European Journal of Operational Research 242 (2015) 212–221

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Decision Support

Critical infrastructure protection using secrecy – A discrete simultaneous game

Chi Zhang[a], José Emmanuel Ramirez-Marquez[b,d,*], Jianhui Wang[c]

[a] Department of Industrial Engineering, Tsinghua University, Beijing 100084, PR China
[b] School of Systems and Enterprises, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ, 07030, USA
[c] Decision and Information Sciences Division, Argonne National Laboratory, IL, 60439, USA
[d] Graduate School, Tecnológico de Monterrey – Campus Guadalajara, Av. General Ramón Corona # 2514, Guadalajara, 45201, Mexico

ARTICLE INFO

Article history:
Received 31 March 2014
Accepted 1 October 2014
Available online 13 October 2014

Keywords:
Critical infrastructure protection
Simultaneous game
Intentional attack
Information
Secrecy

ABSTRACT

In this research, critical infrastructure protection against intentional attacks is modeled as a discrete simultaneous game between the protector and the attacker, to model the situation that both players keep the information of their resource allocation secret. We prove that keeping the information regarding protection strategies secret can obtain a better effect of critical infrastructure protection than truthfully disclosing it. Solving a game theoretic problem, even in the case of two players, has been known to be intractable. To deal with this complexity, after proving that pure-strategy Nash equilibrium solutions do not exist for the proposed simultaneous game, a new approach is proposed to identify its mixed-strategy Nash equilibrium solution.

1. Introduction

The economic development and social wellbeing of modern societies are highly dependent on critical infrastructures, such as energy transmission and distribution, transportation and telecommunication (Ramirez-Marquez, Rocco, & Levitin, 2009; Simic, Lugaric, & Krajcar, 2009). Their continued effective performance creates a national sense of confidence, identity and purpose (The White House, 2003). Conversely, the destruction or degradation of such critical infrastructures could have a debilitating impact on the economy, the security, the public health or the safety of a nation (Chakravarty, 2011; Cheatle, 2006; Ojha, Salimath, & D'Souza, 2014). Thus, understanding intelligent and cost-effective approaches for their protection and upkeep has become and will continue to be paramount (Ramirez-Marquez et al., 2009; Zhang, Ramirez-Marquez, & Rocco, 2011).

Intentional attackers have become one of the major threats contemplated against critical infrastructures. They are known to be inventive and resourceful and even have an advantage over the protector in terms of choosing the time, the targets, and the means of attacks (Bier, Cox, & Azaiez, 2009; Levitin & Hausken, 2010). Also, they have the ability to collect the information about an infrastructure (e.g. the configuration and protective measures) and analyze it to develop optimal attack strategies (Brown, Carlyle, Salmeron, & Wood, 2006). Most importantly, they can be adaptive so as to change their attack strategies in response to the change of protection strategies.

Thus, the interaction between the attacker and the protector need to be addressed, in order to develop cost-effective strategies to protect critical infrastructures from intentional attacks. Game theoretic approaches have been proven useful to fulfill this purpose (Bier et al., 2009; Hausken & Zhuang, 2011; Zhang & Ramirez-Marquez, 2013; Zhuang, Bier, & Alagoz, 2010). The reader is referred to Hausken and Levitin (2012) for a review of infrastructures defense and attack models.

One of the most important issues encountered by the protector when implementing game theoretic approaches is the information disclosure policy. One policy, referred to as truthful disclosure in this research, is that the protector truthfully discloses all the information regarding the protection measures adopted, so that the attacker can obtain these information before making decisions. This policy is usually modeled as a two-stage game in the literature (Azaiez & Bier, 2007; Bier, Nagaraj, & Abhichandani, 2005; Hausken & Levitin, 2009; Hausken & Zhuang, 2011; Korzhyk, Yin, Kiekintveld, Conitzer, & Tambe, 2011; Levitin, 2009; Zhang & Ramirez-Marquez, 2013), within which the protector allocates resources to protect the infrastructure in the first stage. Then, in the second stage, after being aware of how the defensive resources are allocated without any uncertainty, the attacker determines the optimal attack strategy.

Another policy of information disclosure, referred to as secrecy in this research, is that the protector keeps the whole or partial information of protection strategies secret so that the attacker has no or only

[*] Corresponding author. Tel.: +1 2012168003.
E-mail address: Jose.Ramirez-Marquez@stevens.edu (J.E. Ramirez-Marquez).

http://dx.doi.org/10.1016/j.ejor.2014.10.001
0377-2217/© 2014 Elsevier B.V. All rights reserved.

limited information about the allocation of protection resources when determining attack strategies. Zhuang and Bier (2010) described several applications, without quantitative analysis, where secrecy would be preferred to truthful disclosure, such as a theft game, Lojack, and onboard air marshals. In the case of onboard air marshals, if the information about which specific planes have air marshals is kept secret, attack deterrence can be obtained by having air marshals aboard only a limited number of planes.

However, the comparisons between the two aforementioned information disclosure policies conducted by a series of studies, such as Bier (2007), Zhuang and Bier (2007), Hausken (2011b) and Hausken and Bier (2011), indicate that the protector should truthfully disclose the information about protection strategies, instead of keeping it secret. It has been suspected that the possible reasons for this conclusion lie in the assumptions adopted by these studies: 1) the protector has no private information; 2) the success probability of an attack is a convex function of the amount of protection resources allocated; 3) decision variables (i.e., the amount of resources allocated to each component) are continuous (Dighe, Zhuang, & Bier, 2009; Zhuang & Bier, 2010). Moreover, they did not consider mixed strategies.

Another drawback of existing studies considering secrecy is that they are usually restricted to systems with trivial structures (e.g., isolated components, series, parallel, series–parallel, etc.). In the proposed zero-sum game, Major (2002) considered a system as the combination of isolated components. Levitin and Hausken (2010) considered only parallel systems with identical components to study the influence of the attacker's unprotected component detection capacity on the development of protection strategies.

Based on the rent-seeking model, Hausken and Bier (2011) described a simultaneous game between one protector and multiple attackers, viewing the studied system as an isolated component. Hausken (2011a) studied interlinked components, but modeled the total damage under attack as a weighted-sum of damages to certain series and parallel systems. The structure studied by Hausken (2010) is more realistic. However, he transferred the game theoretic problem into a reliability analysis problem, which has been known to be NP-hard (Agrawal & Barlow, 1984).

Although Zhuang et al. (2010) and Zhuang and Bier (2011) identified secrecy at equilibrium, these studies are also focused on an isolated component. They also assume that the protector has private information, such as target valuations and expense effectiveness. Assuming that the success probability of an attack is a non-convex function of the amount of protection resources allocated and strategies are discrete, Dighe et al. (2009) also indicates that secrecy should be preferred to truthful disclosure by the protector. However, they only considered two isolated components.

In all, the benefits of secrecy over truthful disclosure have not yet been properly studied in the context of real-world infrastructures, which usually have more general structures than those studied by existing studies. Also, how to efficiently allocate defensive resources among potential components of an infrastructure to make use of secrecy when possible is still an open question.

Secrecy can be studied in a simultaneous game, within which each player has to make their decisions before knowing their opponents' strategies (Zhuang & Bier, 2007, 2011). Therefore, to address current research gaps, this research proposes a simultaneous game between the protector and the attacker, to model the problem of critical infrastructure protection against intentional attacks using secrecy. Comparatively, when truthful disclosure of information is employed by the protector, the game is modeled as a two-stage game with the protector moving first, as in the literature.

A flow network is employed to represent a critical infrastructure. In the proposed games, the protector seeks to find the optimal protection strategy, which is to protect a subset of the network links within his/her resources, while the attacker seeks to inflict the highest level of damage to the network by attacking a subset of the network links, also within his/her resources. The maximal network flow between the source and sink nodes of the network is employed in this research as a figure of merit. Destruction of network links leads to the decrease of the maximal network flow and the amount of this decrease is understood as the total damage to the whole infrastructure. Thus, the objective of the protector and the attacker is to respectively maximize and minimize the maximal network flow, assuming that they are both rational players.

Given the protection and attack strategies described above, the two information disclosure policies can be further clarified as follows. If the attacker knows exactly which specific links have been protected at the time of making decisions, we say that the protector is truthfully disclosing information about his/her strategies. Comparatively, as long as the attacker cannot be sure about which specific links have been protected before making decisions, it is viewed that the secrecy policy has been adopted by the protector.

Secrecy can be achieved, for example, by randomly choosing links to protect, as in a mixed strategy, which is known as a probability distribution over the player's actions (Osborne, 2004). Under a mixed strategy, the protector randomly chooses links to protect in each time period, according to the specific probability distribution. This way, although the attacker may be able to infer the probabilities that each link is protected, he/she is uncertain about which specific links have been protected when making decisions. We believe that this uncertainty provides the protector more cost-effective utilization of scarce protection resources.

As a building block to solving more realistic problems, we assume that, once a link is protected, it cannot be destroyed by the attacker. Thus, the attack success probability is considered as a non-convex function of the amount of protection resources devoted. We also assume that except for the exact allocation of attack and defensive resources are kept secret by the attacker and the protector respectively when the policy of secrecy is adopted, there is no other private information held by the two players. Specifically, each player knows his/her opponent's resource constraints, valuation of the infrastructure, the infrastructure's topology and so forth.

Note that in the proposed simultaneous game, the two players do not have to move at exactly the same time. The game can be viewed as a simultaneous game as long as no players have information of their opponents' strategies (i.e., the subset of links protected/attacked). Under the described assumptions, we prove that pure-strategy Nash equilibrium solution does not exist for the proposed simultaneous game and, it is preferred keeping information of protection resource allocation secret, as in the simultaneous game, rather than truthfully disclosing it, as in the sequential game.

The number of protection/attack strategies increases exponentially as the number of network links increases, which leads to a computational challenge considering that real-world infrastructures usually have thousands of or even millions of components (consider national power grids, public telecommunication systems, and the world wide web). Approaches based on complete set of strategies of each player (e.g., Lemke–Howson algorithm (Lemke & Howson, 1964)) would be too time consuming to identify Nash equilibrium solution of the proposed game.

To deal with this challenge, this research tailored the algorithm described by Godinho and Dias (2010, 2013) to solve the proposed simultaneous game. One of the most important steps for implementing this algorithm is to identify the best response of each player to his/her adversary's strategy. This problem is modeled as a Network Interdiction Problem (NIP).

The remainder of this paper is organized as follows. In Section 2, the problem is described and the simultaneous game is proposed. Section 3 describes the algorithm of identifying the equilibrium solution to the game described in Section 2. In Section 4, experimentation is presented to illustrate the proposed approach. Finally, Section 5 discusses the proposed approach and concludes the article.