, vol. 1, IFAAMAS, 2009, pp. 689–696.
[27] J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, S. Kraus, Using game theory for los angeles airport security, AI Mag. 30 (1) (2009) 43–57.
[28] E. Shieh, B. An, R. Yang, M. Tambe, C. Baldwin, J. DiRenzo, B. Maule, G. Meyer, Protect: An application of computational game theory for the security of the ports of the United States, in: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems, vol. 1, IFAAMAS, 2012, pp. 13–20.
[29] J. Tsai, C. Kiekintveld, F. Ordóñez, M. Tambe, S. Rathi, Iris-a tool for strategic security allocation in transportation networks, in: Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems, IFAAMAS, 2009, pp. 37–44.
[30] Z. Yin, A.X. Jiang, M.P. Johnson, M. Tambe, C. Kiekintveld, K. Leyton-Brown, T. Sandholm, J.P. Sullivan, Trusts: Scheduling randomized patrols for fare inspection in transit systems, in: IAAI, AAAI, 2012.
[31] F. He, J. Zhuang, Modelling 'contracts' between a terrorist group and a government in a sequential game, J. Oper. Res. Soc. 63 (6) (2012) 790–809.
[32] X. Shan, J. Zhuang, Subsidizing to disrupt a terrorism supply chain-a four-player game, J. Oper. Res. Soc. 65 (7) (2014) 1108–1119.
[33] V.M. Payyappalli, J. Zhuang, V.R. Jose, Deterrence and risk preferences in sequential attacker-defender games with continuous efforts, Risk Anal. 37 (11) (2017).
[34] R. Albert, H. Jeong, A.L. Barabási, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.
[35] T. Basar, G.J. Olsder, Dynamic Noncooperative Game Theory, Academic Press, San Diego, CA, 1995.