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.