Computers & Industrial Engineering 110 (2017) 515–526

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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

A robust approach to infrastructure security games ☆

Abdolmajid Yolmeh [a], Melike Baykal-Gürsoy [b,*]

[a] Industrial and Systems Engineering Department, Rutgers University, 96 Frelinghuysen Rd, Piscataway, NJ 08854, United States
[b] Industrial and Systems Engineering Department, RUTCOR, CAIT, Rutgers University, 96 Frelinghuysen Rd, Piscataway, NJ 08854, United States

ARTICLE INFO

Article history:
Received 2 February 2017
Received in revised form 17 May 2017
Accepted 24 June 2017
Available online 27 June 2017

Keywords:
Infrastructure security
Robust approach
Non-cooperative game
Incomplete information
Matrix game

ABSTRACT

Most infrastructure security games assume that the parameters of the game are either deterministic or follow a known distribution. Whereas in reality some parameters of the game may be uncertain with no known distribution or distributional information about them may be unreliable. In this paper we develop distribution-free models of the incomplete-information infrastructure security game with and without private information. We assume that the players are uncertain about the node values and detection probabilities and they use a robust optimization approach to contend with such uncertainty. Moreover, the aim of the attack, to inflict maximum damage or to infiltrate, may be private to the adversary. Depending on the objective of the adversary and the existence of private information, we present three models for this game. We then prove the existence and uniqueness of the Nash equilibrium for the first two models and characterize the shape of the Nash equilibrium for the third model. Our results show that the equilibrium strategy for the robust game with private information is of threshold type. Finally, we apply the proposed approach to real data in order to determine the best allocation of defense resources.

1. Introduction

Terrorist attacks are a serious concern for national economy and quality of life. Every year thousands of people lose their lives or get injured or kidnapped due to these attacks. In 2015, a total of 11,774 terrorist attacks occurred worldwide, resulting in more than 28,300 deaths and more than 35,300 injuries. In addition, more than 12,100 people were kidnapped or taken hostage (Bureau of Counterterrorism, 2016). The psychological impact of the continued threat of terrorism is also considerable. Such incidents create fear, panic, anxiety and distress in the society.

Countering terrorism is currently at the top of the national security agenda in the United States and in many other countries around the world. Indeed, terrorism is widely regarded to be the greatest security challenge of our time. These reasons along with many high profile terrorist attacks that has happened during the past decade, has highlighted modeling and analyzing security of such infrastructures as a major research agenda. The consequences of attacks could be substantially reduced by evaluating the risk associated with each site within the infrastructure, mitigation planning, and designing protection strategies and response policies. To this end, infrastructure security has been a subject of increased interest from researchers recently. Different approaches have been proposed to model strategic interactions in security problems, these methods include system analysis (Paté-Cornell & Guikema, 2002), mathematical modeling (Harris, 2004), probabilistic risk analysis (Garcia, 2005; Garrick et al., 2004; Kaplan & Garrick, 1981; McGill, Ayyub, & Kaminskiy, 2007; Paté-Cornell & Guikema, 2002; Paté-Cornell, 2002) and adversarial risk analysis (Insua, Rios, & Banks, 2009). However, since terrorists can be strategic in their attacks, game theoretic analysis of such attacks yields more realistic results. Recent studies concentrated on developing game theoretic models to capture terrorism risk and applying the results in enhancing security measures. One such model, ARMOR (Paruchuri et al., 2008; Paruchuri, Pearce, Tambe, Ordóñez, & Kraus, 2007; Paruchuri, Tambe, Ordóñez, & Kraus, 2006; Pita et al., 2008) has been deployed at the Los Angeles International Airport (LAX) to enhance security of the airport.

Baykal-Gürsoy, Duan, Poor, and Garnaev (2014) present game theoretic models of the interaction between an adversary and a defender in order to study the security problem within a transit infrastructure. They introduce a risk measure based on the consequence of an attack in terms of the number of people affected or

☆ This material is based upon work supported by the National Science Foundation under Grant No. 1436288.

* Corresponding author.
E-mail addresses: abdolmajid.yolmeh@rutgers.edu (A. Yolmeh), gursoy@rutgers.edu (M. Baykal-Gürsoy).

http://dx.doi.org/10.1016/j.cie.2017.06.032
0360-8352/

the occupancy level of the critical infrastructure. In the proposed non-cooperative game setting, the objective of the adversary is to inflict the maximum damage to the infrastructure by attacking a set of sites in the infrastructure, while the defender attempts to minimize the expected damage by allocating defensive resources to the sites within the infrastructure. They analyze both static and dynamic games and provide a closed form solution for the unique equilibrium strategy pair and game value in the static case. Garnaev, Baykal-Gürsoy, and Poor (2014) examine the adversary's purpose in attacking the infrastructure. There are two types of attackers in this model: maximum damage attacker and infiltrating attacker. Maximum damage attacker aims at inflicting the highest damage, however the infiltrating attacker seeks just to have a successful attack regardless of the damage amount. In order to study such a game, they suggest a simple Bayesian game-theoretic model in which the defender does not know what the adversary is seeking in this attack, e.g., to inflict the maximal damage to the network or to infiltrate. They supply explicit solutions for the equilibrium strategies of this game. Such games in which both players take their action simultaneously are called Nash games. On the other hand, in Stackelberg games, one of the players acts as the leader and reveals her decision to the other player, while the other player, after observing the decision of the leader, takes his action as the follower. ARMOR model casts the patrolling/monitoring problem as a Bayesian Stackelberg game. This model helps the security agent to randomize her actions appropriately, even when the adversary's type is not known (Paruchuri et al., 2008; Paruchuri et al., 2007; Paruchuri et al., 2006; Pita et al., 2008). Garnaev, Baykal-Gürsoy, and Poor (2016) study a situation, in which the defender has to make decisions without knowing if the adversary will play a Nash game or a Stackelberg game. Konak, Kulturel-Konak, and Snyder (2015) consider the reliable server assignment problem under attacks. In this model there are two players, a designer and an adversary. At first the designer determines the locations of the servers on a graph, then, after observing the strategy of the designer, the attacker selects edges to attack to inflict maximum damage to the reliability of the system. They model this problem as a bi-level optimization problem, with the network designer acting as the leader and the adversary acting as the follower. They develop a game-theoretic genetic algorithm with two populations to solve this problem. Garnaev, Baykal-Gürsoy, and Poor (2015) analyze a game that the attacker can also choose his attack type.

Majority of these papers assume that the parameters of the game (such as occupancy levels, detection probabilities etc.) are known with certainty, however this is not a realistic assumption because in reality we can only estimate some of these parameters based on historical data or expert judgments, which both can be inaccurate. Although occupancy levels may be available to the defender through infrared or vision sensors, the attacker may only gather historical data. One possible approach to incorporate parameter uncertainty within a game is the Bayesian game model (Harsanyi, 1967, 1968a, 1968b) that uses distributional information about the game parameters. However, such distributional information may not be readily available to the players, or they may opt not to use potentially inaccurate distributional information. Moreover, the equilibrium strategy of the defender may be seriously affected by such pre-specified probability distributions. Consequently, some researchers consider robustness to address parameter uncertainty in game theoretic models. For example, Aghassi and Bertsimas (2006) relax the assumptions of Harsanyi's Bayesian game model and present an alternative distribution-free equilibrium concept, *robust-optimization equilibrium*, for games with payoff uncertainty. In this approach, players try to optimize their worst case payoff functions simultaneously. The authors prove the existence of such equilibrium points for arbitrary robust finite games with bounded polyhedral payoff uncertainty sets. In the context of security applications, Nikoofal and Zhuang (2012) develop a game theoretic model in which the defender uses a robust approach to tackle her uncertainty about the attacker's valuation of the targets. In this model they suggest a Stackelberg game model in which the defender acts as the leader and the attacker is the follower. This means that the attacker can observe the defender's decision and acts accordingly, which might not always be the case. In some cases the defender may opt not to reveal her decision, in such cases, simultaneous move games are more appropriate than Stackelberg games. Nikoofal and Zhuang (2015) study significance of the first mover's advantage and robustness of strategies under secrecy in the presence of private information. Shan and Zhuang (2013) investigate the robustness of the proposed game theoretic model under the presence of strategic and non-strategic attackers. One difference between their model and ours is that in their model one of the attackers is completely non-strategic, however in our model, attackers are both strategic having different objectives. Moreover, robustness in their paper refers to the sensitivity of the equilibrium to the defender's mistaken assumption about the attacker's type. However, in our paper, robustness is introduced with respect to the parameter uncertainty. Kiekintveld, Islam, and Kreinovich (2013) present Stackelberg type security games and apply a robust optimization approach to optimize the worst case payoff for the defender. However, they do not address the attacker's private information in their model. Kardeş (2014) proposes a robust optimization model for n-person stochastic games with finite states and actions, and uncertain payoffs. He develops an explicit mathematical programming formulation to compute the equilibrium strategies for the case of polytopic uncertainty sets. As an example, he applies this model to solve an incomplete information version of the traveling inspector model. The private information about player types is not included in the model. However, in reality, players may have private information, such as their personal preferences or their attitude toward risk, that is not shared with other players. Qian, Haskell, and Tambe (2015) study a Stackelberg game in which the adversary is risk averse, however, the defender is uncertain about the degree of the attacker's risk aversion and uses a robust approach to contend with this uncertainty. In this model the adversary has complete knowledge about the defender's payoff, however in our model both players are uncertain about the game parameters. Xu and Zhuang (2016) introduce a model in which the defender has private information about her own vulnerability. The adversary can invest in learning activities to gain intelligence about the defender's private information, while the defender decides on investment in counter-learning efforts. This paper is different from our study in the sense that in their paper, the defender has private information. While in our model, the adversary has private information. Moreover, they do not address parameter uncertainty in their model.

In this paper, we develop a robust model for the infrastructure security games, both with and without private information, in which the players use a robust optimization approach to cope with payoff uncertainty. We present analytical results about the existence and uniqueness of robust equilibrium for this game. We then apply the proposed approach to real data on annual terrorism losses in the 10 most valuable urban areas of the United States. The results of the proposed model can be implemented to determine the optimal defensive resource allocation among these areas. The rest of the paper is organized as follows. In Section 2 the problem under consideration is described, three models are proposed to capture the security game under uncertainty. In Section 3 the proposed approach is applied to real data. Main conclusions of the paper and future research suggestions are addressed in Section 4.

2. Problem description

This section introduces a one-shot infrastructure security game. There are N sites in the infrastructure that are potential targets. There is a single defender and a single adversary, therefore each player can choose only one site in the one shot game. The adversary and the defender simultaneously choose their strategies over the potential sites. Payoff matrices for both the defender and the adversary are based on the occupancy level, $\tilde{C}_i$, of each site i in the infrastructure. $\tilde{C}_i$ is an uncertain parameter that has a compact and convex support $\left[\underline{C}_i, \overline{C}_i\right]$, and this range is known to both players. If the defender defends site i and the adversary attacks site j, $j \neq i$, a successful attack on site j will be launched. Therefore payoff to the defender is $-\tilde{C}_j$ and the adversary receives a payoff of $\tilde{C}_j$. However if both players choose the same site i, the attack will be detected with probability $\tilde{d}_i$, which is also uncertain and $\tilde{d}_i \in \left[\underline{d}_i, \overline{d}_i\right]$. Hence the defender's payoff becomes $-\left(1-\tilde{d}_j\right)\tilde{C}_j$ and the adversary's becomes $\left(1-\tilde{d}_j\right)\tilde{C}_j$. This means that even when both rivals are at the same site, there is a probability that the defender may not detect the adversary. There are no assumptions about distributions of the uncertain parameters over their respective uncertainty intervals.

While the defender always attempts to minimize her expected damage, the objective of the adversary may vary depending on his type. There are two possible types of the adversary: maximum damage (MD) adversary and infiltration/harassment (INF) adversary. The MD adversary seeks to maximize his expected payoff, thus differentiates between the potential sites based on their occupancy levels. However, this is not the case for an INF adversary, for whom all sites are the same and the aim is to increase the probability of having a successful attack. In this paper, three models are investigated. In the first model the defender plays the security game with a MD adversary and knows the type of the adversary, in the second model the defender plays the security game against an INF adversary type, in the third model the defender is uncertain about the type of the adversary and only knows that with probability q, the adversary is a MD adversary and with probability $1-q$ the adversary is an INF adversary. Throughout the paper we assume that the sites are sorted in the order of decreasing $\underline{C}_i$s and $\underline{C}_i$s are distinct, i.e., $\underline{C}_1 > \underline{C}_2 > \ldots > \underline{C}_N$. The first assumption is not restrictive by any means, it only requires rearrangement of site indexes so that the sites are sorted. As for the second assumption, our results will still hold even when $\underline{C}_i$s are not distinct, however we are making this assumption in order to simplify the resulting formulas. In the following subsections we describe and analyze each model.

2.1. Model 1: Maximum damage game

In this model the adversary wants to inflict the maximum damage. We assume that the defender knows the intention of the adversary i.e. there is no private information. In this case the payoff to the adversary is:

$$u_A^1(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i,$$

where x_i and y_i are the probability of choosing site i, by the defender and adversary, respectively. Therefore $\mathbf{x} = [x_1, x_2, \ldots, x_N]$ and $\mathbf{y} = [y_1, y_2, \ldots, y_N]$ are the defender's and the adversary's mixed strategies, respectively, and $y_i \geq 0$, $x_i \geqslant 0$, $\forall i = 1, 2, \ldots, N$, $\sum_i x_i = \sum_i y_i = 1$. In order to contend with the uncertainty of the game both players use the robust approach, meaning that they seek to optimize their worst case expected payoff, where the worst case is taken with respect to the set of possible values for the uncertain parameters and the expectation is taken with respect to the mixed strategies of both players (Aghassi & Bertsimas, 2006). Hence the adversary's best response to the defender's strategy $\mathbf{x}$ is:

$$\mathbf{y}^* = \arg\min_{\mathbf{y}} \min_{\substack{\tilde{d}_i \in \left[\underline{d}_i, \overline{d}_i\right] \\ \tilde{C}_i \in \left[\underline{C}_i, \overline{C}_i\right]}} \left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i\right).$$

Note that the minimum of $\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i\right)$ in the above equation occurs when $\tilde{d}_i = \overline{d}_i$ and $\tilde{C}_i = \underline{C}_i$, thus giving the attacker's best response as $\mathbf{y}^* = \arg\max_{y}\left(\sum_{i=1}^{N}\left(1-\overline{d}_i x_i\right)\underline{C}_i y_i\right)$. Using the same robust approach, the defender wants to minimize the maximum expected damage, therefore her best response to the adversary's mixed strategy $\mathbf{y}$ is:

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} \max_{\substack{\tilde{d}_i \in \left[\underline{d}_i, \overline{d}_i\right] \\ \tilde{C}_i \in \left[\underline{C}_i, \overline{C}_i\right]}} \left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i\right).$$

The maximum of $\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i\right)$ in the above equation happens at $\tilde{d}_i = \underline{d}_i$ and $\tilde{C}_i = \overline{C}_i$. Hence the defender's best response is $\mathbf{x}^* = \arg\min_{x}\left(\sum_{i=1}^{N}(1-\underline{d}_i x_i)\overline{C}_i y_i\right)$. The following presents the payoff matrix to both players:

$$P = \begin{array}{c} i \setminus j \\ 1 \\ 2 \\ \vdots \\ N \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \cdots & N \end{array} \\ \begin{pmatrix} -(1-\underline{d}_1)\overline{C}_1, (1-\overline{d}_1)\underline{C}_1 & -\overline{C}_2, \underline{C}_2 & \cdots & -\overline{C}_N, \underline{C}_N \\ -\overline{C}_1, \underline{C}_1 & -(1-\underline{d}_2)\overline{C}_2, (1-\overline{d}_2)\underline{C}_2 & \cdots & -\overline{C}_N, \underline{C}_N \\ \vdots & \vdots & \ddots & \vdots \\ -\overline{C}_1, \underline{C}_1 & -\overline{C}_2, \underline{C}_2 & \cdots & -(1-\underline{d}_N)\overline{C}_N, (1-\overline{d}_N)\underline{C}_N \end{pmatrix} \end{array}.$$

In this matrix at each position the first number is the payoff to player 1(defender) and the second number is the payoff to player 2 (adversary). Since the payoffs to the players do not add up to zero, or a fixed amount, this is a non-zero sum game. The following

lemma gives the necessary and sufficient condition for the non-zero sum game to have a pure Nash Equilibrium (NE).

Lemma 1. *The maximum damage game has a pure Nash equilibrium if and only if* $\left(1-\overline{d}_1\right)\underline{C}_1 \geqslant \underline{C}_2$.

Proof. Suppose we have $\left(1-\overline{d}_1\right)\underline{C}_1 \geqslant \underline{C}_2$. It is easy to check that $\mathbf{x}=(1,0,0,\ldots,0)$, $\mathbf{y}=(1,0,0,\ldots,0)$ is a pure NE strategy pair. This establishes the sufficiency part. We prove the necessity part by contradiction, suppose that $\left(1-\overline{d}_1\right)\underline{C}_1 < \underline{C}_2$ and the game has a pure NE, this pure NE is definitely not $\mathbf{x}=(1,0,0,\ldots,0)$, $\mathbf{y}=(1,0,0,\ldots,0)$, because at this strategy profile the adversary can strictly increase his payoff by attacking site 2. Moreover it has to be on the diagonal of the matrix i.e. $x_i=y_i=1$ for some $i>1$ however, this implies that $\left(1-\overline{d}_i\right)\underline{C}_i \geqslant \underline{C}_1$ which contradicts our assumption of sorted $\underline{C}_i$s, thus proving the necessity part. □

Lemma 2 characterizes the conditions under which some strategies of the adversary are dominated by a linear combination of other strategies. This lemma helps us find a critical index to compute the NE.

Lemma 2. *If* $\sum_{j=1}^{k}\frac{\underline{C}_j-\underline{C}_k}{\overline{d}_j\underline{C}_j}>1$, *then the adversary's strategies* $l \geqslant k$ *are strictly dominated by a mixed strategy that is composed of pure strategies* j *for* $1\leqslant j<k$, *i.e., there exist* $\lambda_i \geqslant 0$, $1\leqslant i\leqslant k-1$ *with* $\sum_{i=1}^{k-1}\lambda_i=1$ *such that:*

$$\lambda_1\begin{bmatrix}\left(1-\overline{d}_1\right)\underline{C}_1\\ \underline{C}_1\\ \underline{C}_1\\ \vdots\\ \underline{C}_1\end{bmatrix}+\lambda_2\begin{bmatrix}\underline{C}_2\\ \left(1-\overline{d}_2\right)\underline{C}_2\\ \underline{C}_2\\ \vdots\\ \underline{C}_2\end{bmatrix}+\cdots+\lambda_{k-1}\begin{bmatrix}\underline{C}_{k-1}\\ \vdots\\ \left(1-\overline{d}_{k-1}\right)\underline{C}_{k-1}\\ \vdots\\ \underline{C}_{k-1}\end{bmatrix}>\begin{bmatrix}\underline{C}_l\\ \vdots\\ \vdots\\ \left(1-\overline{d}_l\right)\underline{C}_l\\ \vdots\\ \underline{C}_l\end{bmatrix}. \tag{1}$$

Proof. The inequality holds for rows $r\geqslant k$ because $\underline{C}_i$s are sorted, i.e., $\sum_{j=1}^{k-1}\lambda_j\underline{C}_j>\underline{C}_k$.

For rows $r<k$, consider the assumption $\sum_{j=1}^{k-1}\frac{\underline{C}_j-\underline{C}_k}{\overline{d}_j\underline{C}_j}>1$. After some algebraic manipulations this inequality can be rewritten as:

$$\frac{\left(1-\overline{d}_r\right)\underline{C}_r}{\overline{d}_r\underline{C}_r\sum_{m=1}^{k-1}\frac{1}{\overline{d}_m\underline{C}_m}}+\sum_{j=1,j\neq r}^{k-1}\frac{\underline{C}_j}{\overline{d}_j\underline{C}_j\sum_{m=1}^{k-1}\frac{1}{\overline{d}_m\underline{C}_m}}>\underline{C}_k.$$

Setting $\lambda_j=\frac{1}{\overline{d}_j\underline{C}_j\sum_{m=1}^{k-1}\frac{1}{\overline{d}_m\underline{C}_m}}$ gives the result as:

$$\lambda_r\left(1-\overline{d}_r\right)\underline{C}_r+\sum_{j=1,j\neq r}^{k-1}\lambda_j\underline{C}_j>\underline{C}_k>\underline{C}_l. \qquad \square$$

Lemma 3 complements Lemma 2 in characterizing the sites that should be in the mixed Nash equilibrium.

Lemma 3. *If* $\sum_{j=1}^{k}\frac{\underline{C}_j-\underline{C}_k}{\overline{d}_j\underline{C}_j}<1$, *any strategy profile with* $x_k=0$ *is not a Nash equilibrium.*

Proof. By contradiction. Suppose the Nash equilibrium holds with $x_k=0$. If $y_k=0$, consider a critical $k^*\geqslant k$ such that $\sum_{j=1}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}}{\overline{d}_j\underline{C}_j}<1<\sum_{j=1}^{k^*+1}\frac{\underline{C}_j-\underline{C}_{k^*+1}}{\overline{d}_j\underline{C}_j}$. Using Lemma 1 we can conclude that both players are playing a mixed strategy. Moreover using Lemma 2 we have: $x_j=0$, $y_j=0$, $\forall j>k^*$. Therefore the adversary is indifferent towards his choices $i=1,\ldots,k^*$, $i\neq k$, in other words:

$$\left(1-\overline{d}_1x_1\right)\underline{C}_1=\ldots=\left(1-\overline{d}_{k-1}x_{k-1}\right)\underline{C}_{k-1}=\left(1-\overline{d}_{k+1}x_{k+1}\right)\underline{C}_{k+1}$$
$$=\ldots=\left(1-\overline{d}_{k^*}x_{k^*}\right)\underline{C}_{k^*}.$$

Solving these equations along with the equation $\sum_{j=1,j\neq k}^{k^*}x_j=1$ yields:

$$x_{k^*}=\frac{1-\sum_{j=1,j\neq k}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}}{\overline{d}_j\underline{C}_j}}{\overline{d}_{k^*}\underline{C}_{k^*}\sum_{j=1,j\neq k}^{k^*}\frac{1}{\overline{d}_j\underline{C}_j}}.$$

Since $\sum_{j=1}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}}{\overline{d}_j\underline{C}_j}<1$ and $\underline{C}_{k^*}\leqslant\underline{C}_k$, the following inequality holds

$$\sum_{j=1,j\neq k}^{k^*}\frac{\underline{C}_j-\underline{C}_k}{\overline{d}_j\underline{C}_j}<1,$$

which could be rewritten as:

$$\sum_{j=1,j\neq k}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}+(\underline{C}_{k^*}-\underline{C}_k)}{\overline{d}_j\underline{C}_j}<1.$$

This further simplifies to

$$(\underline{C}_{k^*}-\underline{C}_k)<\frac{1-\sum_{j=1,j\neq k}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}}{\overline{d}_j\underline{C}_j}}{\sum_{j=1,j\neq k}^{k^*}\frac{1}{\overline{d}_j\underline{C}_j}}=\overline{d}_{k^*}\underline{C}_{k^*}x_{k^*},$$

giving $\left(1-\overline{d}_{k^*}x_{k^*}\right)\underline{C}_{k^*}<\underline{C}_k$. Therefore the adversary can strictly improve his payoff by increasing y_k to 1. Hence $y_k=1$ should hold. Now the defender can strictly increase his/her payoff by increasing x_k to 1. This is in contradiction with our assumption of $x_k=0$ being a Nash equilibrium. □

Theorem 1 states the uniqueness of the Nash equilibrium (NE).

Theorem 1. *The maximum damage game has a unique NE.*

Proof. Consider a critical k^* such that $\sum_{j=1}^{k^*}\frac{\underline{C}_j-\underline{C}_{k^*}}{\overline{d}_j\underline{C}_j}<1<\sum_{j=1}^{k^*+1}\frac{\underline{C}_j-\underline{C}_{k^*+1}}{\overline{d}_j\underline{C}_j}$, if $k^*=1$ then Lemma 1 and Lemma 2 imply that the game has a unique pure strategy Nash equilibrium. If $k^*\geqslant 2$, then using Lemma 2 and Lemma 3, the mixed strategy Nash equilibrium is determined by solving the following systems of equations:

System 1:

$$\left(1-\overline{d}_1x_1\right)\underline{C}_1=\left(1-\overline{d}_2x_2\right)\underline{C}_2=\ldots=\left(1-\overline{d}_{k^*}x_{k^*}\right)\underline{C}_{k^*},\quad \sum_{j=1}^{k^*}x_j=1.$$

System 2:

$$-(1-\underline{d}_1)\overline{C}_1y_1-\sum_{j=1,j\neq}^{k^*}\overline{C}_jy_j=\ldots=-(1-\underline{d}_{k^*})\overline{C}_{k^*}y_{k^*}-\sum_{j=1,j\neq k^*}^{k^*}\overline{C}_jy_j,\quad \sum_{j=1}^{k^*}y_i=1.$$

Both systems have unique solutions. □

2.2. Model 2: Infiltration game

In this model the adversary wants to infiltrate, i.e., the adversary values all sites equally. Let $\widetilde{C}$ with $\widetilde{C} \in \left[\underline{C}, \overline{C}\right]$ denote this common value. Assume that the defender knows the intention of the adversary. Hence the expected payoff to the adversary under the mixed strategy pair $(\mathbf{x}, \mathbf{y})$ of the defender and the adversary, respectively, is:

$$u_A^2(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \left(1 - \widetilde{d}_i x_i\right) \widetilde{C} y_i.$$

Following the robust approach, the adversary seeks to maximize the minimum expected damage. Using the same reasoning as in Model 1, the adversary's best response to the defender's mixed strategy $\mathbf{x}$ is:

$$\mathbf{y}^* = \arg\max_{\mathbf{y}} \left(\sum_{i=1}^{N} \left(1 - \overline{d}_i x_i\right) \underline{C} y_i \right).$$

Similarly, the defender wants to minimize the maximum expected damage, therefore her best response is:

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} \left(\sum_{i=1}^{N} (1 - \underline{d}_i x_i) \overline{C}_i y_i \right).$$

The following matrix demonstrates the payoff to both players:

$$P = \begin{array}{c} i \setminus j \\ 1 \\ 2 \\ \vdots \\ N \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \cdots & N \end{array} \\ \begin{pmatrix} -(1-\underline{d}_1)\overline{C}_1, (1-\overline{d}_1)\underline{C} & -\overline{C}_2, \underline{C} & \cdots & -\overline{C}_N, \underline{C} \\ -\overline{C}_1, \underline{C} & -(1-\underline{d}_2)\overline{C}_2, (1-\overline{d}_2)\underline{C} & \cdots & -\overline{C}_N, \underline{C} \\ \vdots & \vdots & \ddots & \vdots \\ -\overline{C}_1, \underline{C} & -\overline{C}_2, \underline{C} & \cdots & -(1-\underline{d}_N)\overline{C}_N, (1-\overline{d}_N)\underline{C} \end{pmatrix} \end{array}.$$

Note again that this is a non-zero sum game. It is obvious that the infiltration game does not have a pure NE. Lemma 4 uses this fact to characterize the strategies that take part in the mixed strategy NE. Specifically, this lemma proves that all of the sites will take part in the mixed strategy NE.

Lemma 4. *For the infiltration game, any strategy profile with $x_k = 0$ for some $1 \leqslant k \leqslant N$ is not a Nash equilibrium.*

Proof. By contradiction. Clearly, such a game does not have a pure Nash equilibrium. Suppose that there is a Nash equilibrium with $x_k = 0$ and $x_j > 0, \forall j \neq k$. The mixed strategy of the defender is determined by solving the following system of equations:

$$\left(1 - \overline{d}_1 x_1\right)\underline{C} = \ldots = \left(1 - \overline{d}_{k-1} x_{k-1}\right)\underline{C} = \left(1 - \overline{d}_{k+1} x_{k+1}\right)\underline{C} = \ldots = \left(1 - \overline{d}_N x_N\right)\underline{C},$$

which along with $\sum_{j=1,\, j\neq k}^{N} x_j = 1$, gives:

$$x_j = \frac{\frac{1}{\overline{d}_j}}{\left(\sum_{i=1,\, i\neq k}^{N} \frac{1}{\overline{d}_i}\right)}, \forall j \neq k.$$

Since $x_j > 0$ for $j \neq k$, this implies that:

$$\left(1 - \overline{d}_j x_j\right)\underline{C} = \left(1 - \frac{1}{\left(\sum_{i=1,\, i\neq k}^{N} \frac{1}{\overline{d}_i}\right)}\right)\underline{C} < \underline{C},$$

the right hand side corresponding to the adversary's payoff if an attack targets node k. Therefore the adversary can strictly increase his payoff by increasing y_k to 1. The defender can also improve her payoff by setting $x_k = 1$, however this contradicts our assumption that the current set of strategies is a NE. □

Theorem 2. *The infiltration game has a unique NE.*

Proof. Lemma 4 implies that all of the sites should be involved in the mixed strategy NE. Therefore mixed strategy NE is the unique solution to the following system of $2N$ linearly independent equations with $2N$ unknowns:

$$\left(1 - \overline{d}_1 x_1\right)\underline{C} = \left(1 - \overline{d}_2 x_2\right)\underline{C} = \ldots = \left(1 - \overline{d}_N x_N\right)\underline{C}, \quad \sum_{i=1}^{N} x_i = 1, \tag{3}$$

$$-(1-\underline{d}_1)\overline{C}_1 y_1 - \sum_{j=1, j\neq 1}^{N} \overline{C}_j y_j = \ldots = -(1-\underline{d}_N)\overline{C}_N y_N - \sum_{j=1, j\neq N}^{N} \overline{C}_j y_j, \quad \sum_{i=1}^{N} y_i = 1. \tag{4}$$

□

Remark 1. Clearly, $\underline{C}$ can be eliminated in Eq. (3). Therefore the Nash equilibrium does not depend on the value of $\overline{C}$ or $\underline{C}$ (upper and lower bounds on the infiltrating adversary's valuation). This is natural because for the infiltrating adversary all sites are equal and the value of these sites does not affect his behavior. Moreover, the defender has her own valuation of the sites, therefore the value of $\overline{C}$ or $\underline{C}$ does not affect her behavior either. Hence it is natural that the NE does not depend on the value of $\overline{C}$ or $\underline{C}$. However this was not the case in the previous infrastructure security game models. This is mainly due to the zero-sum nature of the previous models (Garnaev et al., 2014).

2.3. Model 3: Security game with private information

In this model we assume that the defender does not know about the intention of the adversary (inflict maximum damage or infiltrate). We use a Bayesian-robust approach to model this game. Meaning that all players use a robust approach to contend with uncertainty of $\widetilde{C}, \tilde{C}_i$ and $\tilde{d}_i$, however the defender uses a Bayesian approach to contend with the information asymmetry. In other words, the defender knows that the adversary attempts to inflict maximum damage with probability q, and he attempts infiltration

with probability $1-q$. Using the Bayesian robust approach and the definition of NE, the following conditions should be satisfied:

$$\mathbf{y}^{1*}=\arg\max_{\mathbf{y}^1}\min_{\substack{\tilde{d}_i\in[\underline{d}_i,\bar{d}_i],\\ \tilde{C}_i\in[\underline{C}_i,\bar{C}_i]}}\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i^*\right)\tilde{C}_i y_i^1\right),\ \sum_{i=1}^{N}y_i^{1*}=1,\ y_i^{1*}\geqslant 0,$$

$$\mathbf{y}^{2*}=\arg\max_{\mathbf{y}^2}\min_{\substack{\tilde{d}_i\in[\underline{d}_i,\bar{d}_i],\\ \tilde{C}\in[\underline{C},\bar{C}]}}\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i^*\right)\tilde{C}y_i^2\right),\ \sum_{i=1}^{N}y_i^{2*}=1,\ y_i^{2*}\geqslant 0,$$

$$\mathbf{x}^*=\arg\min_{\mathbf{x}}\max_{\substack{\tilde{d}_i\in[\underline{d}_i,\bar{d}_i],\\ \tilde{C}_i\in[\underline{C}_i,\bar{C}_i]}}\left(q\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i^{1*}+(1-q)\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i^{2*}\right),$$

$$\sum_{i=1}^{N}x_i^*=1,\ x_i^*\geqslant 0,$$

where $\mathbf{y}^1$ is the mixed strategy of the maximum damage adversary, $\mathbf{y}^2$ is the mixed strategy of the infiltrating adversary, and $\mathbf{x}$ is the defender's mixed strategy as before. Note that $\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i^*\right)\tilde{C}_i y_i^1\right)$ is minimized at $\tilde{d}_i=\bar{d}_i$ and $\tilde{C}_i=\underline{C}_i$, $\left(\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i^*\right)\tilde{C}y_i^2\right)$ is minimized at $\tilde{d}_i=\bar{d}_i$ and $\tilde{C}=\underline{C}$, finally $\left(q\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)\tilde{C}_i y_i^{1*}+(1-q)\sum_{i=1}^{N}\left(1-\tilde{d}_i x_i\right)C_i y_i^{2*}\right)$ is maximized at $\tilde{d}_i=\underline{d}_i$ and $\tilde{C}_i=\bar{C}_i$. Thus

$$\mathbf{y}^{1*}=\arg\max_{\mathbf{y}^1}\left(\sum_{i=1}^{N}\left(1-\bar{d}_i x_i^*\right)\underline{C}_i y_i^1\right),$$

$$\mathbf{y}^{2*}=\arg\max_{\mathbf{y}^2}\left(\sum_{i=1}^{N}\left(1-\bar{d}_i x_i^*\right)\underline{C}y_i^2\right)$$

and

$$\mathbf{x}^*=\arg\min_{\mathbf{x}}\left(q\sum_{i=1}^{N}(1-\underline{d}_i x_i)\bar{C}_i y_i^{1*}+(1-q)\sum_{i=1}^{N}(1-\underline{d}_i x_i)\bar{C}_i y_i^{2*}\right).$$

This optimization problem can be solved by direct application of Karush–Kuhn–Tucker conditions (Kuhn & Tucker, 1951). However more insight can be gained by analyzing this game. The following theorem characterizes the Nash equilibrium for the security game with private information.

Theorem 3. *The following strategy profile is a Nash equilibrium for the security game with private information. Let k be an integer such that $\phi_k\leqslant 1<\phi_{k+1}$ where $\phi_i=\sum_{j=1}^{i}\frac{\underline{C}_j-\underline{C}_j}{\bar{d}_j\underline{C}_j}$, and m be an integer such that $\psi_{m-1}<q\leqslant\psi_m$ where $\psi_i=\frac{\left(\sum_{j=1}^{i}\frac{1}{\bar{d}_j\bar{C}_j}\right)}{\left(\sum_{j=1}^{N}\frac{1}{\bar{d}_j\bar{C}_j}\right)}$.*

If $m\leqslant k$ then

$$x_j^*=\begin{cases}\frac{1-\sum_{i=1}^{N}\frac{1}{\bar{d}_i}+\sum_{i=1}^{m}\frac{\underline{C}_j}{\underline{C}_i\bar{d}_i}+\frac{\underline{C}_j}{\underline{C}_m}\sum_{i=m+1}^{N}\frac{1}{\bar{d}_i}}{\left(\sum_{i=1}^{m}\frac{\underline{C}_j\bar{d}_j}{\underline{C}_i\bar{d}_i}+\frac{\underline{C}_j\bar{d}_j}{\underline{C}_m}\sum_{i=m+1}^{N}\frac{1}{\bar{d}_i}\right)}, & j\leqslant m-1,\\ \frac{\left(1-\sum_{i=1}^{m}\frac{\underline{C}_i-\underline{C}_m}{\bar{d}_i\underline{C}_i}\right)}{\bar{d}_m\left(\sum_{i=1}^{m}\frac{\underline{C}_m}{\underline{C}_i\bar{d}_i}+\sum_{i=m+1}^{N}\frac{1}{\bar{d}_i}\right)}, & j=m,\\ \frac{\left(1-\sum_{i=1}^{m}\frac{\underline{C}_i-\underline{C}_m}{\bar{d}_i\underline{C}_i}\right)}{\bar{d}_j\left(\sum_{i=1}^{m}\frac{\underline{C}_m}{\underline{C}_i\bar{d}_i}+\sum_{i=m+1}^{N}\frac{1}{\bar{d}_i}\right)}, & j>m,\end{cases}\tag{5}$$

$$y_j^{*1}=\begin{cases}\frac{1}{q\left(\underline{d}_j\bar{C}_j\right)\left(\sum_{i=1}^{N}\frac{1}{\underline{d}_i\bar{C}_i}\right)}, & j<m,\\ 1-\frac{\sum_{i=1}^{m-1}\frac{1}{\underline{d}_i\bar{C}_i}}{q\sum_{i=1}^{N}\frac{1}{\underline{d}_i\bar{C}_i}}, & j=m,\\ 0, & j>m,\end{cases}\tag{6}$$

and

$$y_j^{*2}=\begin{cases}0, & j<m,\\ \frac{\left(\sum_{j=1}^{m}\frac{1}{\underline{d}_j\bar{C}_j}\right)-q\left(\sum_{j=1}^{N}\frac{1}{\underline{d}_j\bar{C}_j}\right)}{(1-q)\left(\sum_{j=1}^{N}\frac{1}{\underline{d}_j\bar{C}_j}\right)}, & j=m,\\ \frac{1}{(1-q)\left(\underline{d}_j\bar{C}_j\right)\left(\sum_{i=1}^{N}\frac{1}{\underline{d}_i\bar{C}_i}\right)}, & j>m.\end{cases}\tag{7}$$

If $m>k$ then

$$x_j^*=\begin{cases}\frac{\frac{1}{\bar{d}_j\underline{C}_j}}{\sum_{i=1}^{k}\frac{1}{\bar{d}_i\underline{C}_i}}\left(1-\sum_{i=1}^{k}\frac{\underline{C}_j-\underline{C}_j}{\bar{d}_i\underline{C}_i}\right), & j\leqslant k,\\ 0, & j>k,\end{cases}\tag{8}$$

$$y_j^{*1}=\begin{cases}\frac{\frac{1}{\underline{d}_j\bar{C}_j}}{\sum_{l=1}^{k}\frac{1}{\underline{d}_l\bar{C}_l}}, & j\leqslant k,\\ 0, & j>k,\end{cases}\tag{9}$$

$$y_i^{*2}<\frac{q}{(1-q)}\left(\frac{\frac{1}{\underline{d}_i\bar{C}_i}}{\sum_{l=1}^{k}\frac{1}{\underline{d}_l\bar{C}_l}},\right)\forall i>k,\ \sum_{j=k+1}^{N}y_j^{*2}=1.\tag{10}$$

Proof. See Appendix A. □

Remark 2. Similar to the infiltration game, also in this game the Nash equilibrium does not depend on the value of $\bar{C}$ or $\underline{C}$ (upper and lower bounds on the infiltrating adversary's valuation).

Remark 3. For the second case, i.e., $m>k$, similar to Garnaev et al. (2014) there is a continuum of NE strategies for the infiltrating adversary.

3. Numerical analysis

In this section we apply our approach to real data from Willis, Morral, Kelly, and Medby (2006) which provides estimates of the expected annual terrorism losses for the 10 most valuable urban areas of the United States. We use the proposed robust game model to allocate defensive resources among these urban areas. The data is presented in Table 1. In this table, three aspects of the expected damage have been estimated: monetary value (represented by expected property loss), mortality value (represented by total number of fatalities and injuries) and political value (represented by total air departures from major and minor airports). In the following sections each one of these dimensions will be investigated individually.

3.1. Analysis for monetary value data

In this section we perform the analysis based on the monetary data for each urban area. We study how the defender's strategy is affected by the probability of a maximum damage type adversary, q. This probability is an indicator of the uncertainty over type of the adversary i.e. maximum damage or infiltrating. We also study the effect of this probability on the expected property loss at each urban area.

Table 1
Expected damage data for the 10 urban areas with the highest losses.

Urban area	Expected property loss ($million)	Expected fatalities & injuries	Air departures (major & minor airports)
New York (NY)	413	5350	23599
Chicago (CH)	115	1212	39949
San Francisco (SF)	57	472	19,142
Washington, DC-MD-VA-WV (WDC)	36	681	17,253
Los Angeles-Long Beach (LA)	34	402	28,816
Philadelphia, PA-NJ (PHL)	21	199	13,640
Boston, MA-NH (BSTN)	18	225	11,625
Houston (HSTN)	11	160	20,979
Newark (NW)	7.3	74	12,827
Seattle-Bellevue-Everett (STL)	6.7	88	13,578
Total	719	8863	201,408

For the probability of detecting an attack set to 0.9, i.e., $d = 0.9$, Fig. 1 displays how defensive strategy may vary among sites for different values of q, and also Fig. 2 illustrates how the expected property loss at each urban area may vary over q. Fig. 1 shows that the defensive resources are evenly distributed for low values of q. This is due to the fact that for low values of q, the defender effectively plays the game against an infiltration type attacker, hence the defense resources are distributed proportionally with respect to the detection probabilities at different urban areas. However since we have assumed the same detection probability for each area as $d_i = d = 0.9$, the defensive resources are evenly distributed. As q increases beyond a certain level, more resources are allocated to NY and CH, which are the areas with highest property loss, and fewer resources are allocated to other areas. This shift in resource allocation happens around $q = 0.05$, that corresponds to a threshold point. As q increases further, the game is effectively turned into a maximum damage game and all defensive resources are distributed between two areas, namely NY and CH. Further increase in q does not change the allocation of resources. Fig. 2 shows distribution of the expected property loss at each urban area as a function of q. As seen in this figure, for low values of q, since the attacks are distributed among all areas and the defensive strategy is also to distribute the defensive resources evenly among all areas, the expected damage is roughly the same for all areas. As the value of q increases beyond a certain level, the defensive strategy changes to play the MD game. As the value of q increases further, the expected damage to important areas (such as NY, CH and SF)

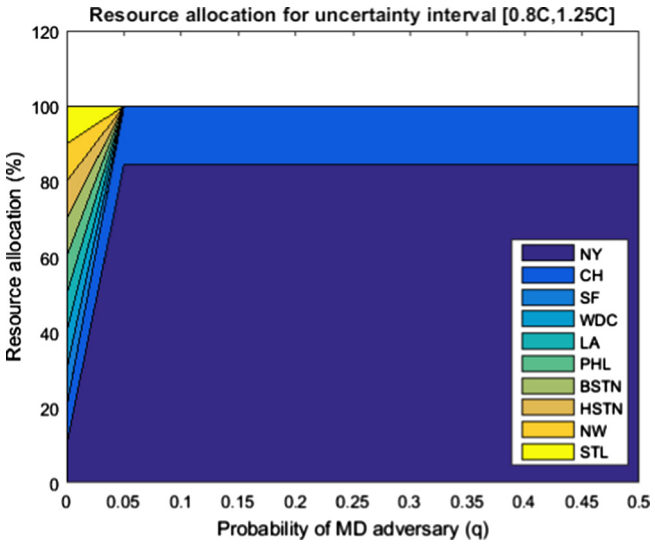

Fig. 1. Allocation of defensive resources for monetary data.

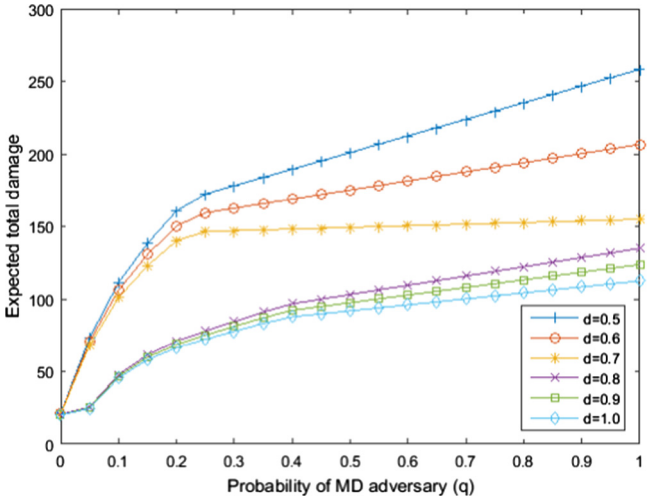

Fig. 3. Expected property loss over various detection probabilities.

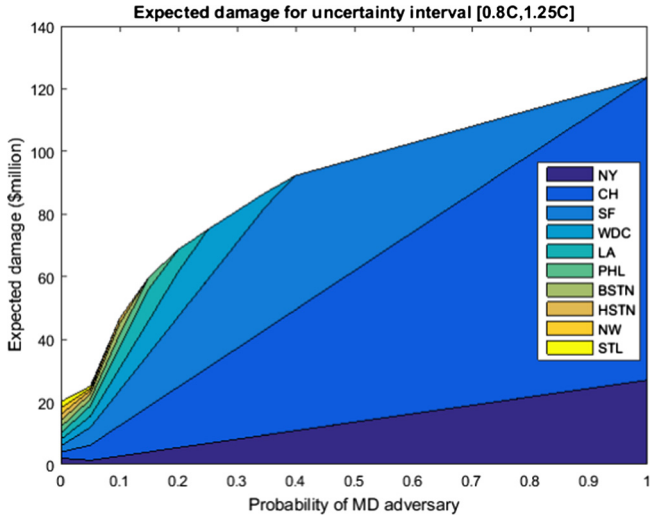

Fig. 2. Distribution of expected property loss.

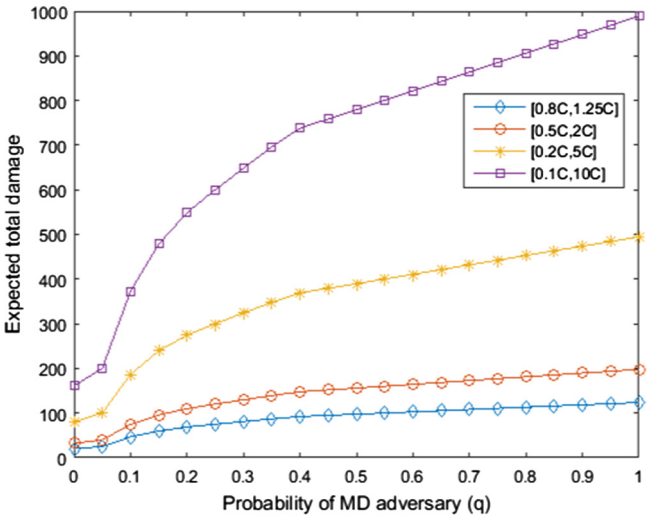

Fig. 4. Expected property loss over various uncertainty ranges.

increase and the expected damage to other areas decrease. This effect is observed because the adversary's attacks get more targeted towards high impact areas as q increases. Fig. 3 shows the expected total property loss as a function of q for different values of probability of detection, d. As seen in this figure, the damage is higher for smaller values of d and the difference increases as q increases. This is due to the increasing importance of the efficiency of defensive resources as the adversary targets high impact areas with higher probability.

Fig. 4 displays how expected total property loss changes as a function of q over various uncertainty ranges. As seen in this figure, for wider ranges of uncertainty the expected total damage is higher than scenarios with smaller uncertainty ranges.

3.2. Analysis for mortality value data

In this section we perform the robust game analysis based on the mortality value of each urban area. We study how the defenders strategy is affected by q. For $d_i = d = 0.9$, Fig. 5 illustrates how the defensive strategy changes for various values of q. As seen in the figure, for low values of q, because the game is effectively an infiltration game, defensive resources are evenly distributed among urban areas. As q increases beyond a certain level, more resources are allocated to NY and CH, which are the areas with highest population density, and fewer resources are allocated to other areas. This shift in resource allocation happens around $q = 0.05$. As q increases further, the game is effectively turned into

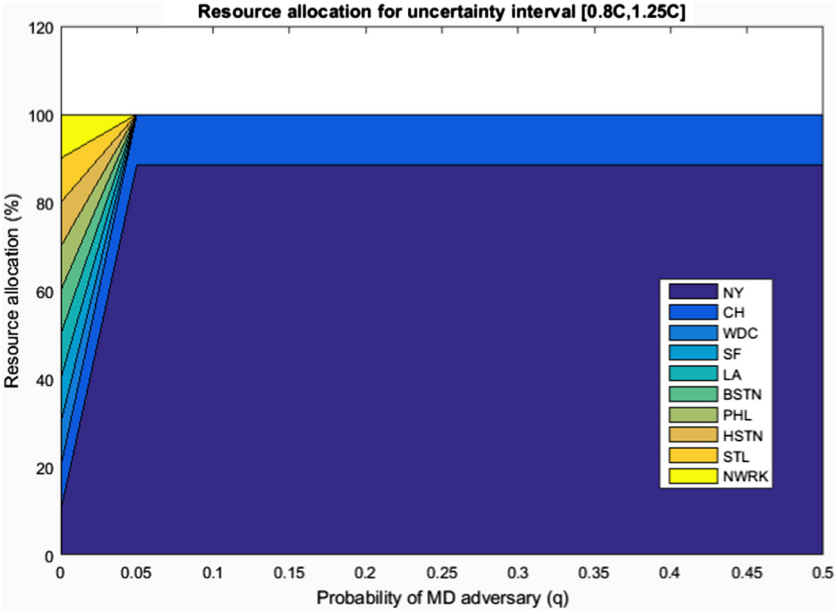

Fig. 5. Allocation of defensive resources for mortality data.

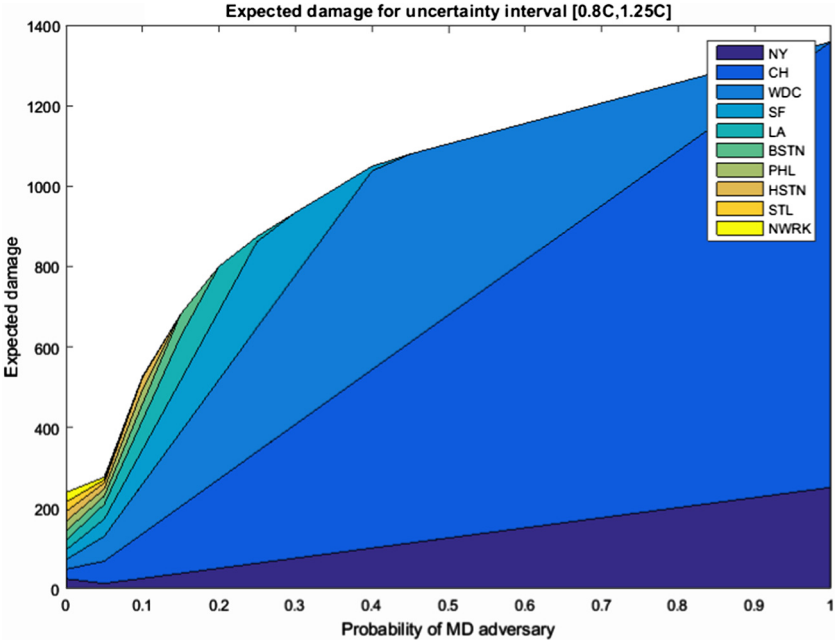

Fig. 6. Distribution of expected damage for mortality data.

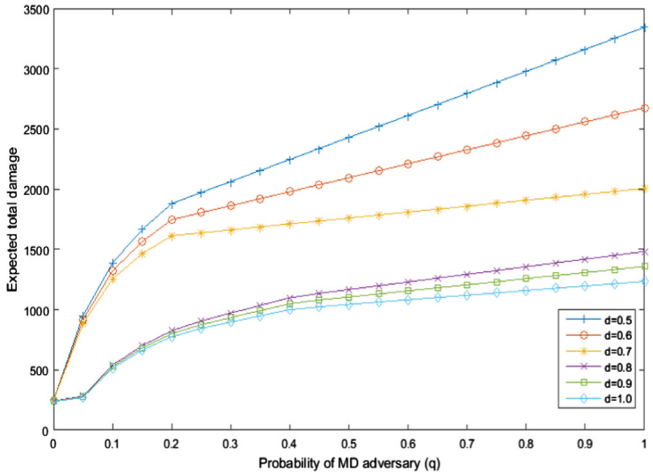

Fig. 7. Expected total damage for various detection probabilities.

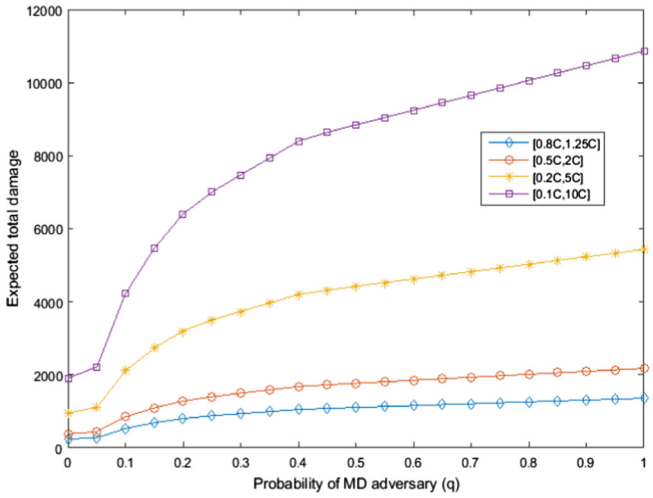

Fig. 8. Expected total damage for various uncertainty ranges.

a MD game and all defensive resources are distributed between two major areas, namely NY and CH. Further increase in q does not change the allocation of resources. Fig. 6 shows how the expected number of fatalities and injuries at each urban area changes for different values of q. As seen in this figure for low values of q, the expected damage is roughly the same for all areas. As the value of q increases beyond a certain level, the defensive strategy changes to play the MD game. As the value of q increases further, the expected damage on important areas (such as NY, CH and SF) increases and the expected damage for other areas decrease. This is due to the fact that as q increases, the adversary targets more important areas with higher probability. Fig. 7 displays the expected total damage as a function of q for various values of d. As seen in this figure, the damage is higher for smaller value of d and the difference increases as q increases. Fig. 8 illustrates how the expected total damage changes as a function of q for various uncertainty ranges. As seen in this figure, for wider ranges of uncertainty the expected total damage is higher than scenarios with smaller uncertainty ranges.

3.3. Analysis for political value data

In this section we perform the analysis based on the political value of each urban area. We study the effect of q on the defenders strategy. For $d_i = d = 0.9$, Fig. 9 shows how the defensive strategy changes for different values of q, and also Fig. 10 shows how the expected damage on each urban area may vary for different values of q.

As seen in Fig. 9, for low values of q, defensive resources are evenly distributed. As q increases beyond a certain level, more resources are allocated to CH, LA and NY which are the most important areas in terms of political value, and fewer resources are allocated to other areas. This shift in resource allocation happens around $q = 0.05$, which corresponds to a threshold point. Further shifts in defensive strategy happen at around $q = 0.1$, $q = 0.15$ and $q = 0.2$. At each of these threshold points, more defensive resources are assigned to the most important areas and fewer resources are allocated to other areas. As q increases further, the game is effectively a MD game and all defensive resources are distributed among four areas, namely CH, LA, NY and HSTN.

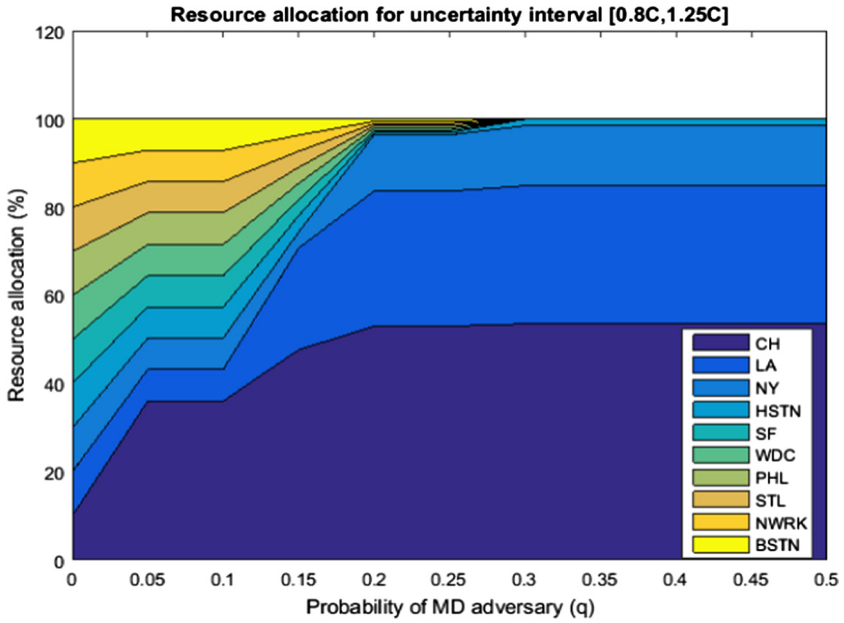

Fig. 9. Allocation of defensive resources for political data.

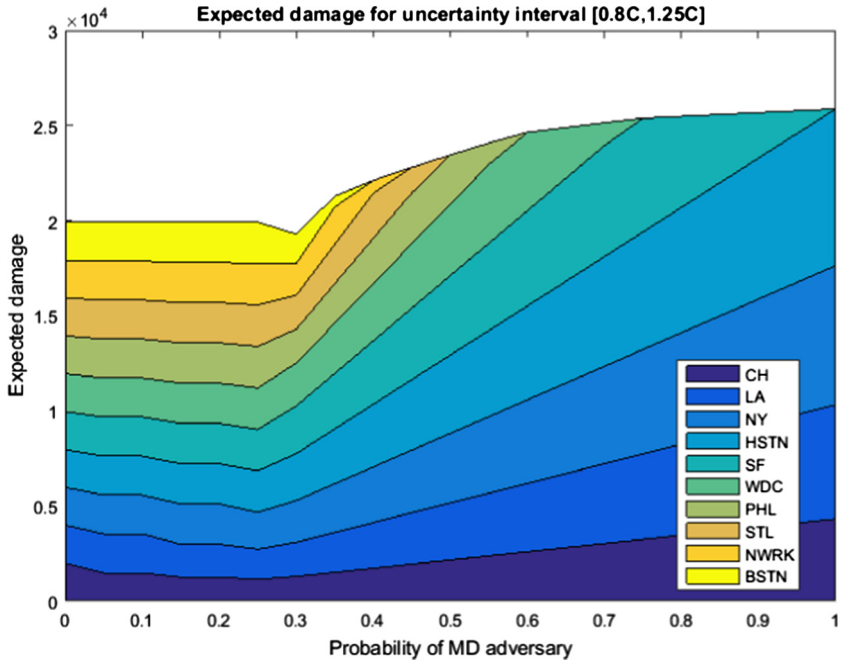

Fig. 10. Distribution of expected damage for political data.

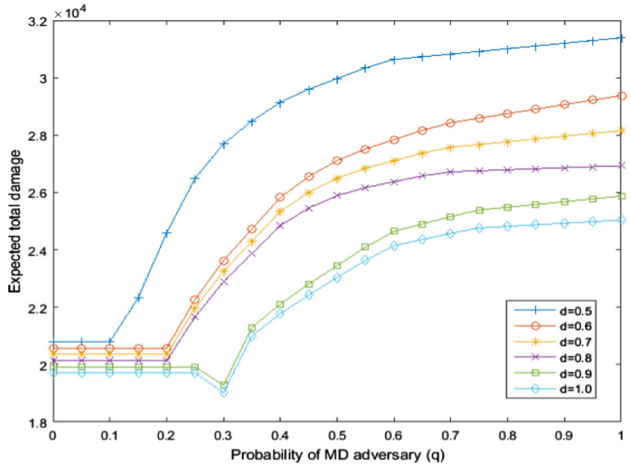

Fig. 11. Expected total damage for various probability of detection.

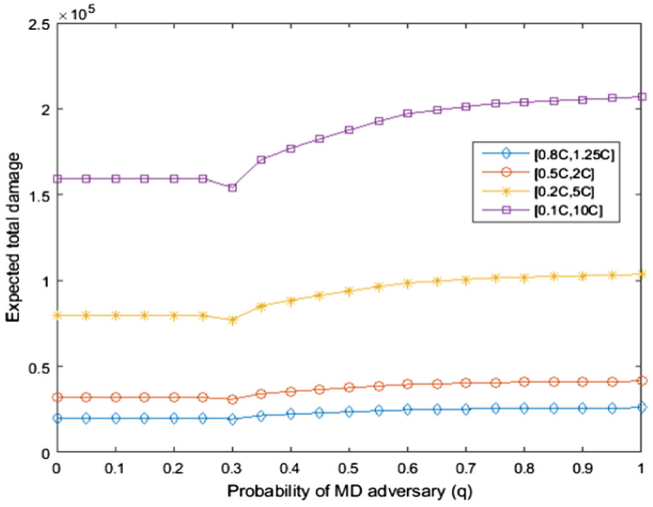

Fig. 12. Expected total damage for various uncertainty ranges.

After a certain point, further increase in q does not change the allocation of resources.

Fig. 10 displays the average expected damage to each urban area as a function of q, for low values of q, the expected damage is roughly the same for all areas. As the value of q increases further, both defender and the adversary focus more on the most important areas, therefore the expected damage on important areas (such as CH, LA, NY and HSTN) increases and the expected damage for other areas decrease.

Fig. 11 shows the expected total damage as a function of q for various values of d. As seen in this figure, the damage is higher for smaller value of d and the difference increases as q increases.

Fig. 12 illustrates how the expected total damage changes as a function of q for various uncertainty ranges. As seen in this figure, for wider ranges of uncertainty the expected total damage is higher than scenarios with smaller uncertainty ranges.

4. Conclusions and future research

In this paper we used a robust approach to model parameter uncertainty in the infrastructure security games. We developed three distribution-free models of incomplete informations games in which the players use a robust approach to contend with parameter uncertainty: maximum damage game, infiltration game and the game with information asymmetry. For the first two models, we prove existence and uniqueness of the Nash equilibrium and for the third model we characterize the shape of the Nash equilibrium. We showed that for the robust game with private information, the equilibrium strategy is of threshold type. We then applied the proposed approach to the real data on the expected annual terrorism losses at the 10 most valuable urban areas of the United States. We used the proposed robust game model to allocate defensive resources among these urban areas based on three aspects of the expected damage.

This paper extends the previous models by considering a non-zero-sum robust setting for the infrastructure security games. However, there are some limitations that call for further research in this area. Extending the model to accommodate multiple defenders and/or multiple adversaries is of current interest. Moreover, our proposed models assume that the detection probabilities are fixed and known in advance. Releasing this assumption is another avenue for future research in this area.

Appendix A. Proof of Theorem 3

Proof. The proof follows similar steps as the one in Garnaev et al. (2014). By definition of Nash Equilibrium, $(x,(\mathbf{y^1},\mathbf{y^2}))$ is an equilibrium if and only if for some v^1, v^2 and v:

$$(\overline{d}_i x_i - 1)\underline{C}_i \begin{cases} = v^1, & y_i^1 > 0, \\ \geqslant v^1, & y_i^1 = 0, \end{cases} \tag{A.1}$$

$$(\overline{d}_i x_i)\underline{C} \begin{cases} = v^2, & y_i^2 > 0, \\ \geqslant v^2, & y_i^2 = 0, \end{cases} \tag{A.2}$$

$$q\left(\underline{d}_i\overline{C}_i y_i^1 - \sum_{j=1}^{N}\overline{C}_j y_j^1\right) + (1-q)\left(\underline{d}_i\overline{C}_i y_i^2 - \sum_{j=1}^{N}\overline{C}_j y_j^2\right) \begin{cases} = v, & x_i > 0, \\ \leqslant v, & x_i = 0. \end{cases} \tag{A.3}$$

These conditions imply that $0 \leqslant v^2 \leqslant \underline{C}$ and $v^1 \leqslant 0$. There are two possible cases: (A) $x_i > 0$ for every i. (B) $x_i = 0$ for some i. As will be shown shortly, these two cases are equivalent to the cases $m \leqslant k$ and $m > k$, respectively.

Case (A): $x_i > 0$ for all i

Then, Eq. (A.2) indicates that $v^2 > 0$. Moreover, from Eq. (A.3), for every i, one can deduce that only three cases are possible:

Case A1: $\boldsymbol{y_i^1 > 0}$, $\boldsymbol{y_i^2 > 0}$. By Eqs. (A.1) and (A.2), $(\overline{d}_i x_i - 1)\underline{C}_i = v^1$, and $\overline{d}_i x_i \underline{C} = v^2$ holds, hence

$$C_i = -\frac{v^1}{1-\frac{v^2}{\underline{C}}}, \quad \textit{and} \quad x_i = \frac{v^2}{\overline{d}_i\underline{C}} = \frac{1}{\overline{d}_i}\left(\frac{v^1}{\underline{C}_i}+1\right), \qquad \forall\{i : y_i^1, y_i^2 > 0\}. \tag{A.4}$$

Case A2: $\boldsymbol{y_i^1 > 0}$, $\boldsymbol{y_i^2 = 0}$. Then, the appropriate equality and inequality from (A.1) and (A.2) become $(\overline{d}_i x_i - 1)\underline{C}_i = v^1$ and $\overline{d}_i x_i \underline{C} > v^2$, respectively, thus giving

$$\underline{C}_i \geqslant -\frac{v^1}{1-\frac{v^2}{\underline{C}}}, \quad \textit{and} \quad x_i = \frac{1}{\overline{d}_i}\left(\frac{v^1}{\underline{C}_i}+1\right), \qquad \forall\{i : y_i^1 > 0, y_i^2 = 0\}. \tag{A.5}$$

Case A3: $\boldsymbol{y_i^1 = 0}$, $\boldsymbol{y_i^2 > 0}$. The appropriate inequality and equality from (A.1) and (A.2) are $(\overline{d}_i x_i - 1)\underline{C}_i \geqslant v^1$ and $\overline{d}_i x_i \underline{C} = v^2$, respectively, therefore

$$\underline{C}_i \leqslant -\frac{v^1}{1-\frac{v^2}{\underline{C}}}, \quad \textit{and} \quad x_i = \frac{v^2}{\overline{d}_i\underline{C}}, \qquad \forall\{i : y_i^1 = 0, y_i^2 > 0\}. \tag{A.6}$$

Now, since $\underline{C}_i$ values are sorted it is obvious that there exists an m such that

$$\underline{C}_m = -\frac{v^1}{1-\frac{v^2}{\underline{C}}},$$

$$y_i^1 \begin{cases} > 0, & i \leqslant m-1, \\ \geqslant 0, & i = m, \\ = 0, & i \geqslant m+1, \end{cases} \tag{A.7}$$

$$y_i^2 \begin{cases} = 0, & i \leqslant m-1, \\ \geqslant 0, & i = m, \\ > 0, & i \geqslant m+1, \end{cases} \tag{A.8}$$

and:

$$x_i = \begin{cases} \frac{1}{\overline{d}_i}\left(\frac{v^1}{\underline{C}_i}+1\right), & i \leqslant m-1, \\ \frac{v^2}{\overline{d}_m\underline{C}} = \frac{1}{\overline{d}_m}\left(\frac{v^1}{\underline{C}_m}+1\right), & i = m, \\ \frac{v^2}{\overline{d}_i\underline{C}}, & i \geqslant m+1. \end{cases} \tag{A.9}$$

In turn, Eqs. (A.3), (A.7) and (A.8) imply:

$$y_i^1 = \begin{cases} \frac{v+(1-q)\sum_{j=1}^{N}\overline{C}_j y_j^2 + q\sum_{j=1}^{N}\overline{C}_j y_j^1}{\underline{d}_i\overline{C}_i q}, & i \leqslant m-1, \\ y_m^1, & i = m, \\ 0, & i \geqslant m+1, \end{cases} \tag{A.10}$$

$$y_i^2 = \begin{cases} 0, & i \leqslant m-1, \\ y_m^2, & i = m, \\ \frac{v+(1-q)\sum_{j=1}^{N}\overline{C}_j y_j^2 + q\sum_{j=1}^{N}\overline{C}_j y_j^1}{\underline{d}_i\overline{C}_i(1-q)}, & i \geqslant m+1, \end{cases} \tag{A.11}$$

and:

$$qy_m^1 + (1-q)y_m^2 = \frac{1}{\underline{d}_m\overline{C}_m}\left(v + (1-q)\sum_{j=1}^{N}\overline{C}_j y_j^2 + q\sum_{j=1}^{N}\overline{C}_j y_j^1\right). \tag{A.12}$$

From Eqs. (A.10) and (A.11) it can be easily seen that the right hand side of (A.12) can be written as

$$qy_m^1 + (1-q)y_m^2 = \frac{\underline{d}_i\overline{C}_i q y_i^1}{\underline{d}_m\overline{C}_m}, \quad \forall i \leqslant m-1, \tag{A.13}$$

$$qy_m^1 + (1-q)y_m^2 = \frac{\underline{d}_i\overline{C}_i(1-q)y_i^2}{\underline{d}_m\overline{C}_m}, \quad \forall i \geqslant m+1. \tag{A.14}$$

Because $\mathbf{y^1}$ and $\mathbf{y^2}$ are probability vectors, we have

$$\sum_{j=1}^{N} y_i^1 = 1, \quad \textit{and} \quad \sum_{j=1}^{N} y_i^2 = 1.$$

Hence, summing Eq. (A.13) for $1 \leqslant i \leqslant m-1$ yields $1 - y_m^1$, while summing Eq. (A.14) for $m+1 \leqslant i \leqslant N$ yields $1 - y_m^2$ and both provide the following equalities respectively.

$$qy_m^1\sum_{j=1}^{m}\frac{1}{\underline{d}_j\overline{C}_j} + (1-q)y_m^2\sum_{j=1}^{m-1}\frac{1}{\underline{d}_j\overline{C}_j} = \frac{q}{\underline{d}_m\overline{C}_m},$$

$$qy_m^1\sum_{j=m+1}^{N}\frac{1}{\underline{d}_j\overline{C}_j} + (1-q)y_m^2\sum_{j=m}^{N}\frac{1}{\underline{d}_j\overline{C}_j} = \frac{1-q}{\underline{d}_m\overline{C}_m}.$$

Finally, summing the above equations gives

$$qy_m^1 + (1-q)y_m^2 = \frac{1}{\underline{d}_m\overline{C}_m\sum_{j=1}^{N}\frac{1}{\underline{d}_j\overline{C}_j}},$$

in turn this leads to the unique solution in Eqs. (6) and (7).

In order to compute m note that $\mathbf{y^1}$ and $\mathbf{y^2}$ are probability vectors, thus $y_m^2 \geqslant 0$, $y_m^1 \geqslant 0$ in Eqs. (6) and (7), implying that $q \leqslant \psi_m$ and $q \geqslant \psi_{m-1}$, respectively.

The defender's strategy can be obtained from (A.1) and (A.2) that indicate

$$x_i = \frac{v^1 + \underline{C}_i}{\underline{C}_i\overline{d}_i}, \quad i \leqslant m, \tag{A.15}$$

$$x_i = \frac{v^2}{\underline{C}\overline{d}_i}, \quad i \geqslant m, \tag{A.16}$$

together with the normalization equation, $\sum_{i=1}^{N} x_i = 1$, yielding Eq. (5). To show that $m \leqslant k$, it is enough to show $\phi_m \leqslant 1$. From Eq. (A.15), we have $x_m = \frac{v^1 + \underline{C}_m}{\underline{C}_m \overline{d}_m}$, which leads to $v^1 \geqslant -\underline{C}_m$. Using this inequality, we have:

$$\phi_m = \sum_{j=1}^{m} \frac{\underline{C}_j - \underline{C}_m}{\overline{d}_j \underline{C}_j} \leqslant \sum_{j=1}^{m} \frac{\underline{C}_j + v^1}{\overline{d}_j \underline{C}_j} = \sum_{j=1}^{m} x_j \leqslant 1.$$

Case B:

Suppose there exists an i such that $x_i = 0$. Then by (A.2) $v^2 = 0$, therefore $y_i^2 = 0$ for $x_i > 0$. From Eqs. (A.1)–(A.3), for every i, one can deduce that only three cases are possible:

Case B1: $\boldsymbol{y_i^1 > 0}$, $\boldsymbol{y_i^2 > 0}$. Eqs. (A.1) and (A.2), again imply (A.4).

Case B2: $\boldsymbol{y_i^1 > 0}$, $\boldsymbol{y_i^2 = 0}$. Then, (A.5) holds.

Case B3: $\boldsymbol{y_i^1 = 0}$, $\boldsymbol{y_i^2 > 0}$. Then (A.6) immediately follows.

Since $\underline{C}_i$ values are sorted, and from Eqs. (A.1), (A.3), (A.4), (A.5) and (A.6) there exists a k such that

$$x_i = \begin{cases} \frac{1}{\overline{d}_i}\left(\frac{v^1}{\underline{C}_i} + 1\right), & y_i^1 > 0, \\ 0, & y_i^1 = 0, \end{cases} \tag{A.17}$$

$$y_i^1 = \begin{cases} \frac{v + (1-q)\sum_{j=1}^{N} \overline{C}_j y_j^2 + q \sum_{j=1}^{N} \overline{C}_j y_j^1}{\underline{d}_i \overline{C}_i q}, & i \leqslant k, \\ 0, & i > k, \end{cases} \tag{A.18}$$

and

$$y_i^2 \begin{cases} = 0, & i \leqslant k, \\ \leqslant \frac{v + q\sum_{j=1}^{N} \overline{C}_j y_j^1 + (1-q)\sum_{j=1}^{N} \overline{C}_j y_j^2}{\underline{d}_i \overline{C}_i (1-q)}, & i > k. \end{cases} \tag{A.19}$$

Solving these equations together with the normalization equations leads to the solution characterized in Eqs. (8)–(10).

To compute k, note that $x_k \geqslant 0$, implying $\phi_k \leqslant 1$. To show that $m > k$ it is enough to show $\psi_k < q$. Eq. (10) gives

$$y_i^{*2} < \frac{q}{(1-q)} \left(\frac{\frac{1}{\underline{d}_i \overline{C}_i}}{\sum_{l=1}^{k} \frac{1}{\underline{d}_l \overline{C}_l}} \right), \forall i > k, \quad \sum_{j=k+1}^{N} y_j^{*2} = 1.$$

Using these equations, we have:

$$1 = \sum_{j=k+1}^{N} y_j^{*2} < \frac{q}{1-q} \left(\frac{\sum_{j=k+1}^{N} \frac{1}{\underline{d}_j \overline{C}_j}}{\sum_{j=1}^{k} \frac{1}{\underline{d}_j \overline{C}_j}} \right),$$

which leads to $\psi_k = \frac{\sum_{j=1}^{k} \frac{1}{\underline{d}_j \overline{C}_j}}{\sum_{j=1}^{N} \frac{1}{\underline{d}_j \overline{C}_j}} < q$. This completes the proof. □

References

Aghassi, M., & Bertsimas, D. (2006). Robust game theory. *Mathematical Programming, 107*(1–2), 231–273.

Baykal-Gürsoy, M., Duan, Z., Poor, H. V., & Garnaev, A. (2014). Infrastructure security games. *European Journal of Operational Research, 239*(2), 469–478.

Bureau of Counterterrorism (2016). National consortium for the study of terrorism and responses to terrorism: Annex of statistical information, June.

Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., & Van Arsdale, L. A. (2004). Confronting the risks of terrorism: Making the right decisions. *Reliability Engineering & System Safety, 86*(2), 129–176.

Garcia, M. L. (2005). *Vulnerability assessment of physical protection systems*. Butterworth-Heinemann.

Garnaev, A., Baykal-Gürsoy, M., & Poor, H. V. (2014). Incorporating attack-type uncertainty into network protection. *IEEE Transactions on Information Forensics and Security, 9*(8), 1278–1287.

Garnaev, A., Baykal-Gürsoy, M., & Poor, H. V. (2015). How to deal with an intelligent adversary. *Computers & Industrial Engineering, 90*(C), 352–360. December.

Garnaev, A., Baykal-Gürsoy, M., & Poor, H. V. (2016). Security games with unknown adversarial strategies. *IEEE Transactions on Cybernetics, 46*(10), 2291–2299.

Harris, B. (2004). Mathematical methods in combatting terrorism. *Risk Analysis, 24*(4), 985–988.

Harsanyi, J. C. (1967). Games with incomplete information played by Bayesian players, i–iii: Part i. The basic model&. *Management Science, 50*(12_supplement), 1804–1817.

Harsanyi, J. C. (1968a). Games with incomplete information played by Bayesian players part II. Bayesian equilibrium points. *Management Science, 14*(5), 320–334.

Harsanyi, J. C. (1968b). Games with incomplete information played by Bayesian players, part III. The basic probability distribution of the game. *Management Science, 14*(7), 486–502.

Insua, D. R., Rios, J., & Banks, D. (2009). Adversarial risk analysis. *Journal of the American Statistical Association, 104*(486), 841–854.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis, 1*(1), 11–27.

Kardeş, E. (2014). On discounted stochastic games with incomplete information on payoffs and a security application. *Operations Research Letters, 42*(1), 7–11.

Kiekintveld, C., Islam, T., & Kreinovich, V. (2013). Security games with interval uncertainty. In *Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems* (pp. 231–238). International Foundation for Autonomous Agents and Multiagent Systems.

Konak, A., Kulturel-Konak, S., & Snyder, L. V. (2015). A game-theoretic genetic algorithm for the reliable server assignment problem under attacks. *Computers & Industrial Engineering, 85*, 73–85.

Kuhn, H. W., & Tucker, A. W. (1951). Nonlinear programming. In *Proceedings of the second Berkeley symposium on mathematical statistics and probability* (pp. 481–492). Berkeley, Calif.: University of California Press.

McGill, W. L., Ayyub, B. M., & Kaminskiy, M. (2007). Risk analysis for critical asset protection. *Risk Analysis, 27*(5), 1265–1281.

Nikoofal, M. E., & Zhuang, J. (2012). Robust allocation of a defensive budget considering an attacker's private information. *Risk Analysis, 32*(5), 930–943.

Nikoofal, M. E., & Zhuang, J. (2015). On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research, 246*(1), 320–330.

Paruchuri, P., Pearce, J. P., Marecki, J., Tambe, M., Ordóñez, F., & Kraus, S. (2008). Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games. In *Proceedings of the 7th international joint conference on autonomous agents and multiagent systems-Volume 2* (pp. 895–902). International Foundation for Autonomous Agents and Multiagent Systems.

Paruchuri, P., Pearce, J. P., Tambe, M., Ordóñez, F., & Kraus, S. (2007). An efficient heuristic approach for security against multiple adversaries. In *Proceedings of the 6th international joint conference on autonomous agents and multiagent systems* (pp. 181). ACM.

Paruchuri, P., Tambe, M., Ordóñez, F., & Kraus, S. (2006). Security in multiagent systems by policy randomization. In *Proceedings of the fifth international joint conference on autonomous agents and multiagent systems* (pp. 273–280). ACM.

Paté-Cornell, E., & Guikema, S. (2002). Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research, 7*(4), 5–23.

Paté-Cornell, E. (2002). Fusion of intelligence information: A Bayesian approach. *Risk Analysis, 22*(3), 445–454.

Pita, J., Jain, M., Marecki, J., Ordóñez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., & Kraus, S. (2008). Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In *Proceedings of the 7th international joint conference on autonomous agents and multiagent systems: Industrial Track* (pp. 125–132). International Foundation for Autonomous Agents and Multiagent Systems.

Qian, Y., Haskell, W. B., & Tambe, M. (2015). Robust strategy against unknown risk-averse attackers in security games. In *Proceedings of the 2015 international conference on autonomous agents and multiagent systems* (pp. 1341–1349). International Foundation for Autonomous Agents and Multiagent Systems.

Shan, X., & Zhuang, J. (2013). Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *European Journal of Operational Research, 228*(1), 262–272.

Willis, H. H., Morral, A. R., Kelly, T. K., & Medby, J. J. (2006). *Estimating terrorism risk*. Rand Corporation.

Xu, J., & Zhuang, J. (2016). Modeling costly learning and counter-learning in a defender-attacker game with private defender information. *Annals of Operations Research, 236*(1), 271–289.