European Journal of Operational Research 239 (2014) 469–478

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Decision Support

Infrastructure security games ☆

Melike Baykal-Gürsoy [a,*], Zhe Duan [b], H. Vincent Poor [c], Andrey Garnaev [d]

[a] Department of Industrial and Systems Engineering, RUTCOR and CAIT, Rutgers University, 96 Frelinghuysen Rd, Piscataway, NJ 08854-8018, United States
[b] Department of Management Science, School of Management, Xi'An Jiaotong University, Shaanxi Province 710049, China
[c] Department of Electrical Engineering, Princeton University, Princeton, NJ, United States
[d] Department of Computer Modeling and Multi-Processor Systems, Saint Petersburg State University, St Petersburg, Russia

ARTICLE INFO

Article history:
Received 27 June 2013
Accepted 23 April 2014
Available online 14 May 2014

Keywords:
Uncertainty modeling
Game theory
Matrix game
Bayesian game
Moving targets

ABSTRACT

Infrastructure security against possible attacks involves making decisions under uncertainty. This paper presents game theoretic models of the interaction between an adversary and a first responder in order to study the problem of security within a transportation infrastructure. The risk measure used is based on the consequence of an attack in terms of the number of people affected or the occupancy level of a critical infrastructure, e.g. stations, trains, subway cars, escalators, bridges, etc. The objective of the adversary is to inflict the maximum damage to a transportation network by selecting a set of nodes to attack, while the first responder (emergency management center) allocates resources (emergency personnel or personnel-hours) to the sites of interest in an attempt to find the hidden adversary. This paper considers both static and dynamic, in which the first responder is mobile, games. The unique equilibrium strategy pair is given in closed form for the simple static game. For the dynamic game, the equilibrium for the first responder becomes the best patrol policy within the infrastructure. This model uses partially observable Markov decision processes (POMDPs) in which the payoff functions depend on an exogenous people flow, and thus, are time varying. A numerical example illustrating the algorithm is presented to evaluate an equilibrium strategy pair.

1. Introduction

The September 11, 2001 attacks introduced the term *homeland security* into the public consciousness around the world. In the United States, this term is defined as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (Homeland Security Act 2002 Congress, 2002). Within this effort, protecting critical infrastructure has become an utmost priority for governments (Moteff, 2005). Executive Order 13010 (Clinton, 1996) signed by President Clinton in 1996 identifies transportation infrastructure as a critical system supporting the national security and economic well-being of this nation. Moreover, as the Bali and Madrid bombings illustrate, terrorists also target large crowds. Public transit systems, used daily by 32 million mass transit riders in the United States, and places of mass gathering such as shopping malls and stadiums are considered part of the critical infrastructure (Bennett, 2007; Boin & Smith, 2006; Rothery & Branch, 2005). Public transit systems by design are open structural environments equipped to move large numbers of mass transit patrons in an effective and efficient manner. Therefore, mass transit systems are considered *soft targets* similar to the other public places that are inherently vulnerable and susceptible to terrorist attacks and which, because of the continuous hours of service, cannot be closed and secured as may other sectors of the area transportation system (Loukaitou-Sideris, Taylor, & Fink, 2006). Successful and attempted terrorist attacks throughout the world such as New York, Bali, Madrid, London, Mumbai, Russia, and Norway clearly demonstrate that terrorists' primary mission remains to be to cause mass human casualties in addition to panic and chaos (Bennett, 2007). The threat to any given infrastructural component or "infrastructure" could be substantially reduced by analyzing the risk associated with each transit infrastructure, mitigation planning, and employing best prevention and response policies.

There has been a recent interest in issues related to infrastructure security. A major tool for risk assessment, probabilistic risk analysis (PRA) (Kaplan & Garrick, 1981), has also been applied to terrorism risks (Garcia, 2005; Garrick et al., 2004; McGill, Ayyub,

☆ This research has been supported by the Rutgers University TCC/FTA (Transportation Coordinating Council/Federal Transit Administration).

* Corresponding author. Tel.: +1 (848) 445 5465.
E-mail addresses: gursoy@rci.rutgers.edu (M. Baykal-Gürsoy), zheduan@mail.xjtu.edu.cn (Z. Duan), poor@princeton.edu (H.V. Poor), garnaev@yahoo.com (A. Garnaev).

http://dx.doi.org/10.1016/j.ejor.2014.04.033
0377-2217/

& Kaminskiy, 2007; Paté-Cornell, 2002a; Paté-Cornell, 2002b). On the other hand, the National Research Council N.R.C. of the National Academies, 2008 has emphasized game theoretic models (Cournot, 1971; Isaacs, 1965; Nash, 1951; Von Neumann & Morgenstern, 1944; Von Neumann, Morgenstern, Rubinstein, & Kuhn, 2007) to counter the need for adaptation to the dynamic behavior of the terrorism events and adversarial decision-making processes of terrorists. One such model, ARMOR (Paruchuri et al., 2007, 2008; Paruchuri, Tambe, Ordez, & Kraus, 2005, 2006; Pita et al., 2008), casts the *interdiction* problem as a Bayesian Stackelberg game (Basar & Olsder, 1999), and has been deployed to secure the Los Angeles International Airport. However, this model is static in the sense that it is solved every day with new parameters and the payoff functions for players remain the same throughout the day and the players are assumed to be rational. Aside from the ARMOR game, Brown, Carlyle, Salmeron, and Wood (2006) consider various Stackelberg games, while others study network interdiction games (Atkinson, Cao, & Wein, 2008; Atkinson & Wein, 2008; Johnson & Gutfraind, 2011; Gutfraind & Hagberg, 2009; Lim & Smith, 2007; Morton, Pan, & Saeger, 2007; Washburn & Wood, 1995; Wein & Atkinson, 2007; Wein, 2009; Wood, 1993), secrecy and deception (Dighe, Zhuang, & Bier, 2009; Zhuang & Bier, 2007, 2009; Zhuang, Bier, & Alagoz, 2010), passenger classification (Nie, Batta, Drury, & Lin, 2009a; Nie, Batta, Drury, & Lin, 2009b), and optimal placement of suicide bomber detectors in a grid structure (Nie, Batta, Drury, & Lin, 2007). Hochbaum and Fishbain (2011) investigate the allocation of mobile sensors in an urban environment in order to detect *dirty bombs*. Note that the models in Nie et al. (2009a, 2009b) and Nie et al. (2007) involve only a single controller and not multiple decision makers as in game models.

In this paper, we approach the infrastructure security problem via game theory by modeling it via *hide-and-seek games* (Alpern, Baston, & Gal, 2008; Alpern & Gal, 2003; Alpern, Morton, & Papadaki, 2011; Dobbie, 1968; Garnaev, 2000; Hespanha, Prandini, & Sastry, 2000; Hohzaki, 2007; Jotshi & Batta, 2008; Alpern et al., 2011; Suzuki & Yamashita, 1992; Thomas & Washburn, 1991). There are two settings for such games: static and dynamic. In the static model, a first responder (emergency-management center) allocates resources (emergency personnel, or personnel-hours) to sites of interest in an attempt to find an object (person or bomb, "adversary") that has been hidden, while the adversary selects a set of best sites to attack. Once the object is hidden, it cannot move during the search process. Similarly, the first responder can act only once. Various different games have been defined for dynamic situations depending on the mobility of the agents. *Search games* (Gal, 1980) involve a mobile defender and an immobile adversary, while *ambush games* (Ruckle, 1981) have a mobile adversary and an immobile defender, who waits for the adversary to appear. Finally, if both agents are mobile, such games could be pursuit–evasion games (Isaacs, 1965; Hespanha et al., 2000) or *infiltration games* (Alpern, 1992; Garnaev, Garnaeva, & Goutal, 1997). Most research has focused on the case in which the cells are identical. However, Neuts (1963) and later on Sakaguchi (1973) consider a zero-sum dynamic search game with node dependent inspection costs. Moreover, there may be a possibility of type 1 error, i.e., false negative, associated with each node, i.e., the probability that the first responder finds the adversary given that the adversary is in the searched node may be less than 1. In general, in the hide-and-seek games there are no attack targets, in fact, the adversary is the target. One exception arises in the *interdiction games* (Washburn & Wood, 1995; Wood, 1993) in which the adversary tries to reach a target while the defender tries to prevent the adversary from reaching the target, thereby protecting the target. Recently, interdiction games with various targets have been considered. Such games are called *protection games* (please see Basilico, Gatti, & Amigoni (2012) and the references therein).

In this paper, we study protection games. Focusing on severe attacks, we consider the loss of human life as the consequence of the attack, i.e., the payoff to the adversary. This measure typically depends on the occupancy level of the facility and we assume that the occupancy level can be estimated over time. Hence the crowds are the targets in this game and since they are moving over time they are dynamically moving targets. The static version of this game becomes a simple zero-sum game related to the one considered by Neuts (1963) and Sakaguchi (1973). However, contrary to their case we observe that in our game a continuum equilibrium for the adversary may exist under certain conditions. In the dynamic game model, we assume that the first responder can move among the nodes to search for a hidden immobile adversary. This game is called as *patrolling* game (Alpern et al., 2011; Basilico et al., 2012) with the additional feature of multiple mobile targets. We sometimes refer to resources allocated to the nodes also as first responders. The main idea here is that if the emergency-management center has a finite number of first responders, it then allocates fractions of first responders to the nodes. Throughout we use first responder and defender, and, respectively, adversary and attacker, synonymously.

The contributions of this paper are itemized below.

- A new static game is introduced that considers the occupancy of a node as the payoff to the adversary. This game is shown to have a unique equilibrium for the first responder in closed form. However, the adversary may have a continuum of equilibria, also given in closed form. The equilibria are of threshold type, i.e., the resources are allocated to the nodes with occupancy higher than a threshold value.
- A novel protection game with dynamically moving targets is introduced, and its solution algorithm through an illustrative example is provided.

The structure of the paper is as follows. In Section 2, we consider the static game and present the unique equilibrium in closed form. In Section 3, a people flow model is introduced. In Section 4, a dynamic game between an immobile adversary and a mobile first responder is discussed. In Section 5, we present a numerical example for the dynamic game. Finally, further applications and future research directions are discussed in Section 6.

2. Static infrastructure game model

In this section, we consider the one-step security problem. The adversary and the first responder simultaneously choose their strategies over the potential sites. Payoff matrices for both responder and adversary are based on the occupancy level of each site in the infrastructure. Even when both rivals are at the same site, there is a probability that the first responder may not detect the adversary. We do not consider the possibility of type 2 error, false positive, and assume that if an attacker is found then s/he is the adversary with certainty.

We assume that the infrastructure can be partitioned into nodes. This could be achieved, for example, as described in Kolling and Carpin (2008) and Portugal and Rocha (2012). We further assume that the impact of an attack will be based upon the occupancy level of the specific node at which the attack happens and can only endanger the people at that node. People in neighboring nodes will not be hurt directly due to this attack. We assume that the probability of detection, and the occupancy of each node, are known to both rivals.