

Optimizing Investment Decisions for Railway Systems Protection

Maria Paola Scaparra, Stefano Starita and Claudio Sterle

Abstract As demonstrated by recent events, railway systems are often the target of terrorist bombings and attacks. To preserve public safety and essential economic functions, railroad networks should be made as secure and resilient as possible. However, railway protection investments may involve significant and often unaffordable capital expenditure. Given the limited resources available for protection efforts, it is essential that a strategic approach to the planning of security investments is adopted. This chapter presents a mathematical model for identifying the optimal allocation of protective resources among the components of a railway network. The aim is to minimize the impact on passenger flow of worst-case disruptions which might affect both railway stations and tracks. The proposed model is tested on an Italian railroad network to demonstrate how the model results can be used to inform policy making and protection investment decisions.

1 Introduction

In light of numerous recent terrorist attacks to transportation systems, the issue of protecting critical transportation infrastructures has become a necessity. Railways, in particular, have often been the target of terrorist activity. Examples include the 1995 Paris metro bombing, the 2004 Madrid train bombing, the 2005 London underground suicide attacks, and the 2010 Moscow bombing. These events have demonstrated that rail systems are a crucial yet sensitive component of a nation's

M.P. Scaparra (✉) · S. Starita
University of Kent, Canterbury Kent CT2 7PE, UK
e-mail: M.P.Scaparra@kent.ac.uk

S. Starita
e-mail: ss882@kent.ac.uk

C. Sterle
University of Naples Federico II, Naples, Italy
e-mail: claudio.sterle@unina.it

infrastructure and that disruptions in railroad services can have a significant adverse impact not only on the economy but also on public health and safety.

In some countries like the US, the rail industry and the government have undertaken extensive efforts to protect the movement of freight and passenger trains. Nevertheless, rail security remains an exercise in risk mitigation, as opposed to risk prevention, and protection efforts are mostly undermanned and underfunded [1]. Undoubtedly, railway protection presents some inherent difficulties, due to the specific characteristics of rail systems. First of all, railways are geographically extensive, open and easily accessible infrastructures. As an example, the Italian railroad comprises 16,741 km of operational rail lines, and 2,260 passenger stations. Strengthening all these assets to targeted safety levels may require unacceptable expenditures. In addition, effective security improvements specific to rail transport are difficult to identify and implement. Security mechanisms used by other transportation modes (e.g., aviation passenger screening) cannot be readily applied in the rail environment. Given these difficulties, it is key that protection expenditures are invested wisely in a manner that optimises both service efficiency and public safety.

Railway security can be improved by optimizing the allocation of protection devices within a single asset (e.g., security cameras in a station) but also through a cost efficient allocation of protective resources across the entire railway network. This involves identifying the most critical network components whose loss or temporary closure might have the greatest impact on daily service provision and allocating protection resources among these components so as to make the overall system as robust as possible to external disruptions.

Several quantitative models and analytical approaches have been developed in recent years to identify critical components of and sound protection strategies for distribution and transportation networks. These can be broadly categorized into protection models to counter probabilistic risks and models to counter strategic or premeditated risks [2]. Probabilistic models deal with protection investments against random disruptions (e.g., accidental failures or natural hazards) and imply that the probability of failure of single assets is known or can be estimated, for example through the analysis of historical data or by using domain-specific information provided by structural engineers. Protection models for strategic risks consider protection investments to minimize the impact of worst-case scenario disruptions. These are suitable to model man-made or intentional disruptions (e.g., terrorist attacks or labour union strikes). However, they can be applied to natural disasters as well, if the aim is to protect the system against worst-case scenario losses or if failure probabilities cannot be easily obtained or accurately estimated.

Modeling strategic disruption risks requires emulating the *game* played between a network *attacker* (or *interdictor*) and a network *defender*. Game theory has, therefore, been widely used to model and design defensive strategies against malicious attack. Defender-attacker games can be expressed mathematically as bilevel optimization models where the upper level problem of optimally allocating protection resources has embedded within it a lower-level problem which endogenously generates worst-case scenario losses [3–5].

This chapter considers a bilevel optimization model to deal with security resource allocation in railway systems. We model the rail system as a network of nodes and links, where the nodes represent the stations and the links are the track segments. A limited budget is available for increasing the system security through the protection of nodes and or links. Different security measures can be employed, depending upon the asset to be protected. For example, a link containing a bridge or a tunnel can be protected through monitoring devices or structural reinforcement. A station can be protected by increasing surveillance and patrolling, or installing security cameras. Obviously, different costs are incurred for protecting different components (e.g., protecting a high-traffic commuter station requires significantly more protective resources than protecting a small station or a secondary rail track). Costs also depend on the type of security measure adopted. We assume that a protected component becomes completely invulnerable to possible disruptions. Likewise, if a failure occurs, the affected component becomes completely inoperable and unable to provide service. The aim of the model is to identify a cost-efficient allocation of the available budget so as to minimize the impact of worst-case scenario disruptions to the system. We focus, in particular, on passenger traffic and measure the disruption impact in terms of lost customer flow or demand. More specifically, we assume that if a node or a link fails, traffic must be rerouted through alternative paths on the network. However, detour routes may not exist or be too long from a user point of view. In this case, passengers may resort to different transport modes or abandon the trip all together. The amount of customer flow which is lost provides an indication of the disruption extent. To evaluate the worst-case amount of disrupted flow, we use an adaptation of the flow interdiction model proposed by Murray et al. [6]. A common assumption in interdiction modeling is that there is a limit to the number of components that can be lost simultaneously. Without loss of generality, we also assume that interdiction resources are limited and that the amount of resources needed to disable a component varies according to the component size and topology.

2 Background

The use of network optimization models as a tool for identifying the most vital components of a network dates back several decades (see, for example, the seminal works by [7–9]). Many optimization models, also known as *interdiction* models, have been developed throughout the years to assess the importance and criticality of network components in different settings [10, 11]. These models identify the network links or nodes that, if lost or damaged, have the worst-case impact on system performance. System performance can be measured in a variety of ways, depending upon the topology of the system, the operational protocol in use, and the type of service provided. Typical system performance measures include travel time, connectivity, average throughput or flow, transportation cost, demand coverage, and recovery times among others.

Interdiction models are a useful tool for assessing facility importance and several authors have suggested using the outcome of interdiction models to prioritize protection and or recovery investment efforts [12–14]. However, it can be easily demonstrated that securing those assets that are identified as critical in an optimal interdiction solution does not necessarily provide the greatest protection against malicious attacks [15]. Protection decisions must, therefore, be explicitly captured within a modeling framework to guarantee that security investments are optimized. Optimization models which incorporate protection decisions embed interdiction models to evaluate the worst-case scenario loss in response to each protection strategy.

Most of the protection models existing in the literature have been developed for allocating protection resources among service and supply facilities (e.g., warehouses, distribution centers and power plants) within distribution type networks [5, 16, 17]. Within the transportation literature, only a few papers have addressed the problem of optimizing protection investments among systems components and most of them have dealt with stochastic models to hedge against random disruptions rather than intentional attacks. As an example, Liu et al. [18] propose a stochastic optimization model for allocating limited retrofit resources over multiple highway bridges to improve the reliability of transportation networks. The benefit of retrofit is quantified as savings in reconstruction and travel delay costs. Fan and Liu [19] present a two-stage stochastic model for distributing security resources among road segments so as to minimize total physical and social losses caused by random disasters. Peeta et al. [20] optimize investment decisions for strengthening a highway network. They assume that the network links are subject to random failures due to earthquakes and protection investments reduce failure likelihood. The objective is to maximize the post-disaster connectivity for first responders and minimize the travel time in the surviving network. Miller-Hooks et al. [21] analyze the optimal investment allocation of a fixed budget between preparedness activities (e.g., protection) and recovery activities. They focus on intermodal freight transport networks and measure network resilience as the expected fraction of demand that can be satisfied post-disaster.

To the best of the authors knowledge, the only defender-attacker game-theoretic approach to hedge against intentional disruptions in transportation networks is the one proposed by Cappanera and Scaparra [22]. Their model aims at identifying the set of components to harden in a freight transport network so as to minimize the length of the shortest path between a supply node and a demand node after a worst-case disruption of some unprotected components. Disruption results in traffic delays and network performance is measured in terms of total travel time.

Focusing on protection models specifically designed for railway systems, the literature is even more sparse. Peterson and Church [23] propose a modeling framework for identifying the impact on rail operations when one or more bridges and tunnels are lost. This model is useful for estimating freight rail network vulnerability but does not explicitly identify countermeasures for protection. Perea and Puerto [24] present a model to distribute security resources over a railway network so as to minimize the probability of a successful bombing attack. They provide

some theoretical results on the optimal protection strategy but do not propose an efficient solution technique to make the model applicable to real-size rail networks.

In this chapter, we attempt to redress this shortcoming in the literature by proposing a model which allocates security resources among railway network components while taking into account railroad specific properties and performance measures.

3 The Railway Protection Investment Model

To formulate the railway protection investment problem mathematically, we consider a railway network as composed of a set of nodes N (the stations) and a set of arcs A (the track segments). We assume that the daily traffic flow between any two stations s and t is known and that, in case of disruption, passengers are willing to use alternative railroad routes only if they are not significantly longer than their normal journey time. We call these routes *acceptable paths* and we compute them in a pre-processing phase. This evaluation is done by comparing each alternative path between an origin and a destination node with the shortest path: all the paths whose length exceeds a given threshold are discarded. The threshold is computed by adding a tolerance parameter to the length of the shortest path.

The other model assumptions can be summarized as follows:

- An interdicted element is excluded from the network.
- Both arcs and nodes can be interdicted. This assumption is made to simulate the disruptions of tunnels, bridges and stations at the same time.
- All the arcs directly linked to an interdicted node are interdicted as well.
- A protected element cannot be interdicted.
- A limited amount of interdiction resources is available.

The mathematical model uses the following notation.

Sets and Indices

N	= set of nodes
A	= set of arcs
$s \in N$	= index used for flow sources
$t \in N$	= index used for flow destinations
$i \in N$	= index used for network nodes
$j \in A$	= index used for network arcs
f_{st}	= traffic demand between s and t
N_{st}	= set of acceptable paths that connect s and t
$\beta \in N_{st}$	= index used for network paths
$N(\beta)$	= set of nodes along path β
$A(\beta)$	= set of arcs along path β
q	= protection budget (or amount of resources available to the defender)
p	= amount of resources available to the attacker
q_i^n	= estimate of the amount of resources needed to protect node i

p_i^n = estimate of the amount of resources needed to disrupt node i
 q_j^n = estimate of the amount of resources needed to protect arc j
 p_j^a = estimate of the amount of resources needed to disrupt arc j

Decision variables:

$$X_i^n = \begin{cases} 1 & \text{if node } i \text{ is disabled} \\ 0 & \text{otherwise;} \end{cases}$$

$$X_j^a = \begin{cases} 1 & \text{if arc } j \text{ is disabled} \\ 0 & \text{otherwise;} \end{cases}$$

$$Y_i^n = \begin{cases} 1 & \text{if node } i \text{ is protected} \\ 0 & \text{otherwise;} \end{cases}$$

$$Y_j^a = \begin{cases} 1 & \text{if arc } j \text{ is protected} \\ 0 & \text{otherwise;} \end{cases}$$

$$Z_{st} = \begin{cases} 1 & \text{if the flow between } s \text{ and } t \text{ is lost} \\ 0 & \text{otherwise;} \end{cases}$$

The railway protection investment model can be formulated as the following bilevel problem:

$$\min_{\mathbf{Y}} F(\mathbf{Y}) \quad (1)$$

$$\sum_i q_i^n Y_i^n + \sum_j q_j^a Y_j^a \leq q, \quad (2)$$

$$Y_i^n \in \{0, 1\} \quad \forall i \in N, \quad (3)$$

$$Y_j^a \in \{0, 1\} \quad \forall j \in A, \quad (4)$$

$$\text{where } F(\mathbf{Y}) = \max_{\mathbf{X}} \sum_s \sum_t f_{st} Z_{st}, \quad (5)$$

$$\text{s. t. } \sum_i p_i^n X_i^n + \sum_j p_j^a X_j^a \leq p, \quad (6)$$

$$X_i^n \leq 1 - Y_i^n \quad \forall i \in N, \quad (7)$$

$$X_j^a \leq 1 - Y_j^a \quad \forall j \in A, \quad (8)$$

$$\sum_{i \in N(\beta)} X_i^n + \sum_{j \in A(\beta)} X_j^a \geq Z_{st} \quad \forall s, t, \beta \in N_{st}, \quad (9)$$

$$X_i^n \in \{0, 1\} \quad \forall i \in N, \quad (10)$$

$$X_j^a \in \{0, 1\} \quad \forall j \in A, \quad (11)$$

$$Z_{st} \in \{0, 1\} \quad \forall s, t \in N. \quad (12)$$

In this leader-follower model the leader chooses the optimal strategy to minimize the objective function F (1), that is the amount of flow that cannot be served after the interdiction. Constraint (2) is the budget constraint: the leader can allocate at most q protection resources among the nodes and arcs of the network. Constraints (3) and (4) are the binary restrictions on the protection variables. The lower level program (5–12) is the interdiction model used to evaluate worst-case losses. The aim of the follower is to choose the attack strategy that maximizes the amount of flow disrupted (5). Constraint (6) is the follower resource constraint: the attacker has at most p resources to interdict the nodes and arcs of the network. Constraints (7) state that protected nodes cannot be disrupted. Similarly, constraints (8) state that protected arcs cannot be disrupted. Constraints (9) state that the flow between s and t can be considered disrupted ($Z_{st} = 1$) only if all the acceptable paths between s and t are disrupted, i.e., at least one of their nodes or arcs is interdicted. If there is at least one acceptable path without interdicted components, the value of the variable Z_{st} is forced to be zero. Finally, constraints (10–12) are binary restrictions on the interdiction and path variables.

4 Solution Methodology

Different methodologies have been used in the literature to solve this type of defender-attacker models. These include: reformulation, dualization, and decomposition [25–27]. To solve the bilevel problem (1–12), we used a decomposition method based on super valid inequalities. Namely, the bilevel model is split into two interlinked subproblems: an upper level protection master problem, and a lower level interdiction subproblem. Each protection strategy identified by the master problem is fed into the subproblem to determine an optimal interdiction plan. Special cuts, called super valid inequalities (SVI), are then generated based on the solution to the interdiction problem and added to the master problem, which then computes a new protection strategy. The process is iterated until a sufficient number of SVIs has been added to make the protection problem unfeasible. This approach had been previously used to solve a two-level protection model in Losada et al. [28].

The decomposition algorithm was implemented in C++ inside the Visual Studio environment. At each iteration, both the master problem and the sub-problem were solved using the IBM ILOG optimization software Cplex 12.5.

5 Case Study and Analysis

To demonstrate the practical applicability of our approach, we applied the model to the railway network infrastructure of Campania, a region in Southern Italy. The region Campania is populated by almost 6 million people, making it the second-most-populous region of Italy. Its capital city is Naples. The railway network under consideration is composed by a primary network which connects major cities in Italy and has high traffic (high speed and inter-regional rail services), a secondary network which connects an highly populated urban centre to outer suburbs (Cumana, Circumlfegrea, Circumvesuviana and north-east metro services), and some complementary lines which connect small regional centres. The overall network is depicted in Fig. 1. The network has 26 nodes, corresponding to cities and towns in the region, and 37 arcs.

In the absence of real data on passenger traffic between pairs of stations, we have generated estimates of the origin-destination flows as a function of the size of the connected cities, and the frequency and capacity of the trains operating on the

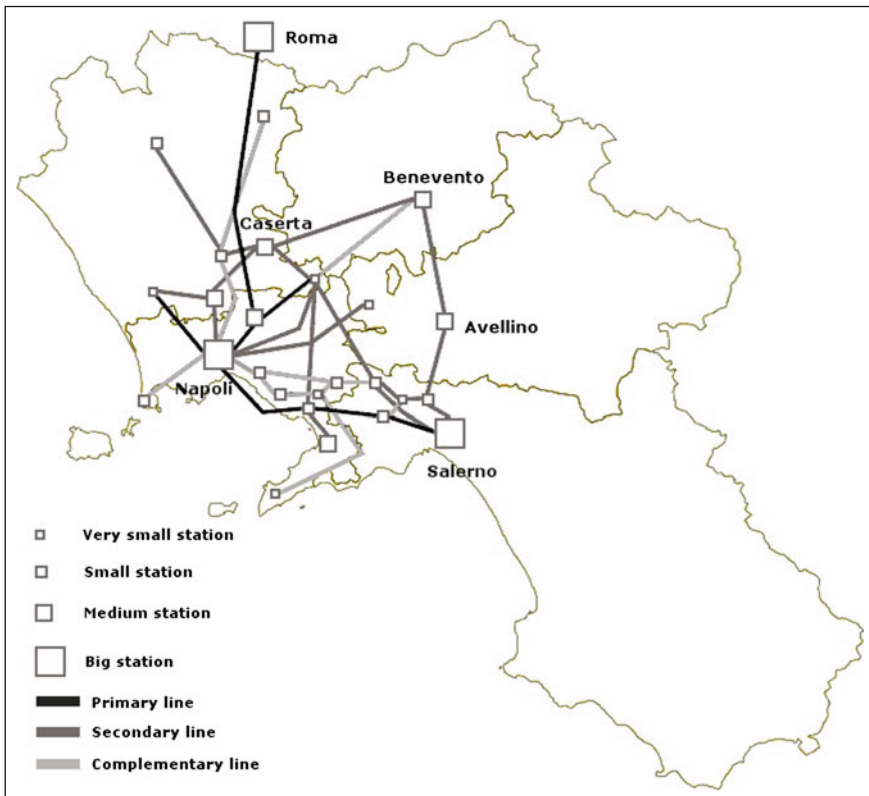


Fig. 1 Campania rail network

network. We assumed that disrupting an arc requires one unit of resource ($p_j^a = 1$), whereas the cost of protecting an arc, q_j^a , depends upon the number of tunnels and bridges along the arc. We do not consider the protection of arcs without tunnels or bridges. To generate realistic values for the interdiction and protection resources associated with the nodes (q_i^n and p_i^n), we have divided the stations in four groups according to their dimension. The values chosen for the stations in each group are shown in Table 1. Obviously, bigger stations require more resources to be protected/disrupted. As an example, Caianello is a very small station and only requires 2 units, whereas Naples is the biggest station and requires 12 units.

In our empirical study, we have analyzed and compared protection strategies to hedge against disruptions of different magnitudes. Specifically, we considered small, medium, large and very large disruptions. The amount of interdiction resources associated with each event size are displayed in Table 2. With this choice, a small disruption can only affect a very small station, whereas a very large event is able to interdict a big station and a few other smaller assets.

The analysis also considers different budget levels. These were chosen as a percentage of the budget needed to protect the whole network.

Some preliminary results are displayed in Table 3, which shows the total amount of flow which is lost in different disruption scenarios and for different protection investment levels. It can be seen that even a small disruption can have a considerable impact on traffic flow if protective measures are not carried out: the worst-case loss

Table 1 Resources needed to protect/interdict a node

Node dimension	Interdiction/protection resources
Very small	2
Small	4
Medium	8
Big	12

Table 2 Disruption scenarios

Size	Resource units
Small	2
Medium	5
Large	10
Very large	20

Table 3 Percentage of lost flow for different disruption scenarios and protection budget levels

	No protection	1 %	5 %	10 %
Small	38	18	10	5
Medium	67	39	20	16
Large	88	75	35	28
Very large	98	96	77	54

after a small disruption can result in a loss of 38 % of the total flow. This can reach 67, 88 and 98 % for medium, large, and very large disruptions respectively. The effect of protecting even as little as 1 % of the assets can be considerable, if protection resources are allocated optimally. This is true especially for small and medium size disruption scenarios, where the total losses can be reduced from 38 to 18 % for small events and from 67 to 39 % for medium events. For large and very large events, greater protection investments are needed to get significant reductions in flow losses. As an example, an optimal investment equal to 5 % of the protection cost of the total network, can more than halve the flow loss resulting from a large disruption (from 88 to 35 %).

To provide a better understanding of how increasing budget levels may affect the system losses in case of disruption, in Fig. 2 we show the percentage marginal reduction in flow losses for each percentage point increase in protection resources. We let the budget vary between 1 and 10 % of the protection cost of the whole network.

This analysis sheds light on possible tradeoffs between protection expenditures and flow loss reductions in case of worst-case system disruptions. As an example, if a large disruptive event is considered, a 1 % investment results in a worst-case loss reduction of about 15 % (first segment of the third bar in the chart). However, if an investment of 2 % can be made, the benefit is more than doubled, bringing an additional 25 % flow loss reduction and an overall reduction of 40 %.

The differences between the four disruption scenarios can be further analyzed through the graphs plotted in Figs. 3, 4, 5 and 6. For each scenario, the corresponding graph displays the contribution of a percentage point increment in protection resources on the overall objective improvement.

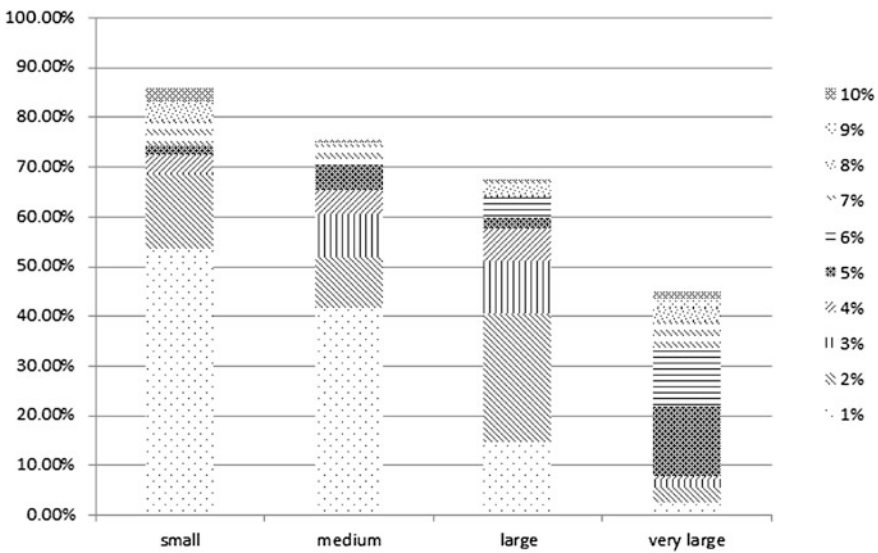


Fig. 2 Marginal percentage decrease in flow loss due to percentage point increments of the protection budget

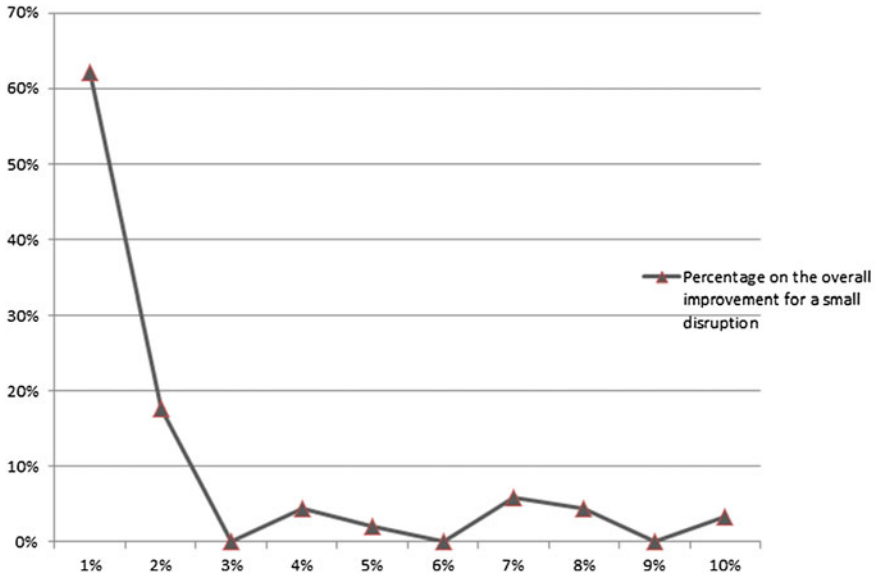


Fig. 3 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for small disruptions

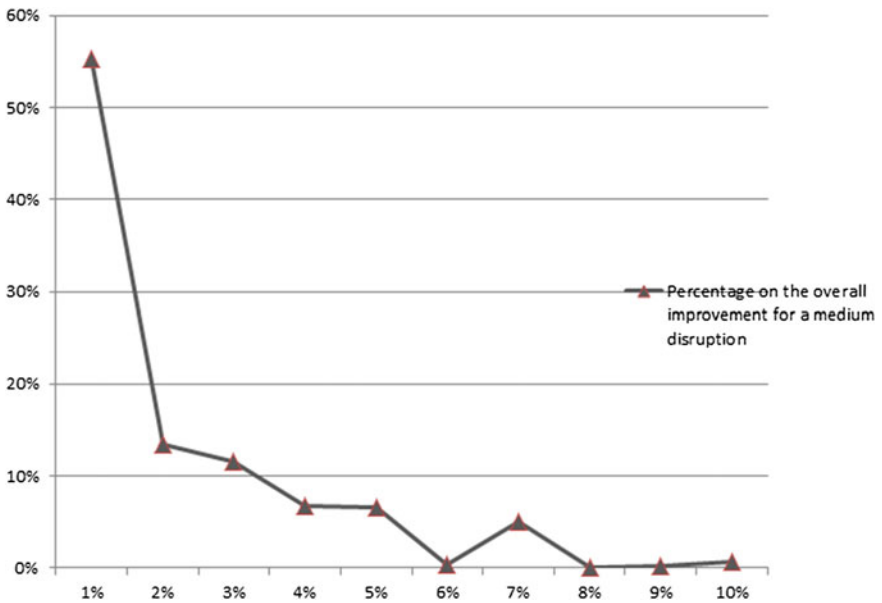


Fig. 4 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for medium disruptions

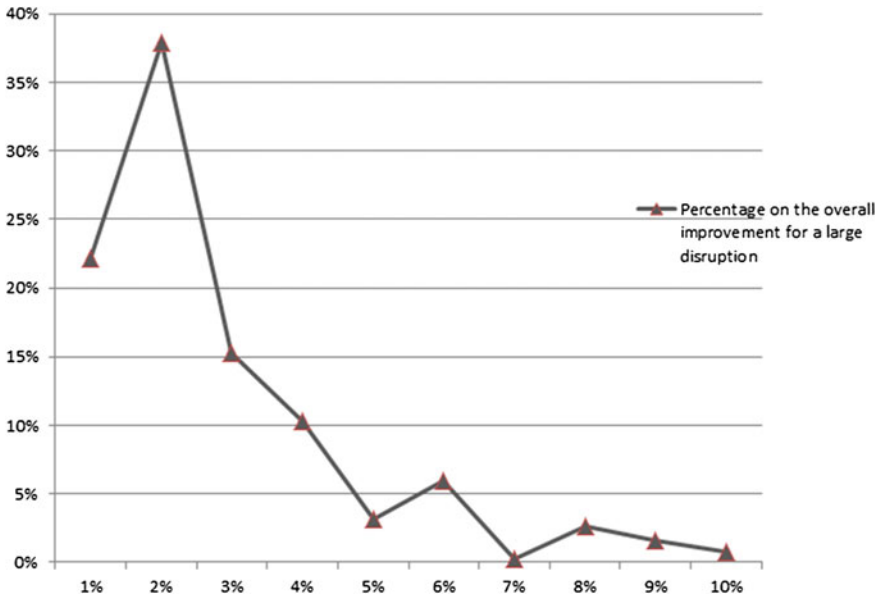


Fig. 5 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for large disruptions

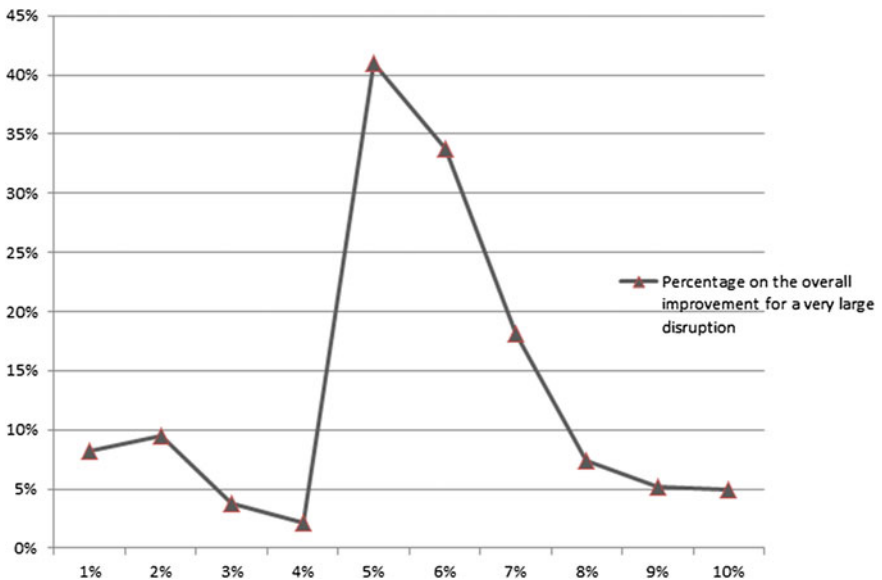


Fig. 6 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for very large disruptions

The first clear difference is that in the scenarios with low and medium level disruptions (Figs. 3 and 4) the first percentage point increase is responsible for more than half of the overall benefit. To reach similar results for large disruptions, a two point increment is needed (Fig. 5). When very large disruptions are considered, the first few increments have a somewhat limited effect on reducing flow losses whereas a peak can be noticed in correspondence of a 5 % investment (Fig. 6). An additional percentage point increase, results in another significant flow loss reduction. This seems to indicate that if large disruptions are anticipated, a protection budget in this range (5–6 % of the total protection costs) should be warranted to maximize the benefits of security investments.

It is clear that the protection strategies identified by the model may differ quite significantly, depending on the magnitude of the disruption given in input to the model (parameter p). Our next analysis aims at identifying protection plans which are robust across all scenarios, so as to hedge against the uncertainty characterizing the size and extent of disruptive events. To this end, we evaluate how the optimal solution identified for a given disruption size performs in all the other scenarios.

The results of this analysis are shown in Tables 4 and 5 for two budget levels, equal to 5 and 10 % of the resources needed to protect the whole network. These cases correspond to values of q equal to 17 and 35 respectively. The tables show the percentage flow loss increase which is observed when the optimal protection strategy computed for a given scenario (*supposed scenario*) is used in a different scenario (*actual scenario*). The last two columns display the maximum and average increase across all the other scenarios. From the analysis of Table 4 ($q = 17$), it is clear that the

Table 4 Cross-comparison of different optimal protection plans

Supposed scenario	Actual scenario				MAX (%)	AVG (%)
	Small (%)	Medium (%)	Large (%)	Very large (%)		
Small	0	98.8	75.2	20.3	98.8	48.6
Medium	21.8	0	0	22.5	22.5	11.1
Large	21.8	0	0	22.5	22.5	11.1
Very large	133.8	104	78.1	0	133.8	79

Relative flow loss increase in percentage. Case $q = 17$

Table 5 Cross-comparison of different optimal protection plans

Supposed scenario	Actual scenario				MAX (%)	AVG (%)
	Small (%)	Medium (%)	Large (%)	Very large (%)		
Small	0	138.4	106.3	74.8	138.4	79.9
Medium	85.7	0	8.6	71.6	85.7	41.5
Large	98.1	3.2	0	74	98.1	43.8
Very large	126.1	19.9	19.7	0	126.1	41.4

Relative flow loss increase in percentage. Case $q = 35$

Table 6 Optimal protection plans for different disruption scenarios and different protection budgets

Disruption size	Protection resources			
	$q = 1 \%$	$q = 2 \%$	$q = 5 \%$	$q = 10 \%$
Small	Naples-Barra Naples-Afragola	Naples-Barra Naples-Afragola T. Annunziata-C. Stabia	Torregaveta-Naples Naples-Afragola Naples-Barra S. Maria C. V.-Caserta T. Annunziata-C. Stabia T. Annunziata-Nocera	Torregaveta-Naples Rome-Afragola Naples-Afragola Naples-Barra Naples-T. Annunziata T. Annunziata-C. Stabia T. Annunziata-Nocera
Medium	Naples-Barra T. Annunziata-C. Stabia	Barra Naples-Barra T. Annunziata-C. Stabia	Barra T. Annunziata Naples-Aversa Naples-Afragola Naples-Barra Naples-T. Annunziata T. Annunziata-C. Stabia T. Annunziata-Nocera	Barra T. Annunziata S. Giorgio a C. Torregaveta-Naples Naples-Aversa Naples-Afragola Naples-Barra Naples-T. Annunziata S. Maria C. V.-Caserta S. Giorgio a C.-T. Annunziata O. T. Annunziata-C. Stabia T. Annunziata-Nocera
Large	Naples-Barra T. Annunziata-Nocera	Barra Naples-Afragola Naples-Barra	Barra T. Annunziata Naples-Aversa Naples-Afragola Naples-Barra Naples-T. Annunziata T. Annunziata-C. Stabia T. Annunziata-Nocera	Barra T. Annunziata S. Giorgio a C. Torregaveta-Naples Naples-Aversa Naples-Afragola Naples-Barra Naples-T. Annunziata Barra-P. Marino T. Annunziata-C. Stabia T. Annunziata-Nocera T. Annunziata O.-P. Marino

(continued)

Table 6 (continued)

Disruption size	Protection resources			
	$q = 1 \%$	$q = 2 \%$	$q = 5 \%$	$q = 10 \%$
Very large	Naples-Afragola Samo-Codola	Naples-Aversa S.Maria C.V.-Caserta T.Annunziata-C.Stabia T.Annunziata-Nocera	Naples Barra Naples-Barra	Naples Barra T.Annunziata Nocera Naples-Aversa Naples-Afragola Naples-Barra Naples- T.Annunziata T.Annunziata-C.Stabia T.Annunziata-Nocera Nocera-Codola Samo-Codola

Table 7 Post-protection worst-case losses in different disruption scenarios and for different protection budgets

Disruption size	Protection resources			
	$q = 1\%$	$q = 2\%$	$q = 5\%$	$q = 10\%$
Small	Rome-Afragola T. Annunziata-C. Stabia	Rome-Afragola Naples-T. Annunziata	Rome-Afragola Sorrento-T. Annunziata O.	Naples-S. Maria C.V. S. Maria C.V.
Medium	Barra P. Marino-Sarno	V. Literno-Naples Rome-Afragola Naples-Aversa Aversa-Caserta T. Annunziata-C. Stabia	Torregaveta-Naples Rome-Afragola Barra-P. Marino S. Giorgio a C.-T. Annunziata O. P. Marino-Sarno	Nocera Rome-Afragola
Large	Barra Torregaveta-Naples Naples-Afragola S. Maria C.V.-Caserta Afragola-Cancello T. Annunziata-C. Stabia Naples-T. Annunziata P. Marino-Sarno	Cancello V. Literno-Naples Torregaveta-Naples Naples-Aversa Barra-P. Marino S. Maria C.V.-Caserta T. Annunziata-Nocera P. Marino-Sarno	Cancello Torregaveta-Naples Rome-Afragola Rome-Afragola Aversa-Caserta T. Annunziata-C. Stabia Naples-T. Annunziata S. Giorgio a C.-T. Annunziata O. Nocera-Codola Nocera-Salerno	S. Giorgio a C. Rome-Afragola S. Maria C.V.-Caserta
Very large	Naples Cancello S. Maria C.V.-Caserta Caserta T. Annunziata-C. Stabia Nocera-Codola Nocera-Salerno Mercato-Salerno	Naples Cancello Nocera Aversa-Caserta Mercato-Salerno	Cancello S. Giorgio a C. V. Literno-Naples Torregaveta-Naples Naples-S. Maria C.V. Naples-Aversa Naples-Afragola Naples-T. Annunziata S. Maria C.V.-Caserta Aversa-Caserta Barra-P. Marino T. Annunziata-C. Stabia P. Marino-Sarno Nocera-Codola Nocera-Salerno	Cancello S. Giorgio a C. Afragola Aversa- Torregaveta-Naples S. Maria C.V.-Caserta Aversa-Caserta Barra-P. Marino P. Marino-Sarno Nocera-Salerno

optimal solution for medium and large events is the same. It is also the solution that works better across the different scenarios, with an average error of 11.1 % and a maximum error of 22.5 %. In the second case (Table 5), all the solutions are different and the best choice, in terms of average percentage increase of disrupted flow, is the optimal protection strategy computed for very large disruptions. Nevertheless, assuming a medium size disruption may result in a better compromise solution: the average percentage increase is really close to the one obtained for very large events (41.5 vs. 41.4 %) but the maximum value is considerably smaller (85.7 vs. 126.1 %). Overall this analysis indicates that the assumptions made on the disruption size may have a significant impact on the identification of effective protection strategies. In general, avoiding the extreme cases and assuming medium to large disruptions leads to the most robust defensive plans.

Finally, in Tables 6 and 7 we display the solutions to the model for different disruption scenarios and protection budget levels. Table 6 shows the network components chosen for protection, whereas Table 7 shows the interdiction plans (i.e., the worst-case losses) after protection.

We can see that Afragola and Barra appear quite often in the protection and disruption strategies. This can be explained by noticing that the first station is a crucial node of the high speed service and its disruption affects the connection between Rome and Naples; the second station belongs to the Circumvesuviana railway network and intercepts a huge portion of the traffic generated by that service. It is interesting to note that Cancellò appears very frequently among the components to be interdicted, in spite of being a very small station. This may be due to its very central position. Cancellò, in fact, intercepts the flow between the largest cities of the region and this makes it an attractive target for an intelligent attacker. Finally, it can be noted that Naples only appears in a few solutions probably because, although it is the most important station, is also the most difficult and expensive asset to protect and or disrupt.

6 Conclusions and Discussion

To increase railway system security, it is crucial that scarce protection resources are allocated across the network assets in the most cost-efficient way. This chapter has presented an optimization model for the strategic planning of protection investments. The proposed model identifies the optimal allocation of defensive resources to hedge against worst-case scenario flow losses due to malicious attacks. We have demonstrated how the model results can be used to identify the optimal investment level to achieve a desirable degree of protection, and highlighted possible trade-offs between protection expenditure and traffic flow preserved. Finally, we have shown how to select robust solutions that perform well under disruptive scenarios of different magnitude.

The proposed model can be extended in several ways to capture additional realism and the complexities characterizing railway systems. As an example, our

model objective is to minimize the amount of passenger flow which is lost after a disruption. Other performance measures could be considered which combine both system cost and customer disutility into a multi-objective model. These measures should include issues such as delays, increased travel time and duration of the disruption. We also made the assumptions that protected components are completely immune to failure and that attacks on unprotected components are always successful. Other modeling frameworks should be developed to model different degrees of protection and interdiction. For example, partial protection could be considered where protected components only preserve part of their operational capabilities or have shorter recovery times or smaller failure probabilities depending on the level of protection investment.

References

1. Hartong M, Goel R, Wijesekera D (2008) Security and the US rail infrastructure. *Int J Crit Infrastruct Prot* 1:15–28
2. Golany B, Kaplan EH, Marmur A, Rothblum UG (2009) Nature plays with dice—terrorists do not: allocating resources to counter strategic versus probabilistic risks. *Eur J Oper Res* 192:198–208
3. Brown G, Carlyle M, Salmeron J, Wood K (2006) Defending critical infrastructure. *Interfaces* 36:530–544
4. Liberatore F, Scaparra MP, Daskin M (2012) Optimization methods for hedging against disruptions with ripple effects in location analysis. *Omega* 40:21–30
5. Scaparra MP, Church RL (2008) A bilevel mixed integer program for critical infrastructure protection planning. *Comput Oper Res* 35:1905–1923
6. Murray AT, Matisziw TC, Grubestic TH (2007) Critical network infrastructure analysis: interdiction and system flow. *J Geogr Syst* 9:103–117
7. Corley HW, Sha DY (1982) Most vital links and nodes in weighted networks. *Oper Res Lett* 1:157–160
8. Golden B (1978) A problem in network interdiction. *Naval Res Logist Q* 25:711–713
9. Wollmer R (1964) Removing arcs from a network. *Oper Res* 12:934–940
10. Church RL, Scaparra MP, Middleton RS (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. *Ann Assoc Am Geogr* 94:491–502
11. Wood KR (1993) Deterministic network interdiction. *Math Comput Model* 12:1–18
12. Matisziw TC, Murray AT (2009) Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure. *Comput Oper Res* 36:16–26
13. Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. *IEEE Trans Power Syst* 19:905–912
14. Ukkusuri SV, Yushimito WF (2009) A methodology to assess the criticality of highway transportation networks. *J Transp Secur* 2:29–46
15. Church RL, Scaparra MP (2007) Protecting critical assets: the r-interdiction median problem with fortification. *Geogr Anal* 39:129–146
16. Aksen D, Aras N, Piyade N (2013) A bilevel p-median model for the planning and protection of critical facilities. *J Heuristics* 19:373–398
17. Bricha N, Nourelfath M (2013) Critical supply network protection against intentional attacks: a game-theoretical model. *Reliab Eng Syst Saf* 119:1–10
18. Liu C, Fan Y, Ordez F (2009) A two-stage stochastic programming model for transportation network protection. *Comput Oper Res* 36:1582–1590

19. Fan Y, Liu C (2010) Solving stochastic transportation network protection problems using the progressive hedging-based method. *Netw Spat Econ* 10:193–208
20. Peeta S, Salman FS, Gunnec D, Viswanath K (2010) Pre-disaster investment decisions for strengthening a highway network. *Comput Oper Res* 37:1708–1719
21. Miller-Hooks E, Zhang X, Faturechi R (2012) Measuring and maximizing resilience of freight transportation networks. *Comput Oper Res* 39:1633–1643
22. Cappanera P, Scaparra MP (2011) Optimal allocation of protective resources in shortest-path networks. *Transp Sci* 45:64–80
23. Peterson SK, Church RL (2008) A framework for modeling rail transport vulnerability. *Growth Change* 39:617–641
24. Perea F, Puerto J (2013) Revisiting a game theoretic framework for the robust railway network design against intentional attacks. *Eur J Oper Res* 226:286–292
25. Bard JF (1998) *Practical bilevel optimization*. Kluwer Academic Publishers, Boston
26. Dempe S (2002) *Foundations of bilevel programming*. Kluwer Academic Publishers, Dordrecht
27. Gümüş ZH, Floudas CA (2005) Global optimization of mixed-integer bilevel programming problems. *CMS* 2:181–212
28. Losada C, Scaparra MP, O’Hanley JR (2012) Optimizing system resilience: a facility protection model with recovery time. *Eur J Oper Res* 217:519–530