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)
perea@eio.upv.es
[b]*Instituto de Matemáticas de la Universidad de Sevilla*
Calle Tarfia sn. 41012, Sevilla (Spain)
puerto@us.es

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.

Key words: Robust Network Design, Game Theory, Protection resource allocation, Equilibrium.

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 provoked 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, $i = 1, ..., n$. 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 $u_i : S_1 \times ... \times S_n$ 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

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

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).

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 Figure 1. The network maximizing trip coverage in this example is the one consisting of the following three lines:*

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

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).

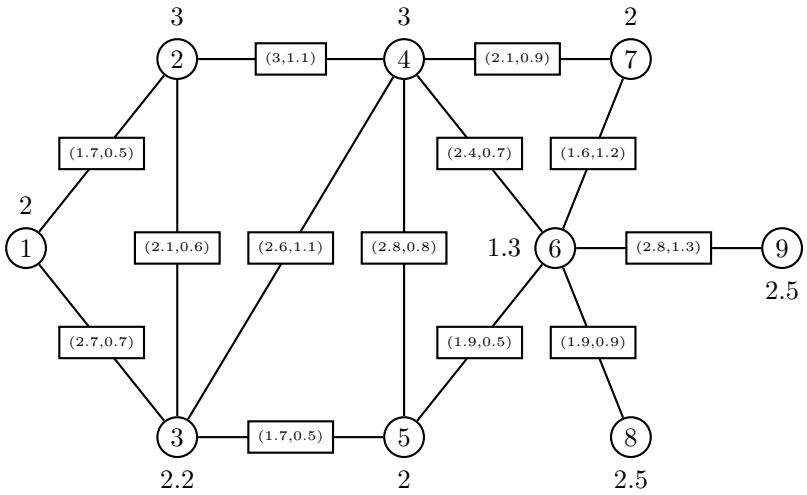

Figure 1: Test network. Over each edge we have two numbers: the first one is the necessary cost to build the corresponding edge, the second one is the necessary time to traverse it using the railway. By each node we have the construction cost of the corresponding station. The origin destination (O/D) 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 the Appendix.

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

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

where R is the set of feasible railway networks and $K(r)$ is the objective function value attained by network $r \in R$.

Unfortunately, not everything always works as planned and therefore the robustness of the network must be taken into account. In this paper we consider possible failures in the normal functioning of the transportation network links. Let $K(r, e)$ be the objective function value of network r if edge e fails ($K(r)$ denotes the value of network r assuming no failures have occurred). Note that $K(r, e) = K(r)$ for all $e \notin r$. In the rest of the paper we will assume that K is a function to be maximized by the operator, like the trip coverage of the network. The reader may note that the minimization case can be studied analogously. The new objective could be:

1. to maximize (over all possible networks) the worst trip coverage of the network when one edge unexpectedly fails

$$\max_{r \in R} \min_{e \in E} K(r, e),$$

   (robustness against intentional attacks).

2. to maximize the expected trip coverage,

$$\max_{r \in R} \{(1 - \sum_{e \in E} \delta_e) K(r) + \sum_{e \in E} \delta_e K(r, e)\},$$

   where δ_e is the probability that edge e randomly fails, which is known, (robustness against random failures).

The (possibly different) solutions to these problems are railway networks expressed as a set of railway lines. These networks can be calculated by solving mixed integer linear programming problems of relatively large size, as shown in Laporte et al. (2010). In this direction, we note that the effects that removing edges can provoke in flows are not easily predicted. The same can happen when removing vertexes, as examined in Martonosi et al. (2011). They identify key vertexes and analyze the flow passing through them as a way to study network disruptions.

2.1. RRND as a game in normal form

In the last section of Laporte et al. (2010) the robust network design problem against intentional attacks was modeled as a noncooperative two-person zero-sum game in normal form, where:

1. Players: $N = \{OPERATOR(PlayerI), ATTACKER(PlayerII)\}$.
2. Strategies: $S_{OPERATOR} = R$, $S_{ATTACKER} = E$.
3. Payoffs: $v_{OPERATOR}(r, e) = K(r, e)$, $v_{ATTACKER} = -K(r, e)$.

We note that the number of strategies for the operator can be enormous. In order to reduce such strategy set, we only consider feasible networks whose trip coverage, in case no failures occur, is greater than or equal to a minimum required value. This truncation is realistic because the network to be designed should, not only be robust, but also (near)optimal in case everything works fine. Consider the following example.

Example 2 *Using the same input data as in Example 1, let us assume that the minimum acceptable trip coverage is 790. In Table 1, the six best networks in terms of trip coverage are shown. In order to calculate such networks, we first calculate* r_1 *by solving the deterministic RND problem, see Appendix A in Laporte et al. (2010). Network* r_{k+1} *is calculated by solving the same problem imposing that* $r_1, ..., r_k$ *are not feasible. Although these problem have been mathematically termed NP-hard, see Appendix B in Laporte et al. (2010), for this instance they are calculated in seconds. These computations, as well as those in the rest of the paper, were done in GAMS 23, using CPLEX 11.2.1. The computer used has 3GB of RAM memory, and a 2.4 GHz processor. The sixth network is dismissed because its trip coverage is lower than the given threshold. Therefore the operator only has 5 feasible strategies. In principle, the attacker can choose any of the 13 potential edges.*

A saddle point is a strategy (r^*, e^*) that satisfies

$$K(r^*, e^*) = \max_{r \in R} \min_{e \in E} K(r, e) = \min_{e \in E} \max_{r \in R} K(r, e)\,, \tag{1}$$

Network	Lines	Trip coverage	Time (seconds)
r_1	(1,2,3,5,6,7), (4,6,9), (6,8)	831	14
r_2	(2,1,3,5,6,8), (7,4,6,9)	825	25
r_3	(1,2,3,5,64,8), (7,4,6,9)	795	39
r_4	(1,3,4,7,6,8), (3,5,6,9)	792	42
r_5	(1,3,4,6,8), (2,3,5,6,7)	791	43
r_6	(1,3,2),(4,3,5,6,8), (6,9)	783	50

Table 1: Optimal networks in terms of trip coverage. For instance, network r_1 gives the highest trip coverage (831). This network is divided into three lines, whose stations are given within the parentheses in a sorted way.

and (r^*, e^*) is a Nash equilibrium strategy, which means that no player can benefit by changing its strategy unilaterally.

If no saddle point exists (which is our case) it is possible for players to enlarge the available set of strategies by considering probability vectors, and look for a saddle point in the enlarged game, in which players can choose a convex combination of their pure strategies, thus defining a *mixed strategy*.

Example 3 *Continuing with the same example, Table 2 gives the trip coverage of each network when each of the potential edges fails. That is, the payoff of player I. Player II's payoffs are the opposite. This table has been populated by solving the robust railway network design problem, see Laporte et al. (2010), imposing that the corresponding network r_k has to be built. Again, although this problem is NP-hard, for instances of this size the calculation can be done in seconds, as shown in the last row of the table. The MaxMin strategy (the security level for player I) is to build network r_5, since this way the operator ensures 588 (the minimum is attained when attacking edge $(1,3)$). The MinMax strategy (the security level for the attacker) is to attack edge $(6,8)$, since this way he ensures that the trip coverage of the network will not be larger than 615. This maximum is attained with network r_2. Since MaxMin $\neq$ MinMax, no saddle point exists in pure strategies. In behavioral (mixed) strategies, a saddle-point strategy is given*

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	
	(1,2)	(1,3)	(2,3)	(3,4)	(3,5)	(4,6)	(4,7)	(5,6)	(6,7)	(6,8)	(6,9)	Time
r_1	723	831	629	831	569	657	831	490	674	588	647	78
r_2	729	596	825	825	548	615	709	461	825	**615**	641	43
r_3	687	795	596	795	536	585	679	457	795	585	611	54
r_4	792	599	792	680	577	792	759	579	735	565	625	95
r_5	791	**588**	665	712	670	711	791	655	639	589	791	26

Table 2: Payoffs of player I: trip coverage of network r_i when edge e_j fails. The MaxMin and MinMax strategies appear in bold face type. Last column shows computational times (in seconds) needed to calculate such $K(r_i, e_j)$ values.

if player I builds r_1 with probability 0.025, r_2 with probability 0.281 and r_5 with probability 0.694, and player II attacks edge e_2 with probability 0.079, edge e_{10} with probability 0.112 and edge e_{12} with probability 0.809. All this results in an expected trip coverage of 596.293 (better than MaxMin for player I).

A normal form (as before) may not provide the full picture of the decision process, since the order in which players act may be important, as well as the information they have available at each moment. The *extensive form* of the two-person zero-sum game explicitly displays the dynamic character of the decision problem. In our robust transportation decision process, player I first designs the network and player II later attacks. In the next section the game will be represented in extensive form. We shall see that such representation gives a more realistic picture of the situation.

3. Robust design as a dynamic game

Let $r_1, ..., r_n$ be the set of possible networks (strategies) for player I, let $e_1, ..., e_m$ be the set of possible edges (strategies) for player II. Denote by $K_{ij} = K(r_i, e_j)$, $i = 1, ..., n, j = 1, ..., m$. Remember that, if $e_j \notin r_i$, then $K(r_i, e_j) = K(r_i)$. We note as well that we are assuming that the attacker values the

effect of his/her attacks in a deterministic way. This assumption has been weakened in the literature. For instance, Nikoofal and Zhuang (2012) allocates defensive budgets assuming that the attacker's valuation of targets is unknown but belongs to bounded intervals. Therefore, for player I there are n possible actions (strategies), $\gamma_1 = r_i,\ i = 1, ..., n$. For player II, however, because he observes the action of player I before deciding his action, there exist m^n possible strategies. One such strategy is, for instance, $\gamma_2(r_i) = e_1$, for all $i = 1, ..., n$, which means to attack edge e_1 no matter which network is built. Another strategy could be $\gamma_2(r_i) = e_1$ if i is even and $\gamma_2(r_i) = e_2$ otherwise. In Figure 2, a representation of a one-stage game with its information sets is shown.

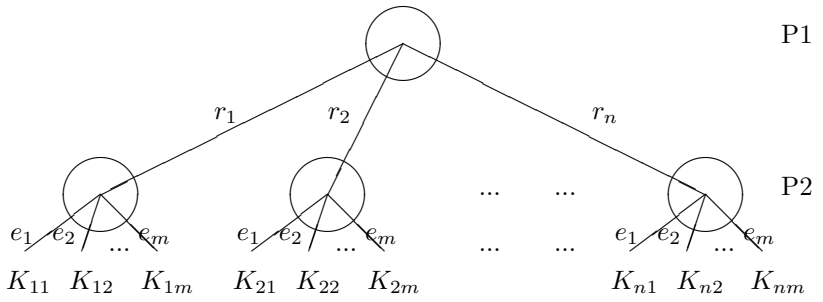

Figure 2: Our example game as a single-act game in extensive form

If we denote by $J(\gamma_1, \gamma_2)$ the payoff of player I when player I and player II employ the strategies γ_1 and γ_2, respectively, we say that $\{\gamma_1^*, \gamma_2^*\}$ is in saddle-point equilibrium if

$$J(\gamma_1, \gamma_2^*) \leq J(\gamma_1^*, \gamma_2^*) \leq J(\gamma_1^*, \gamma_2),$$

and $J^* = J(\gamma_1^*, \gamma_2^*)$ is known as the saddle-point value of the game.

One way to find a saddle point of the game in extensive form consists of first transforming the game into one in normal form, to then find a saddle-point strategy. Unfortunately, this may lead us to an enormous matrix game (in our case, an $n \times m^n$ matrix). Instead, the method for obtaining a pure strategy

saddle-point of single-act zero-sum games in extensive form in Basar and Olsder (1999) will be adapted, resulting in the following procedure.

Proposition 1 *For the previously defined dynamic game, the following procedure provides a saddle-point equilibrium. Such equilibrium coincides with the MaxMin strategy for the operator.*

1. *For each feasible network* r_i*, let* j_i *such that* $K_{i,j_i} = \min_j K_{ij}$.
2. *Let* i^* *such that* $K_{i^*,j_{i^*}} = \max_i K_{i,j_i}$.
3. $\gamma_1^* = r_{i^*}$ *is the saddle-point strategy of player I (the network operator).*
4. $\gamma_2^*(r_i) = e_{j_{i^*}}$ *is the saddle-point strategy of player II (the attacker).*

$\{\gamma_1^*, \gamma_2^*\}$ *is the saddle-point strategy of the game, leading to the actions* $u^1 = r_{i^*}, u^2 = e_{j_{i^*}}$. *The value of the game is* $K(r_{i^*}, e_{j_{i^*}})$.

Proof. The process leads to a saddle-point equilibrium because it is a mere adaptation of that in Basar and Olsder (1999). Note that $K(r_{i^*}, e_{j_{i^*}}) = \max_i K(r_i, e_{j_i}) = \max_i \min_j K(r_i, e_j)$, which is the MaxMin strategy defined before (security level for player I). □

Remark 1 *A more realistic picture could be modeled by allowing that, once the network is built, the attacker can place bombs more than once. Zero-sum games in which at least one player is allowed to act more than once, and with possibly different information sets at each level of play, are known as* multi-act zero-sum games. *Within this class, our game belongs to the subclass of* feedback games, *which satisfy:*

1. *at the time of his action, each player has perfect information concerning the current level of play.*
2. *information sets of the first-acting player (what he knows about the situation of the game at each moment) at every level of play are singletons, and the information sets of the second-acting player at every level of play are such that none of them include nodes corresponding to branches emanating from two or more different information sets of the other player.*

Note that the designer/operator cannot redesign the network at will, because designing and building a railway network is too expensive. Therefore his strategies must be the same at every stage of the game.

There is a recursive procedure to determine the saddle-point strategies of a feedback game, see Basar and Olsder (1999). It is easy to see that this procedure leads to player I choosing network r_{i^*} and player II attacking edge e_{i^*} at each stage of the game. Note that in the multi-stage representation of our game, saddle-point strategies are merely a repetition of the minmax strategies calculated for the former one-stage game. In any case, both approaches represent an advance over the normal form representation where most of the times we have to resort to mixed strategies to represent equilibria. Such mixed strategies are very hard to implement and to explain to designers/managers.

4. A joint model for network design and security resource allocation

In this section we propose a more general game in which player I, the operator, can distribute a certain number of security guards $X \in \mathbb{Z}_+$ over the edges. Then, the set of strategies of player I is defined as (r_i, x), where r_i is the network to be built and $x \in \mathbb{Z}_+^m$ is the distribution of security guards, where x_j is the number of guards assigned to edge e_j, satisfying that $\sum_{j=1}^m x_j \leq X$. We will assume that the probability for an attack made by player II over a certain edge to be successful is a decreasing function on the number of guards located on that edge. Therefore, let $\mathcal{K}((r_i, x), e_j)$ be the expected trip coverage of network r_i when edge e_j is attacked and player I distributes its security resources according to x.

As we have justified in the previous section, if player II has perfect information about the strategy followed by player I (which network has been built and which is the security distribution along the edges) before an attack, the best player I can do is to build its security level strategy, which consists of finding a network $\bar{r}$ and a security guard vector $\bar{x}$ such that

$$\max_{(r_i,x)} \min_{e_j} \mathcal{K}((r_i,x),e_j) = \min_{e_j} \mathcal{K}((\bar{r},\bar{x}),e_j).$$

This problem can be modeled as:

$$\begin{array}{ll} \max & z_{min} + \alpha \sum_{i=1}^{n} z_i + \beta \sum_{i=1}^{n} \sum_{j=1}^{m} \mathcal{K}((r_i,x_i),e_j) \\ \text{s.t.:} & \mathcal{K}((r_i,x_i),e_j) \geq z_i,\ i=1,...,n \\ & z_{min} \leq z_i,\ i=1,...,n \\ & \sum_{j=1}^{m} x_{ij} \leq X,\ i=1,...,n \\ & x_{ij} \in \mathbb{Z}_+,\ i=1,...,n; j=1,...,m \end{array} \tag{2}$$

where x_{ij} is the number of guards to be located on edge e_j if r_i is built, z_i is the minimum trip coverage of network r_i when one of the edges fails, and z_{min} is the minimum z_i.

Note the second term in the objective function, which makes the maximization of the average minimum trip coverage of a network when edges are attacked a second objective, and the third term, which makes the average security a third objective. Therefore α and β are small positive numbers with $\alpha \gg \beta$.

Remark

An instance of $\mathcal{K}((r_i,x_i),e_j)$ could be the following. Assume that, if no guards are located on an edge, then the probability of an attack on such edge to be successful is 1, whereas if there are u_j guards the probability of success is 0. Assuming that having a number of guards between 0 and u_j decreases the probability of success linearly, we end up with:

$$\mathcal{K}((r_i,x),e_j) = \begin{cases} K(r_i,e_j) & \text{if } x_{ij}=0 \\ K(r_i,e_j) + \frac{x_{ij}}{u_j}(K(r_i) - K(r_i,e_j)) & \text{if } 0 < x_{ij} < u_j \\ K(r_i) & \text{if } x_{ij} \geq u_j. \end{cases}$$

Therefore, problem (2) can be written as a mixed integer linear programming problem as follows:

x	(1,2)	(1,3)	(2,3)	(3,4)	(3,5)	(4,6)	(4,7)	(5,6)	(6,7)	(6,8)	(6,9)
r_1	3	0	7	0	8	6	0	8	5	7	6
r_2	3	7	0	0	8	7	4	8	0	7	6
r_3	3	0	7	0	8	7	4	8	0	7	6
r_4	0	8	0	6	8	0	0	8	3	9	8
r_5	0	8	6	4	6	4	0	7	7	8	0

Table 3: Optimal values of variables x_{ij}.

$$
\begin{aligned}
\max \quad & z_{min} + \alpha \textstyle\sum_{i=1}^{n} z_i + \beta \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{x_{ij}}{u_j} (K(r_i) - K(r_i, e_j)) \\
\\
\text{s.t.:} \quad & K(r_i, e_j) + \tfrac{x_{ij}}{u_j}(K(r_i) - K(r_i, e_j)) \geq z_i, \ i = 1, ..., n \\
& z_{min} \leq z_i, \ i = 1, ..., n \\
& \textstyle\sum_{j=1}^{m} x_{ij} \leq X, \ i = 1, ..., n \\
& x_{ij} \leq u_j, \ i = 1, ..., n; j = 1, ..., m \\
& x_{ij} \in \mathbb{Z}_+, \ i = 1, ..., n; j = 1, ..., m
\end{aligned}
\tag{3}
$$

Example 4 *As an example of this situation, consider the same network as before, and assume that for any of the links, having 10 security guards guarantees total security and, therefore, no attack is to be successful. Consider as well that the number of guards available is* $X = 50$*. With this data, a solution to Problem (3) taking* $\alpha = 10^{-4}$ *and* $\beta = 10^{-7}$ *is given in Table 3, whereas the expected trip coverage of each network when each of the feasible links is attacked and guards are distributed according to Table 3 is shown in Table 4. We note that both tables are obtained from the solution to problem (3), which is solved in around 0.2 seconds. Note as well that for solving this problem one needs the data given in tables 1 and 2.*

The minimum expected coverage for each potential network when one of the edges fails is: $z_1 = 752.5, \ z_2 = 751.4, \ z_3 = 719.4, \ z_4 = 747.2, \ z_5 = 740.6$*, and therefore the security strategy for player I is to build network* r_1 *with the secu-*

$\mathcal{K}$	(1,2)	(1,3)	(2,3)	(3,4)	(3,5)	(4,6)	(4,7)	(5,6)	(6,7)	(6,8)	(6,9)
r_1	755.4	831.0	770.4	831.0	778.6	761.4	831.0	762.8	752.5	758.1	757.4
r_2	757.8	756.3	825.0	825.0	769.6	762.0	755.4	752.2	825.0	762.0	751.4
r_3	719.4	795.0	735.3	795.0	743.2	732.0	725.4	727.4	795.0	732.0	721.4
r_4	792.0	753.4	792.0	747.2	749.0	792.0	759.0	749.4	752.1	769.3	758.6
r_5	791.0	750.4	740.6	743.6	742.6	743.0	791.0	750.2	745.4	750.6	791.0

Table 4: Values of expected trip coverage $\mathcal{K}((r_i, x_i), e_j)$ assuming the values of x_i as given in Table 3.

rity distribution showed in Table 3. This way the operator ensures an expected trip coverage of, at least, 752.5 (no matter which edge the attacker decides to attack). Note that in this case the attacker would prefer to attack edge (6,7), since an attack in this edge would produce the highest expected damage in the ridership. Therefore the actions $((r_1, (3, 0, 7, 0, 8, 6, 0, 8, 5, 7, 6)), (6, 7))$ *derive a saddle-point strategy.*

Note again that the optimal strategies for player I are MaxMin strategies, but the corresponding solution network need not be the same as in the games presented in Section 3 (note that these models applied to our example resulted in network r_5 *as the MaxMin strategy for the operator).*

5. A model for security resource allocation

In this section we assume that the operator has already built network r, but still the competition game between the operator and the attacker continues. The operator can now install a security system over the network that is difficult to modify and known by the attacker. Therefore this situation is modeled as a Stackelberg game in which the operator is the leader and the attacker is the follower.

Following the work in Bakir (2011), we now propose a problem in which the attacker wants to locate a bomb so that the maximum damage is caused to the network, and the operator wants to design a security system that allows

interdicting the possible attacks. Let K_j be the cost incurred by the operator if a bomb is successfully detonated on edge e_j, and let $p_j \in [0,1]$ be the probability that a bomb located on edge e_j is interdicted (both parameters are known by the players). The cost to keep this probability is $c(p_j) = \frac{d_j}{(1-p_j)^{\alpha_j}} - d_j$, where $c(p_j)$ can represent, for instance, the investment in a security system to interdict a bomb on edge e_j with probability p_j, and d_j is the length of edge e_j. This cost function, as noted in Bakir (2011) and Bier et al. (2007), has some nice properties ($c(0) = 0, c' > 0, c'' > 0, \lim_{p_j \to 1} c(p_j) = +\infty$). Assuming that the attacker tries to locate a bomb where his expected payoff is maximized, that is, on edge $e_{j'} : j' = \arg\max_j \{(1-p_j)K_j\}$, the defender's objective is to minimize

$$\begin{array}{ll} \min & \sum_{j=1}^{m} c(p_j) + (1-p_{j'})K_{j'} \\ \text{s.t.:} & (1-p_j)K_j \leq (1-p_{j'})K_{j'} \ \forall\ j = 1, ..., m, j \neq j' \\ & p_j \in [0,1]. \end{array} \tag{4}$$

Note that, in order to solve this problem, we first have to find out which edge $e_{j'}$ is. A first idea using brute force would be to solve problem (4) for any possible edge $e_{j'}$, which does not seem to be an appropriate method. The following theorem provides a more suitable way for finding an equilibrium of this game. We will prove that, whenever the costs incurred by the operator when one bomb explodes are sufficiently large (which is a logical assumption) the equilibrium of this game is for the operator to choose its security system so that the expected cost of not interdicting a bomb is constant for every edge.

Theorem 1 *Consider an instance of the Stackelberg game defined in this section. If K_j is sufficiently large for all e_j, the equilibrium is for the operator to choose the interdiction probabilities p_j so that $(1-p_j)K_j$ is constant for all j.*

Proof. Consider the problem in (4). For convenience, define a new variable $z = (1-p_{j'})K_{j'}$. Let us apply the Karush-Kuhn-Tucker (KKT) conditions for this problem, see Bazaraa et al. (1979). The KKT conditions are necessary conditions for optimality. Because the objective function is convex, and the constraints are linear, KKT conditions are also sufficient.

The Lagrangean function of problem (4) is:

$$L(p_1,...,p_m,z,\lambda_1,...,\lambda_m)=\sum_{j=1}^{m}(\frac{d_j}{(1-p_j)^{\alpha_j}}-d_j)+z+\sum_{j=1}^{m}((1-p_j)K_j-z)\lambda_j.$$

The KKT conditions for this case consist of solving the following system of equations:

$$\frac{\partial L}{\partial p_j}=\frac{\alpha_j d_j}{(1-p_j)^{\alpha_j+1}}-K_j\lambda_j=0. \tag{5}$$

$$1-\sum_{j=1}^{m}\lambda_j=0. \tag{6}$$

If $(1-p_j)K_j$ is constant for all e_j, in particular we have that $(1-p_j)K_j = z^* \ \forall \ j=1,...,m$ (or equivalently $p_j = 1-\frac{z^*}{K_j}$). Therefore a solution to the previous system of equations satisfies:

$$\lambda_j^*=\frac{\alpha_j d_j}{K_j(z^*/K_j)^{\alpha_j+1}}, \tag{7}$$

$$\sum_{j=1}^{m}\frac{\alpha_j d_j}{K_j(z^*/K_j)^{\alpha_j+1}}=1, \tag{8}$$

$$p_j^*=1-\frac{z^*}{K_j}. \tag{9}$$

We first see that the value of z^* is well defined. Let $f(z)=\sum_{j=1}^{m}\frac{\alpha_j d_j}{K_j(z/K_j)^{\alpha_j+1}}$. It is easy to see that $\lim_{z\to\infty}f(z)=0,\ \lim_{z\to 0^+}f(z)=+\infty$, and that f is a continuous function in $(0,+\infty)$. Applying Bolzano's theorem we get that there exixts $z^*\in(0,+\infty)$ so that $f(z^*)=1$. For p_j^* to be well defined, we need to impose $0\leq p_j^*<1$ (note that by the definition of the cost function $c(\cdot)$ we have that $p_j\neq 1$), which is guaranteed if $K_j>z^*$ or, as we stated in the hypotheses of the theorem, K_j is sufficiently large for every j.

□

In other words, this theorem says that if the costs provoked by the attack are large enough, then what the operator should do is to balance its expected loss at all edges, so that the maximum damage is minimized. Note as well that if the costs K_j are small enough, not doing anything might be optimal (that is,

make all $p_j = 0$). It goes without saying that the incurred costs for the operator in case we are facing a terrorist attack (K_j) are large enough, and therefore Theorem 1 is valid for these situations. Let us see an example of the application of this result.

Example 5 *Assume the operator has already designed network r_1 as defined in Example 2 and suggested in Example 4, and assume as well that the loss incurred by the operator if a bomb explodes in edge e_j is $K_j = 1000(K(r_1) - K(r_1, e_j)) = 831000 - 1000K(r_1, e_j)$ (the values of $K(r_1, e_j)$ are shown in Table 2.) The choice of d_j and α_j is constant and equal to 1 for every j. As a conclusion to the previous theorem, the reader may note that an optimal solution to problem*

$$\begin{array}{ll} \min & \sum_{j=1}^{m} c(p_j) + z \\ s.t.: & (1 - p_j)K_j \leq z \ \forall \ j = 1, ..., m \\ & p_j \in [0, 1] \end{array} \tag{10}$$

coincides with the solution to Problem 4 for any j', and is:

$$p_1^* = 0.988, p_3^* = 0.994, p_5^* = 0.995, p_6^* = 0.993, p_8^* = 0.996,$$
$$p_9^* = 0.992, p_{10}^* = 0.995, p_{11}^* = 0.993, z^* = 1292.672 = K_j(1 - p_j) \ \forall \ j,$$

with an optimal value of 2577.343. This optimal value is the cost incurred by the operator if the attacker explodes the bomb at any edge plus the cost to keep probabilities p_j^*. The execution time for this non-linear programming problem, using CONOPT with GAMS 23, is around 0.2 seconds.

6. Conclusions

In this paper we have extended some previously introduced models about the competition between a transportation network operator and an attacker. The operator wants to design a network that optimizes certain objective function and the attacker wants to produce as much damage in the network as possible by placing a bomb on one of the network links. This situation is modeled as a

two-player non-cooperative game in which player I is the network operator and player II is the attacker. The strategies for player I are the possible networks to be built and the strategies for player II are the edges that can be attacked.

The first idea expressed here is that the models presented in previous papers miss the dynamic aspects of these situations: the attacker can attack many times. We have proven that, in the dynamic version of the game, the best strategy for the operator is to design a network that optimizes the worst case scenario.

We have also proposed variations of this game, in which the operator can manage the security system in the network. The first model assumes that the strategies for the operator are the possible networks to be built and a distribution of security guards over the network, the strategies for player II remain the same: the set of network edges. We have modeled this situation as a mathematical mixed integer programming problem that, depending on the function that models the probability of success in the attacks of player II, can be linear. An example has shown that the resulting network need not be the same as in the dynamic model presented before, where the only strategies for the operator where which network to build.

The last model introduced in this paper assumes that the network has already been built and that the possible strategies for player I are the investment on a security system: the more you invest in one particular edge, the less likely to be successful an attack on this edge is. This model assumes that the security system cannot be changed easily and, therefore, in the dynamic version of the game player I has to restrict to the same strategy at all the stages. So this situation has been modeled as a Stackelberg game. We have proven that an optimal strategy for the operator is to distribute the security efforts in such a way that the expected cost incurred by the operator does not depend on the attacker's targeted edge.

This research line is still in progress, specially from the algorithmic point of view. The applicability of the models presented to real-sized transportation networks is still an open issue. Calculating the payoff function is an NP-hard

problem. For this reason a first set of heuristics has been proposed in Garcia-Archilla et al. (2011). Note that the application of heuristics would yield an approximation of the payoff function, and the interesting research line of approximated games, in which the characteristic or payoff function is approximated would apply, see Perea (2011). Further research will focus on efficient algorithms that help finding equilibria in the models presented.

Acknowledgments

The research activities of the authors have been supported by the projects FQM-5849 (Junta de Andalucía\FEDER) and MTM2010-19576-C02-01 (MICINN, Spain). Special thanks are due to two anonymous referees for their valuable comments and suggestions.

Appendix: Matrices in example

$$G = \begin{pmatrix} 0 & 9 & 26 & 19 & 13 & 12 & 4 & 6 & 4 \\ 11 & 0 & 14 & 26 & 7 & 18 & 3 & 7 & 9 \\ 30 & 19 & 0 & 30 & 24 & 8 & 3 & 9 & 11 \\ 21 & 9 & 11 & 0 & 22 & 16 & 21 & 18 & 16 \\ 14 & 14 & 8 & 9 & 0 & 20 & 12 & 18 & 9 \\ 26 & 1 & 22 & 24 & 13 & 0 & 11 & 28 & 21 \\ 7 & 5 & 6 & 19 & 15 & 13 & 0 & 16 & 14 \\ 5 & 9 & 11 & 16 & 17 & 25 & 17 & 0 & 21 \\ 6 & 8 & 10 & 18 & 11 & 20 & 14 & 20 & 0 \end{pmatrix};$$

$$V = \begin{pmatrix} 0 & 1.6 & 0.8 & 2 & 1.6 & 2.5 & 4 & 3.6 & 4.6 \\ 2 & 0 & 0.9 & 1.2 & 1.5 & 2.5 & 3.2 & 3.5 & 4.5 \\ 1.5 & 1.4 & 0 & 1.3 & 0.9 & 2 & 3.3 & 2.9 & 3.9 \\ 1.9 & 2 & 1.9 & 0 & 1.8 & 2 & 2 & 3.8 & 4.1 \\ 3 & 1.5 & 2 & 2 & 0 & 1.5 & 3 & 2 & 3 \\ 2.1 & 2.7 & 2.2 & 1 & 1.5 & 0 & 2.5 & 3 & 2.5 \\ 3.9 & 3.9 & 3.9 & 2 & 3 & 2.5 & 0 & 2.5 & 2.5 \\ 5 & 3.5 & 4 & 4 & 2 & 3 & 2.5 & 0 & 2.5 \\ 4.6 & 4.5 & 4 & 3.5 & 3 & 2.5 & 2.5 & 2.5 & 0 \end{pmatrix}.$$

References

Atamturk, A., Zhang, M., 2007. Two-stage robust network flow and design under demand uncertainty. Operations Research 55 (4), 662–673.

Bakir, N. O., 2011. A stackelberg game model for resource allocation in cargo container security. Annals of Operations Research 187, 5–22.

Basar, T., Olsder, G. J., 1999. Dynamic Noncoopoerative Game Theory, 2nd Edition. SIAM's Classics in Applied Mathematics. Academic Press, New York.

Bazaraa, M., Sherali, H., Shetty, C., 1979. Nonlinear Programming, Theory and Applications. John Wiley and Sons.

Bier, V., Oliveros, S., Samuelson, L., 2007. Choosing what to protect: Strategic defensive allocation against an unknown attacker. Journal of Public Economic Theory 9 (4), 563–587.

Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R., Culpen, A. M., 2008. Optimal resource allocation for defense of targets based on differing measures of attractiveness. Risk Analysis 28 (3), 763–770.

Cappanera, P., Scaparra, M. P., 2011. Optimal allocation of protective resources in shortest-path networks. Transportation Science 45 (1), 64–80.

Forgö, F., Szèp, J., Szidarovsky, F., 1999. Introduction to the theory of games. Kluwer academic publisher.

Garcia-Archilla, B., Lozano, A. J., Mesa, J. A., Perea, F., 2011. GRASP algorithms for the robust railway network design problem. Journal of Heuristics Article in press, DOI 10.1007/s10732-011-9185-z.

Golany, B., Kaplan, E. H., Marmur, A., Rothblum, U. G., 2009. Nature plays with dice – terrorists do not: Allocating resources to counter strategic versus probabilistic risks. European Journal of Operational Research 192, 198–2008.

Hollander, Y., Prashker, J., 2006. The applicability of non-cooperative game theory in transport analysis. Transportation 33 (5), 481–496.

Laporte, G., Marín, A., Mesa, J., Perea, F., 2011. Designing robust rapid transit networks with alternative routes. Journal of advanced transportation 45, 54–65.

Laporte, G., Mesa, J., Perea, F., 2010. A game theoretic framework for the robust railway transit network design problem. Transportation Research Part B 44, 447–459.

Lownes, N. E., Wang, Q., Ibrahim, S., Ammar, R. A., Rajasekaran, S., Sharma, D., 2011. Many-to-many game-theoretic approach for the measurement of transportation network vulnerability. Journal of the Transportation Research Board 2263, 1–8.

Martonosi, S.E., Altner, D., Ernst, M., Ferme, E., Langsjoen, K., Lindsay, D., Plott, S., and Ronan, A.S. 2011. A New Framework for Network Disruption CoRR abs/1109.2954: arXiv:1109.2954v1 [cs.SI]

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

Owen, G., 1995. Game Theory. Academic Press.

Perea, F., 2011. Multidimensional assignment: applications and some thoughts. Boletín de Estadística e Investigación Operativa 27 (1), 14–28.

Scaparra, M. P., Church, R. L., 2008. An exact solution approach for the interdiction median problem with fortification. European Journal of Operational Research 189, 76–92.

Ukkusuri, S., Mathew, T., Waller, S., 2007. Robust transportation network design under demand uncertainty. Computer-Aided Civil and Infrastructure Engineering 22 (1), 6–18.

Wood, R., 1993. Deterministic network interdiction. Mathematical and Computer Modeling 17 (2), 1–18.