European Journal of Operational Research 226 (2013) 286–292

Contents lists available at SciVerse ScienceDirect

European Journal of Operational Research

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

Decision Support

Revisiting a game theoretic framework for the robust railway network design against intentional attacks

Federico Perea [a,*], Justo Puerto [b]

[a] Departamento de Estadística e Investigación Operativa Aplicadas y Calidad, Universitat Politècnica de València, Camino de Vera sn., 46022 Valencia, Spain
[b] Instituto de Matemáticas de la Universidad de Sevilla (IMUS), Calle Tarfia sn., 41012 Sevilla, Spain

ARTICLE INFO

Article history:
Received 8 April 2012
Accepted 10 November 2012
Available online 27 November 2012

Keywords:
Robust network design
Game theory
Protection resource allocation
Equilibrium

ABSTRACT

This paper discusses and extends some competitive aspects of the games proposed in an earlier work, where a robust railway network design problem was proposed as a non-cooperative zero-sum game in normal form between a designer/operator and an attacker. Due to the importance of the order of play and the information available to the players at the moment of their decisions, we here extend those previous models by proposing a formulation of this situation as a dynamic game. Besides, we propose a new mathematical programming model that optimizes both the network design and the allocation of security resources over the network. The paper also proposes a model to distribute security resources over an already existing railway network in order to minimize the negative effects of an intentional attack. For the sake of readability, all concepts are introduced with the help of an illustrative example.

1. Introduction

Terrorist attacks have often targeted collective transportation networks, specially railways. Examples of such attacks are numerous: 1995 Paris attack, 2004 Madrid train bombings, 2005 London bombings, 2010 Moscow metro bombings, to mention only a few. This is one of the reasons why the operators of these transportation modes should:

- Try to design a network that efficiently works in case one of its components fails (the so-called *robustness* of the network), which is addressed in the network design phase. In this paper we will consider that such failures are caused by intentional attacks.
- Once the network is built, distribute the available security resources so that the damage caused by potential attacks is minimized.

The robustness analysis of transportation networks has been widely analyzed in the literature from different points of view. For instance, Laporte et al. (2011) consider that a railway network is robust when passengers have several options to reach their destination. Atamturk and Zhang (2007) and Ukkusuri et al. (2007) consider robustness of a transportation network with respect to uncertainty in the origin–destination matrix.

The relationship between game theory and robust transportation network design has attracted lots of attention. A game is a decision process in which several agents (called *players*) with possibly conflicting objectives converge. At the end of the process each player receives a *payoff*, which may be affected by the decision of other players. Roughly speaking, games can be divided into two main branches: cooperative games, in which players are allowed to enforce cooperative behavior; and noncooperative games, in which players compete and no cooperation between them is allowed. The reader may consult Forgö et al. (1999) or Owen (1995) for a complete introduction to game theory. The models presented in this paper follow a competitive scheme.

A non-cooperative game can be defined as follows: assume there are n players, and let S_i be the set of possible strategies (decisions) available for player i, $i = 1,\ldots,n$. Let $(s_1,\ldots,s_n)$ be a combination of strategies of the n players, where $s_i \in S_i$ is the strategy chosen by player i. Let u_i: $S_1 \times \cdots \times S_n$ be the payoff function of player i, and therefore let $u_i(s_1,\ldots,s_n)$ be the payoff received by player i if players act according to the strategies $(s_1,\ldots,s_n)$. This game can be represented as:

$$G = \{S_1,\ldots,S_n;\ u_1,\ldots,u_n\}.$$

Game theory has already been applied to model problems in transportation (the reader is referred to Hollander and Prashker (2006) for a review of such applications). In a more recent paper, Lownes et al. (2011) presents an iterative process for measuring network vulnerability to edge disruptions in a game between a router (who aims at minimizing travel costs) and a network tester (who aims at maximizing travel costs by disabling network links).

* Corresponding author. Tel.: +34 654111231; fax: +34 963877499.
E-mail addresses: perea@eio.upv.es (F. Perea), puerto@us.es (J. Puerto).

0377-2217/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ejor.2012.11.015

Game theory has also been used to model and design defensive strategies against intentional attacks in different settings. In Bier et al. (2007) a sequential situation in which one attacker can attack one of two locations protected by one defender is modeled. They discuss on whether it is better to let the attacker know your defense plans or not and they prove that, in equilibrium, it might be optimal for the defender to leave locations unprotected. Bier et al. (2008) discusses how to allocate a limited budget in order to defend multiple potential targets (cities) and how such optimal allocation depends on: cost effectiveness of security investments, how the defender values the potential targets and how certain the attacker's target valuation is. Golany et al. (2009) distinguishes between probabilistic defense, which aims at fighting chance, and strategic defense, which aims at fighting intentional attacks. The authors prove that, under probabilistic threats, one should invest security resources on priority sites, whereas under intentional threats one should focus on decreasing the potential damage in the most vulnerable sites. More recently, Bakir (2011) analyzes the problem of allocating security resources to defend from an attacker the trajectory of cargo containers and models this situation as a Stackelberg game. The author arrives at a similar conclusion as this paper does: in equilibrium the defender should keep a level of security at each site so that the expected damage is constant.

Our problem shares some features with the interdiction problem as introduced in Wood (1993), in which the aim is to attack arcs on a capacitated network so that the maximum flow from a source s to a sink t is minimized. Another interdiction problem is proposed in Scaparra and Church (2008), in which protection resource allocation is tackled so that the effects of intentional attacks on a system of facilities are minimized. More recently, Cappanera and Scaparra (2011) consider networks subject to external disruptions in some of their components that may cause traffic flow delays and propose an allocation of resources that protect the shortest path between a supply node and a demand node in such a way that hits on protected components have no effect. Their trilevel defender-attacker-user model is reduced to a bilevel model.

As opposed to the network interdiction problem, in our models the operator aims to maintain the efficiency of the network as much as possible. The efficiency is here measured as the number of potential travelers that find such network more attractive than the already existing competing transportation network.

Although the railway network design problem in this paper is based on Laporte et al. (2010), which in turn is based on Laporte et al. (2011), two main new contributions from a methodological point of view can be underlined: the application of dynamic game theory to the problem introduced in Laporte et al. (2010), and the modeling of a new security resource distribution problem over a railway network as a Stackelberg game.

The rest of the paper is structured as follows. Section 2 is devoted to introducing some previous concepts and models. Section 3 studies the problem of designing a railway transportation network that is robust against an intentional attack assuming that the situation is dynamic (the attacker is allowed to iteratively place as many bombs as he/she wants) and the only strategy of the designer is the choice of the network to be built. In Section 4, we assume that the designer can also choose where to locate a certain amount of security resources over the network. In Section 5, we consider that the network is already built. In this case the competition takes place between the attacker, who wants to cause as much damage as possible, and the operator, who can decide where to set security resources over the network. The paper closes with conclusions and some pointers at future research.

2. Preliminaries

We consider the same railway network design (RND) problem as in Laporte et al. (2010), which can be summarized as follows. Over a geographical area, where there already exists a transportation mode (for instance a bus), a railway system is to be designed or enlarged, with the following input data:

- A set $N = \{1,2,\ldots,n\}$ of nodes representing potential sites for stations is given.
- A set $E \subseteq \{(i,j): i,j \in N, i<j\}$ of m feasible edges linking the elements of N is known.
- Every feasible edge $(i,j) \in E$ has an associated length d_{ij}, which can be interpreted as the necessary time to traverse the link joining stations i and j.
- c_i is the cost of building a station at node i, $i \in N$, c_{ij} is the cost of building link $(i,j) \in E$. The available budget is limited by $C_{\max}$.
- The mobility pattern is given by a matrix $G = (g_{pq})$: $(p,q) \in W$, where W is the ordered index pair set: $W = \{(p,q): (p,q) \in N\}$, also referred to as the set of demands. Therefore, g_{pq} is the expected number of travelers from station p to station q.
- The generalized cost of satisfying each demand (p,q) by the complementary mode is v_{pq}. In this application v_{pq} is the time to reach station q from station p using the competing transportation mode.

Example 1. As an example of our RND problem consider the network depicted in Fig. 1. The network maximizing trip coverage in this example is the one consisting of the following three lines:

$$L_1 = (1,2,3,5,6,7), \quad L_2 = (4,6,7), \quad L_3 = (6,8).$$

Each line is represented by its sorted set of stations. For instance, L_2 starts at node 4, continues to node 6, and ends at node 7. All lines run both ways. The trip coverage of a network is calculated as the number of travelers for whom using the railway network is faster than using the alternative transportation mode. This problem is proposed and solved in Laporte et al. (2010).

Our goal is to choose a subset of edges satisfying the budget constraints, so that a certain objective function is optimized. Examples of such objective functions are trip coverage (to be maximized) or total traveling time (to be minimized). Therefore, our RND problem reduces to

$$\max_{r \in R} K(r) \quad \text{or} \quad \min_{r \in R} K(r),$$

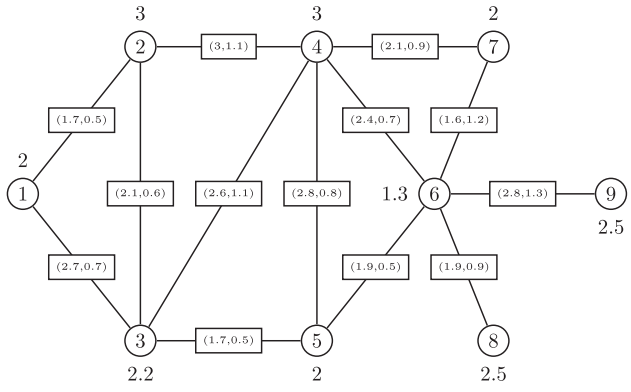

Fig. 1. Test network. Over each edge we have two numbers: the first one is the necessary cost to build the corresponding edge, the second one is the necessary time to traverse it using the railway. By each node we have the construction cost of the corresponding station. The origin destination (O/D) demands g_{pq} and their travel times via the alternative mode v_{pq} for each demand pair $(p,q) \in W$ are given by matrices G and V, see Appendix A.