Passenger railway network protection: A model with variable post-disruption demand service

Stefano Starita* Maria Paola Scaparra†

Abstract

Protecting transportation infrastructures is critical to avoid loss of life and to guard against economic upheaval. This paper addresses the problem of identifying optimal protection plans for passenger rail transportation networks, given a limited budget. We propose a bilevel protection model which extends and refines the model previously introduced by Scaparra et al. (2015). In our extension, we still measure the impact of rail disruptions in terms of the amount of unserved passenger demand. However, our model captures the post-disruption user behaviour in a more accurate way by assuming that passenger demand for rail services after disruptions varies with the extent of the travel delays. To solve this complex bi-level model, we develop a simulated annealing algorithm. The efficiency of the heuristic is tested on a set of randomly generated instances and compared with the one of a more standard exact decomposition algorithm. To illustrate how the modelling approach might be used in practice to inform protection planning decisions, we present a case study based on the London Underground. The case study also highlights the importance of capturing flow demand adjustments in response to increased travel time in a mathematical model.

Keywords: Railway networks, disruption, protection, bi-level models, decomposition, simulated annealing.

1 Introduction

A critical infrastructure, as the name suggests, is a system deemed to be vital to a country. Several comparable interpretations of the adjective *critical* have been utilized. The H.R.3162 Patriot Act (2001), enacted by the U.S. government, states that critical infrastructures are "*systems and assets, whether physical or virtual, so vital to the United States*

*Corresponding author. Warwick Business School, University of Warwick, CV4 7AL Coventry, UK, E-mail: Stefano.Starita@wbs.ac.uk

†Kent Business School, University of Kent, CT2 7PE Canterbury, UK.

that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". An analogous definition is provided by the EU in the Council Directive 2008/114/EC.

Examples of critical infrastructures include telecommunications, transportation systems (including rail networks), energy supply chains, banking systems, and water supply networks. As demonstrated by numerous recent events, natural disasters, terrorism and unintentional accidents pose serious threats to critical infrastructures. For example, the Fukushima nuclear disaster in 2011 caused thousands of deaths and led to the evacuation of 300,000 people. Several railway stations were completely washed away, railway services were suspended in several cities and thousands of people were stranded at stations. The interruption of rail services in Tokyo caused a near-paralysis of the city. Similarly, the London bombings in 2005 killed 56 people and severely disrupted the rail and other transportation and telecommunication systems in the central area of the city. On a smaller scale, the Philadelphia train derailment in 2015 killed 8 people, injured hundreds and disrupted train services for several days.

To reduce systems vulnerabilities and mitigate post-disruption losses, protection strategies are needed. When dealing with rail systems, the protection measures should account for the assets needing protection and the threats to the infrastructure (e.g., man-made, natural and accidental threats). For example, in recent years, railways-related copper theft in the UK has been escalating - causing frequent train delays and an estimated annual cost to the UK economy of 770m (Milmo, 2011). To head off copper thieves, cables need to be secured and intrusion detection devices along track sections need to be installed. Other measures against man-made threats include the installation of Closed Circuit Television systems (CCTV) and the use of video analysis software to protect critical assets like stations, bridges and tunnels (Fiumara, 2015). Natural events can also cause severe disruptions to railway services. For example, the collapse of a sea wall in Devon (UK), due to severe weather, disrupted the railway to Cornwall and required about 100M for repairs (Robinson, 2014). Structural reinforcements (i.e., barriers and pits to prevent disruptions from flooding or hardening structures vulnerable to earthquakes) are typical protection measures against natural events.

Protecting critical infrastructures can involve massive financial investments. Therefore it is essential to perform a vulnerability analysis and distribute resources in a cost-efficient way.

In this paper, we present a new optimization problem for railway network protection. We refer to the proposed problem as the Network Protection Problem with Variable Demand Loss (NPVDL). The aim is to find the optimal allocation of protection resources among railway assets (stations, tunnels, bridges, flyovers, rail tracks, etc.) so as to minimize the

impact of worst-case disruptions on the service provision to rail passengers. The disruption impact is measured in terms of passenger flow (or demand) loss. A key aspect of our model is that it takes into account the system users behaviour after a disruption. Travel time is one of the most important factors influencing route choice behaviour (Wang et al., 2014). After a disruption, increased travel times may cause some passengers to abandon the trip or resort to other means of transportation, with associated user disutility and system-wide costs. Failure to capture flow demand adjustments as a response to increased travel time in a mathematical model may lead to the identification of inaccurate and or suboptimal protection plans. Our protection model is unique by virtue of its inclusion of flow demand adjustments in response to increased travel time. Our model also considers the different costs of protection measures associated with the various assets.

The remainder of this paper is organized as follows. Section 2 provides a brief review of the literature. Section 3 presents the problem formulation. Section 4 provides a description of the exact solution approach utilised to evaluate the heuristic accuracy. Section 5 introduces a simualted annealing heuristic used to solve the problem efficiently. In Section 6, some computational results compare the performance of the two proposed algorithms. In Section 7, a case study on the central London underground is presented to illustrate the practical use of the modelling approach. The last section offers conclusions and possible extensions of the NPVDL model.

2 Background

The problem of optimizing the reliability of critical infrastructure systems against disruptions has been widely studied from different angles. Broadly, the proposed models can be split into two major categories: *design models* and *protection models* (Snyder et al., 2006). *Design models* aim at determining reliable system configurations which work efficiently under normal circumstances but also in case of disruption. *Protection models* aim at hardening and securing systems that are already in place. They identify the set of system components to protect so as to mitigate the impact of disruptions. A further distinction can be made based upon the underlying system type: in facility-based systems, only nodes (e.g., warehouses, power plants, hospitals etc.) are subject to disruption; in network-based systems, both nodes and links (e.g., roads or rail tracks) can be disrupted.

Design models that incorporate the issue of disruption have received significant attention in the facility location context. Several works extend popular location models such as the p-median (Hakimi, 1964, 1965) and the uncapacitated fixed-charge location (UFLP) (Balinski, 1965) to include the concept of system reliability. For instance, Snyder and Daskin (2005)

propose reliable versions of the classic p-median and UFLP problems, where multiple facilities can fail independently with a fixed probability and, consequently, unserved demand generates a penalty cost. These reliability models are further analysed and extended in Berman et al. (2007), Cui et al. (2010), and O'Hanley et al. (2013). Chen et al. (2011) propose a non-linear model that incorporates expected inventory and customer costs in the reliable UFLP. Li and Ouyang (2010) extend the UFLP by adding spatially correlated disruptions. Peng et al. (2011) introduce a robust optimization model for designing multi-echelon facility systems subject to failures. Akgun et al. (2015) analyse the location of facilities for prepositioning emergency supplies so as to minimize the risk to which demand points are exposed. Schmitt et al. (2015) investigate the optimal design of multi-location systems, focusing on how centralized or decentralized inventory affects the supply chain's cost under disruptions.

Network design models which include reliability issues have been proposed in a few recent works. For example, Desai and Sen (2010) extend traditional network design models by incorporating mitigation strategies into the design phase so as to reduce the arcs' failure probabilities. Laporte et al. (2010) introduce a game theoretic framework for robust railway planning. They consider link failures and the presence of a competing transportation mode. García-Archilla et al. (2013) introduce a simplified version of this model which is computationally more tractable. A dynamic variation of these robust models is presented by Perea and Puerto (2013), who also consider the allocation of security resources on the network. Gong et al. (2014) study the problem of designing a reliable supply chain system, by formulating an interdependent layered network model. Khaled et al. (2015) propose a train design optimization model for freight railroads which incorporates congestion issues in case of disruption. Azad et al. (2016) propose a risk management approach based on solving a network optimization model to ascertain the criticality of each railroad link. This information is then fed into another model to design a suitable mitigation strategy, including building dis-similar paths for train services, and installing alternative links around critical service legs.

The vast majority of protection models proposed in the literature use a worst-case scenario approach. The problems are formulated as multi-level models to emulate the game between an intelligent attacker and an intelligent defender. These problems can be divided into two categories: interdiction and fortification problems. Interdiction or *attacker-defender* problems are used to identify the assets that, when damaged or removed, reduce a system's performance the most. In other words, they are used to assess the criticality of a system's components. Conversely, fortification or *defender-attacker* problems identify the optimal distribution of limited protective resources so that the system's value loss, after a worst-case interdiction, is minimised.

Several protection models have been recently proposed for facility-based systems. Church

et al. (2004) introduce the interdiction problem for p-median and max-covering problems, to study the set of facilities that, when lost, have the greatest impact on the transportation costs or demand coverage, respectively. Aksen et al. (2010) study a variation of the p-median interdiction problem where the facilities can acquire additional capacity following a disruption, whereas Losada et al. (2012a) consider uncertainty in the outcomes of disruptive events. Aksen et al. (2014) integrate partial disruption and demand outsourcing into the p-median interdiction problem. Church and Scaparra (2007) formulate a bi-level fortification problem to explicitly model protection efforts. Scaparra and Church (2012) consider the fortification problem for capacitated facilities. Liberatore et al. (2011) and Zhu et al. (2013) further extend the fortification model by considering the uncertainty in the number of losses and protection outcomes, respectively. Losada et al. (2012) study the impact of the recovery time of disrupted facilities on the selection of protection plans for median-type systems. Liberatore et al. (2012) propose a tri-level facility protection problem which includes issues such as correlation of disruptive events and disaster propagation effects.

Within the context of network-based systems, a few interdiction and protection models have been introduced for distance-based networks. For example, Fulkerson and Harding (1977) study the effect of partial interdictions on arcs in shortest path networks. Israeli and Wood (2002) formulate the shortest path interdiction problem as a bi-level model. Bayrak and Bailey (2008) consider an extension of this model where the players have asymmetric information about the network. Peeta et al. (2010) propose a fortification model where highway links can be hardened to reduce the likelihood of failure. Cappanera and Scaparra (2011) introduce a tri-level model to optimize protection decisions in shortest-path networks.

A line of research strictly related to our work deals with interdiction and fortification of flow-based networks. The seminal paper on this topic is due to Wollmer (1964), who studies the problem of removing a subsets of arcs from a max-flow network to identify the critical components. Wood (1993) proposes a few max-flow interdiction problems, including partial interdiction, multiple sources and sinks, undirected networks, multiple resources and multiple commodities. Cormican et al. (1998) consider uncertainty in the interdiction outcomes and propose a stochastic model that minimizes the expected max-flow. Lim and Smith (2007) study the interdiction (both partial and complete) of multi-commodity networks. Rad and Kakhki (2013) introduce a dynamic version of the max-flow problem by assigning a traversal time to each arc. Jin et al. (2015) study a tri-level fortification model where nodes of a rail network can be disrupted with multiple intensities. These disruption levels affect the in/out flow capacity of stations. The authors propose a variable neighbourhood search algorithm to solve the model and test it on a case-study based on the Singapore rail transit system. Myung and Kim (2004), Murray et al. (2007), and Matisziw and Murray (2009) study a flow

interdiction problem on a network with multiple sources and destinations, where the system's value is measured in terms of the amount of demand that can still be served after interdiction. Scaparra et al. (2015) build upon these models to devise a protection optimization model for railway systems. They embed the aforementioned flow interdiction problem into a bilevel protection problem and consider both arcs and nodes as possible targets for interdiction and protection. Starita and Scaparra (2016) propose a dynamic version of this protection model, where protection resources become available in different time periods.

A practical limitation of previous interdiction models for flow-based networks (Myung and Kim, 2004, Murray et al., 2007, Matisziw and Murray, 2009) is that the flow between two nodes is considered *lost* or *unserved* only if the two nodes are completely disconnected after interdiction. Although this assumption simplifies the mathematical representation of the problems and their solution, it also limits their practical applicability, especially to the context of transportation networks. In transport systems, in fact, passenger demand between two nodes may be lost even if a connection does exist but the service is significantly deteriorated. As an example, if an interdiction causes long delays, travelers may resort to different modes of transportation or even abandon the trip. Scaparra et al. (2015) and Starita and Scaparra (2016) make the first attempt at redressing this shortcoming by introducing the concept of *acceptable paths*, i.e., paths whose length does not exceed the length of the corresponding shortest path by more than a given threshold. User demand is considered unserved if, after a disruption, no acceptable path is available between the origin and destination nodes. The authors, however, note that their models still present some limitations in that each origin-destination path is either acceptable or not, and the resulting solutions are highly sensitive to the path threshold parameter used to define acceptable paths. In their conclusive remarks, they suggest developing new models which better capture the travelers' behaviour.

In this paper, we extend the work by Scaparra et al. (2015) and propose a novel bi-level protection model for railway infrastructures where the post-disruption user behaviour is modelled in a more accurate and realistic way. We assume that, following a disruption, the proportion of system users willing to use alternative railway routes depends on the travel time of the alternative paths (i.e., as the quality of service decreases, so does the demand for that service). In real applications, this proportion could be estimated by collecting survey data on a sample of railway network users. The inclusion of the post-disruption user behaviour into a mathematical model increases the model complexity quite significantly. As a consequence, the exact methods previously proposed to solve these types of protection-interdiction models are inadequate to solve the NPVDL. We therefore propose a heuristic approach to find good approximations to the optimal protection plans.

To summarize, the contribution of this paper is threefold: we incorporate the user be-

haviour into a protection model for railway infrastructure; we propose an efficient solution approach based on simulated annealing to tackle the computational complexity of the resulting bi-level model; we apply the model to a real-world data driven case study focused on the Central London Tube.

3 Problem statement and formulation

3.1 Model assumptions

The NPVDL problem is formulated as a bi-level linear mixed integer model. The transportation network is modelled as a graph $G(N, A)$, where N is the set of nodes (e.g., stations) and A is the set of arcs (e.g., rail tracks). A limited budget is available for protecting the network. Interdiction resources are also assumed to be limited. This is a common assumption in interdiction modelling, where interdiction resources are used as a surrogate for the disruption magnitude. The demand for service between any two nodes is known and entirely served by the shortest path. If the shortest path becomes unavailable, the amount of flow loss depends on the length of the alternative routes. A disrupted element is completely unusable and, therefore, is removed from the network. An element, once protected, is immune to any disruption. Both arcs and nodes can be disrupted/protected. We also assume that the amount of resources needed to protect/disrupt an element is known.

3.2 A bilevel formulation for the NPVDL problem

The bilevel model for NPVDL uses the following notation.

Indices, sets and parameters
$s \in N$: index used for flow sources.
$d \in N$: index used for flow destinations.
$i \in N$: index used for network nodes.
$j \in A$: index used for network arcs.
c_j : nominal length of arc j.
f_{sd} : passenger flow between s and d.
N_{sd} : set of paths that connect s and d.
$r, t \in N_{sd}$: indexes used for network paths.
$A(r)$: set of arcs along path r.
$N(r)$: set of nodes along path r.
α_r : percentage of passenger flow using the service when path r is the shortest available path.

$\Pi(r) = \{t \in N_{sd} : length(t) < length(r)\}$, i.e. set of all paths connecting s to d which are shorter than path r.
B : protection budget.
P : amount of interdiction resources available.
p_i^n, p_j^a : resource units needed to disrupt node i and arc j, respectively.
q_i^n, q_j^a : resource units needed to protect node i and arc j, respectively.

Decision variables
$X_i^n = 1$ if node i is disabled; 0 otherwise.
$X_j^a = 1$ if arc j is disabled; 0 otherwise.
$Y_i^n = 1$ if node i is protected; 0 otherwise.
$Y_j^a = 1$ if arc j is protected; 0 otherwise.
$\omega_r = 1$ if path r is available; 0 otherwise.
$S_r = 1$ if path r is the shortest non-disrupted path between a given origin and destination; 0 otherwise.
Z_{sd} = percentage of disrupted (or lost or unserved) flow, between s and d.

The problem is formulated as follows:

$$[\text{NPVDL}] \quad \min_{\mathbf{Y}} F(\mathbf{Y}) \tag{1}$$

$$\text{s.t.} \quad \sum_{i \in N} q_i^n Y_i^n + \sum_{j \in A} q_j^a Y_j^a \leq B \tag{2}$$

$$Y_i^n \in \{0,1\} \qquad \forall i \in N \tag{3}$$

$$Y_j^a \in \{0,1\} \qquad \forall j \in A \tag{4}$$

$$\text{where} \quad F(\mathbf{Y}) = \max_{\mathbf{X}} \sum_s \sum_d f_{sd} Z_{sd} \tag{5}$$

$$\text{s.t.} \quad X_i^n \leq 1 - Y_i^n \qquad \forall i \in N \tag{6}$$

$$X_j^a \leq 1 - Y_j^a \qquad \forall j \in A \tag{7}$$

$$\sum_{i \in N} p_i^n X_i^n + \sum_{j \in N} p_j^a X_j^a \leq P \tag{8}$$

$$Z_{sd} = 1 - \sum_{r \in N_{sd}} S_r \alpha_r \qquad \forall s, d \in N \tag{9}$$

$$\sum_{r \in N_{sd}} S_r \leq 1 \qquad \forall s, d \in N \tag{10}$$

$$\sum_{r \in N_{sd}} S_r \geq \sum_{r \in N_{sd}} \omega_r / |N_{sd}| \qquad \forall s, d \in N \tag{11}$$

$$S_r \leq \omega_r \qquad \forall s, d \in N, r \in N_{sd} \tag{12}$$

$$S_r \leq 1 - \sum_{t \in \Pi(r)} \omega_t / |N_{sd}| \qquad \forall s, d \in N, r \in N_{sd} \tag{13}$$

$$\omega_r \geq 1 - \sum_{j \in A(r)} X_j^a - \sum_{i \in N(r)} X_i^n \qquad \forall s, d \in N, r \in N_{sd} \tag{14}$$

$$X_i^n \in \{0, 1\} \qquad \forall i \in N \tag{15}$$

$$X_j^a \in \{0, 1\} \qquad \forall j \in A \tag{16}$$

$$0 \leq Z_{sd} \leq 1 \qquad \forall s, d \in N \tag{17}$$

$$S_r \in \{0, 1\} \qquad \forall s, d \in N, r \in N_{sd} \tag{18}$$

$$\omega_r \in \{0, 1\} \qquad \forall s, d \in N, r \in N_{sd} \tag{19}$$

The aim of the *defender* is to minimize the overall flow loss (1), by distributing protection resources over the elements of the network. Constraint (2) represents the protection budget limit. The aim of the *attacker* is to maximize the flow loss (5), by targeting the unprotected elements of the network. Constraints (6) and (7) state that nodes and arcs cannot be disrupted if they are protected. Constraint (8) limits the number of elements that can be interdicted. Constraints (9) define the percentage amount of flow between s and d which is lost. This is computed based on the available shortest path between the two nodes. Constraints (10) state that, for each pair of nodes, there can be at most one shortest path available. Constraints (11) state that if there is at least one path available between s and d, there must also be a non-disrupted shortest path connecting the two nodes. Constraints (12) impose that a path can be the shortest available path only if it is available (i.e., not disrupted). Constraints (13) ensure that, given an origin-destination pair s and d, a path r can be the shortest available one connecting the two nodes only if all the paths shorter than r are unavailable. Constraints (14) state that a path r is disrupted only if at least one element (node or arc), belonging to that path, is interdicted. Finally, constraints (3)-(4) and (15)-(19) represent the domain restrictions of the decision variables.

4 SVI decomposition algorithm

To evaluate the performance of the heuristic described in the next section and its ability to identify optimal solutions, we develop a decomposition algorithm based on the use of

Super Valid Inequalities (SVI). A SVI is a cutting plane that reduces the feasible region of a problem by making the incumbent solution and eventually other solutions infeasible. Although a SVI can remove feasible integer solutions, it is guaranteed not to eliminate all the optimal solutions, unless an optimal solution has already been found. Examples of SVI-based decomposition approaches for solving bilevel problems to optimality can be found in Israeli and Wood (2002), O'Hanley and Church (2011) and Losada et al. (2012).

The decomposition approach, referred to as SVI-D, involves decomposing the NPVDL into two smaller problems which are solved alternatively: the Relaxed Master Problem (RMP) and the Sub-Problem (SP). The RMP is simply a feasibility seeking problem, consisting of a set of SVIs and constraints (2), (3), and (4). At each iteration, the RMP is solved to identify a feasible protection strategy $\hat{\mathbf{Y}}$. The Sub-Problem is subsequently solved to obtain the most disruptive interdiction strategy, $\hat{\mathbf{X}}$, in response to protection plan $\hat{\mathbf{Y}}$. Namely, SP is the lower level interdiction problem where the protection variables are fixed. SP is defined as follows:

$$\left[SP(\hat{\mathbf{Y}})\right] \quad z_{sp} = \max_{\mathbf{X}} \sum_{s} \sum_{d} f_{sd} Z_{sd} \tag{20}$$

$$\text{s.t.} \quad X_i^n \leq 1 - \hat{Y}_i^n \qquad \forall i \in N \tag{21}$$

$$X_j^a \leq 1 - \hat{Y}_j^a \qquad \forall j \in A \tag{22}$$

$$(8) - (19)$$

By solving SP, we obtain a feasible solution $(\hat{Y}, \hat{X})$ to the NPVDL and an upper bound to the problem. In addition, the new interdiction plan $\hat{\mathbf{X}}$ is used to generate an SVI, which is appended to the RMP in the next iteration. For a given $\hat{\mathbf{X}}$, the corresponding SVI is defined as:

$$SVI(\hat{\mathbf{X}}) : \sum_{i \in N} Y_i^n \hat{X}_i^n + \sum_{j \in A} Y_j^a \hat{X}_j^a \geq 1 \tag{23}$$

Inequality (23) simply states that to thwart an interdiction strategy, at least one element of that strategy must be protected.

The algorithm starts with an empty protection strategy and solves the SPs and the RMPs alternatively. The iterative process terminates when the RMP becomes infeasible, i.e., the available protection resources are insufficient to thwart all the interdiction strategies discovered up to that iteration. Given that protection resources are limited, the algorithm is guaranteed to converge to an optimal solution in a finite number of iterations.

5 Heuristic approach

To solve NPVDL efficiently, we propose a heuristic which consists of a greedy-based construction phase, followed by a Simulated Annealing algorithm. The heuristic, referred to as GSA-H, uses two auxiliary models. The first model, called $USER(\hat{\mathbf{X}})$, is the system user sub-model. It computes the system's value (i.e., the amount of disrupted flow) associated with a specific interdiction plan $\hat{\mathbf{X}}$.

$$\left[USER(\hat{\mathbf{X}})\right] \; z_{user}(\hat{\mathbf{X}}) = \max_{\mathbf{Z}} \sum_{s} \sum_{d} f_{sd} Z_{sd} \tag{24}$$

$$\text{s.t.} \quad (9) - (13)$$

$$\omega_r \geq 1 - \sum_{j \in A(r)} \hat{X}_j^a - \sum_{i \in N(r)} \hat{X}_i^n \qquad \forall s, d \in N, r \in N_{sd} \tag{25}$$

$$(17) - (19)$$

The second model, called $SP2(\hat{\mathbf{Y}})$, is a simplified version of $SP(\hat{\mathbf{Y}})$. This model assumes that the flow between two nodes is entirely lost only if all the paths connecting the two nodes are disrupted. If at least one path is available, independently on its length, all the flow is preserved. The mathematical formulation of $SP2(\hat{\mathbf{Y}})$, therefore, no longer requires the path variables S_r and ω_r and all the constraints associated with these variables. Also, the variables Z_{sd} are redefined as binary.

$$\left[SP2(\hat{\mathbf{Y}})\right] \quad z_{sp2}(\hat{\mathbf{Y}}) = \max_{\mathbf{X}} \sum_{s} \sum_{d} f_{sd} Z_{sd} \tag{26}$$

$$\text{s.t.} \quad (8)(15)(16)(21)(22)$$

$$Z_{sd} \leq \sum_{j \in A(r)} X_j^a + \sum_{i \in N(r)} X_i^n \qquad \forall s, d \in N, r \in N_{sd} \tag{27}$$

$$Z_{sd} \in \{0, 1\} \qquad \forall s, d \in N \tag{28}$$

Constraints (27) state that the flow between an origin s and a destination d is disrupted only if at least one element on each path connecting s and d is interdicted.

In the following sections, heuristic procedures will be identified by the letter H appended to the algorithms' acronyms.

5.1 Greedy construction phase

In the initial step of the heuristic, we estimate how *important* each element of the network is, from the *attacker* point of view. For the sake of clarity, in this section we will ignore the difference between nodes and arcs and we will refer to them as network elements, belonging to the set E. $\mathbf{X}$ and $\mathbf{Y}$ will represent the interdiction and protection variables, respectively. Also, the disruption and protection resource vectors $\mathbf{p^n}, \mathbf{p^a}, \mathbf{q^n}$ and $\mathbf{q^a}$ are merged into two vectors $\mathbf{p}$ and $\mathbf{q}$.

Let $\mathbf{i}$ be a vector such that $i_j = 1$ if $i = j$ and 0 otherwise. Namely, $\mathbf{i}$ is an interdiction strategy where only element $i \in E$ is interdicted. The *importance* ρ_i of element i is computed by first solving $USER(\mathbf{i})$ to obtain $z_{user}(\mathbf{i})$. This value is then weighted by the resources needed to disrupt i. Formally, $\rho_i = z_{user}(\mathbf{i})/p_i$. This parameter is used as an estimate of the likelihood that element i appears in an interdiction plan and, consequently, in a protection plan. Let us further define $\bar{E}$ as the set of disrupted elements in the optimal interdiction plan, obtained by solving $SP(\mathbf{Y^g})$, where $\mathbf{Y^g}$ is the protection plan built during the greedy phase.

The pseudo-code of the greedy construction algorithm (GC-H) is given below:

Algorithm 1 GC-H

$b = 0, \mathbf{Y^g} \leftarrow \mathbf{0}$
for $i = 1$ **to** T **do**
  Remove from E all elements $e : q_e > B - b$
  if E is empty **then**
    Solve $SP(\mathbf{Y^g})$ and set $obj_g = z_{sp}$
    return $\mathbf{Y^g}, obj_g$
  else
    $Y^g_{e'} = 1$ with $e' = argmax\{\rho_e : e \in E \text{ and } Y^g_e = 0\}$
    $b = b + q_{e'}$
  end if
end for
while $b \leq B$ **do**
  Solve $SP(Y^g)$ for $\bar{E}$ and set $obj_g = z_{sp}$
  Remove from $\bar{E}$ all elements $e : q_e > B - b$
  if $\bar{E}$ is empty **then**
    return $\mathbf{Y^g}, obj_g$
  else
    $Y^g_{e'} = 1$ with $e' \in \bar{E} : \rho_{e'} \geq \rho_e, \forall e \in \bar{E}$
    $b = b + q_{e'}$
  end if
end while
return $\mathbf{Y^g}, obj_g$

In the first stage of the algorithm (steps 2-11), the protection plan is initialized with the best T elements with respect to the importance parameter ρ. The exact value of T depends on the network size and protection budget. This stage does not require solving an $SP(\mathbf{Y^g})$ problem unless the set E of candidate elements is empty. In the following stage (steps 12-21), $SP(\mathbf{Y^g})$ is solved to identify the set $\bar{E}$ of interdicted components in response to the current protection plan $\mathbf{Y^g}$. From this set, the best element with respect to ρ, which does not violate the budget constraint, is selected and added to the protection plan. The process is iterated until no element can be added to the solution without violating the budget constraint.

5.2 Simulated Annealing

After the greedy initial solution is built, a standard Simulated Annealing procedure (Kirkpatrick, 1984) is used to explore the solution space in the attempt to find improving solutions. The pseudo-code of this algorithm, referred to as SA-H, is shown below.

Algorithm 2 SA-H

1: $obj_{sp} = obj^g, obj_{sp2} = obj^g, t = t_{in}$
2: $\mathbf{Y^{cur}} \leftarrow \mathbf{Y^g}, \mathbf{Y^{new}} \leftarrow \mathbf{0}, \mathbf{Y^{best}} \leftarrow \mathbf{Y^g}$
3: **while** $t > t_{end}$ **do**
4: $\quad \mathbf{Y^{new}} = Neighbour(\mathbf{Y^{cur}})$
5: $\quad$ Solve $SP2(\mathbf{Y^{new}})$ to obtain z_{sp2}
6: $\quad$ **if** $z_{sp2} \leq obj_{sp2}$ **then**
7: $\quad\quad$ Solve $SP(\mathbf{Y^{new}})$ to obtain z_{sp}
8: $\quad\quad$ **if** $z_{sp} < obj_{sp}$ **then**
9: $\quad\quad\quad \mathbf{Y^{best}} \leftarrow \mathbf{Y^{new}}$, $\mathbf{Y^{cur}} \leftarrow \mathbf{Y^{new}}$
10: $\quad\quad\quad obj_{sp2} = z_{sp2}$, $obj_{sp} = z_{sp}$, $t = t * cr$
11: $\quad\quad$ **else**
12: $\quad\quad\quad \Delta = (z_{sp} - obj_{sp})/obj_{sp}$
13: $\quad\quad\quad$ **if** $e^{-\Delta/t} \geq rand(0,1)$ **then**
14: $\quad\quad\quad\quad \mathbf{Y^{cur}} \leftarrow \mathbf{Y^{new}}$, $t = t * cr$
15: $\quad\quad\quad$ **end if**
16: $\quad\quad$ **end if**
17: $\quad$ **end if**
18: **end while**
19: return $\mathbf{Y^{best}}, obj_{sp}$

The starting solution of the procedure SA-H is initialized with the greedy solution. At each iteration, a new solution is generated by exploring the neighbourhood of $\mathbf{Y^{cur}}$ through the routine *Neighbour*. In order to efficiently evaluate the objective values of new solutions, we first solve the model $SP2$, which is significantly easier to solve than SP and may provide an indication of the quality of the new protection plan. If the new solution to $SP2$ improves

the best solution found for $SP2$ (from the defender perspective), then there are good chances that the same solution may improve SP as well. Otherwise, the problem SP is not solved and another solution in the neighbour is generated. This expedient reduces the number of times that SP is solved and, consequently, the overall computing time of the algorithm. If the new solution ($\mathbf{Y^{new}}$) generated by the *Neighbour* routine improves the best solution, then both the current and the best solutions are updated (9-10). If the new solution is not improving, the current solution is still updated to the new one if condition (13) is met ($rand(0,1)$ generates a random number between 0 and 1). Every time the current solution is updated, the temperature t is cooled by a fixed rate cr. The procedure ends as soon as the temperature drops below a pre-specified value t_{end}.

The pseudo-code for the *Neighbour* routine is displayed below.

Algorithm 3 $Neighbour(\mathbf{Y})$

1: $b = \sum_{e \in E} q_e Y_e$
2: e^{out} is randomly selected from all elements $e \in E : \rho_e < \rho^H \wedge Y_e = 1$
3: $Y_{e^{out}} = 0$
4: $b = b - q_{e^{out}}$
5: **while** $b < B$ **do**
6: Solve $SP2(\mathbf{Y})$ to obtain $\bar{E}$
7: Remove from $\bar{E}$ all elements $e : q_e > B - b \vee \rho_e > \rho^L$
8: **if** $\bar{E}$ is empty **then**
9: return $\mathbf{Y}$
10: **else**
11: e^{in} is randomly selected from $\bar{E}$
12: $Y_{e^{in}} = 1$
13: $b = b + q_{e^{in}}$
14: **end if**
15: **end while**
16: return $\mathbf{Y}$

This routine computes a random one-to-many swap move. Only feasible swaps with respect to the budget constraint are considered. To improve the accuracy of the search phase, we restrict the set of elements that can be swapped out, by only considering those elements e with an importance factor less than a given threshold ρ^H ($\rho_e < \rho^H$). Similarly, we use a parameter ρ^L to reduce the number of elements that can be swapped in. The specific values of ρ^H and ρ^L will be defined in the next section. Note that the set of candidate elements to enter the solution is generated by solving $SP2(\mathbf{Y})$. This set ($\bar{E}$) contains the disrupted elements in the optimal interdiction plan obtained by solving the simplified interdiction problem.

6 Results and analysis

In this section, the two solution approaches SVI-D and the Greedy construction followed by the Simulated Annealing (GSA-H) are tested and compared on some randomly generated instances.

6.1 Data sets and problem parameters

We evaluate the algorithms' performances on a set of undirected networks of different size. We call the networks n-x, where n denotes the number of nodes and x is used to differentiate networks of same size. We consider three different network sizes: 16, 25 and 36. For each size, 5 instances are generated. The steps followed to build the instances are highlighted below:

- n nodes are generated with coordinates drawn randomly in $[0, 50]$
- Euclidean distances between nodes are used to set the link lengths (c_j) and the protection costs (q_j^a).
- Each node can not be directly connected to nodes whose Euclidean distance is larger than 20. With this logic, a set of candidate connections is built for each node.
- We consider nodes with degree (i.e., number of incident edges) equal to 2, 3 and 4, and set loose targets on the number of nodes with a given degree. Namely, between 10% and 30% of nodes must have degree $\delta = 2$, between 40% and 50%, $\delta = 3$, and between 20% and 40%, $\delta = 4$. Links are randomly selected from the candidate connection sets and added to the network as long as the upper degree targets are not violated. Links are generated until all the lower degree targets are satisfied. Note that by allowing flexibility in the percentage of nodes with a given degree, we could always generate connected networks. On the contrary, by using a fixed distance threshold to limit possible connections and imposing fixed degree targets, we could not always guarantee the connectivity of the resulting networks. In addition, the use of soft targets allowed us to generate instances with different shapes and complexity, thus making the result analysis more comprehensive.
- The cost p_j^a of disrupting any arc is set to 1. Tracks, in fact, are highly vulnerable and easy to disrupt because of their length and the presence of accessible and easily attackable structures (overpasses, bridges, tunnels).

– Nodes' degrees are used to categorize stations as small ($\delta = 2$), medium ($\delta = 3$) and big ($\delta = 4$). This classification is further used to set other problem parameters as shown in Table 1. For instance, a medium station requires 10 units of resources to be fully protected and 4 units to be disrupted. The population (*pop*) of the area surrounding a station is generated uniformly in the interval $[1, 10]$. This number is then multiplied by 10 for medium stations and by 100 for big stations. The resulting number can be interpreted as *thousands* of inhabitants.

– The flow matrix is built using a simple gravity model. Formally, $f_{sd} = pop_s pop_d / e_{sd}^2$, where p_s (p_d) is the population of node s (node d), and e_{sd} is the Euclidean distance between s and d.

– The disruption budget, P, is initially chosen to be equal to 6. This indicates that a disruption can disable a big station, 6 different links, or a combination of smaller assets (e.g., one small station and 4 links).

– The protection budget B is defined as a percentage of the budget $\mathcal{T}$ needed to protect the entire network, i.e. $B = Q\mathcal{T}$. We initially consider values of Q equal to 15% and 20%. To guarantee B integrality, we round it to the nearest integer.

	$\delta = 2$	$\delta = 3$	$\delta = 4$
Size	Small	Medium	Big
q_i^n	5	10	15
p_i^n	2	4	6
pop	$U(1, 10)$	$U(1, 10) * 10$	$U(1, 10) * 100$

Table 1: Stations' parameters.

As in Starita and Scaparra (2016), the set of paths N_{sd} connecting each pair of nodes s and d is computed in a preprocessing phase. Namely, for each node pair, the shortest path is computed by solving an LP formulation of the shortest path problem, and added to the path set. A constraint is then added to the LP to prevent the generation of that path again. The problem is then resolved to generate the next shortest path. The procedure is iterated until the newly generated path r becomes excessively long (i.e., α_r is equal to zero).

Finally, the values of the parameters used to model the traveler behaviour, α_r, are given in Table 2. For each origin-destination pair, we use 4 different values which depend on the shortest path length increase. For instance, if the shortest path r connecting two nodes after a disruption is less than 20% longer than the shortest path connecting the two nodes before the disruption, then all the passenger demand is preserved ($\alpha_r = 1$). In contrast, an increase

of the shortest path length by over 100% (i.e., the new shortest path is more than twice as long as the initial shortest path) results in the loss of the entire demand ($\alpha_r = 0$).

Length increment	$\leq 20\%$	$> 20\%$ and $\leq 50\%$	$> 50\%$ and $\leq 100\%$	$> 100\%$
α_r	1	0.5	0.1	0

Table 2: Values of α_r as a function of the shortest path length increase.

6.2 Solution algorithms' setting

Both the exact and heuristic approaches are implemented using Cplex 12.6 embedded in a C++ program. Tests were run on a computer with 2.7 GHz i5 6400 quad-core processor and 8GB of RAM. The SVI-D algorithm uses Cplex default parameters. We enforce a time limit of $10,000$ seconds for its execution. The values of the parameters used by GSA-H were chosen empirically after some preliminary tests. Their setting is as follows:

- $t_{in} = 100$.
- $t_{end} = 0.01$.
- $cr = 0.93$.
- ρ^H is the T^{th} highest value of ρ.
- ρ^L is chosen such that $|E^L| = |E|/4$, where $E^L = \left\{i \in E : \rho_i < \rho^L\right\}$.

The values of T, shown in Table 3, were chosen empirically. These values depend on the network size and the protection budget. For example, for the 25-x networks and with a 15% budget, $\mathbf{Y^g}$ is initialized with the first 3 best elements.

	Network name		
Q	16-x	25-x	36-x
15%	2	3	8
20%	4	6	14

Table 3: Values of T for each combination of network size and protection budget values.

6.3 Performance comparison

In Table 4 and Table 5 we compare the performance of SVI-D and GSA-H for two protection budget levels: 15% and 20%, respectively. For both algorithms, the tables list the objective

values and the computing times. The gap column shows the percentage error of the GSA-H solutions compared with the SVI-D solutions. For the heuristic approach, we also show the execution time of the algorithm.

		SVI-D		GSA-H				
Network name	Number of arcs	Objective value	Computing time(s)	Objective value (AVG)	Objective value(Best)	Gap (AVG)	Gap (Best)	Computing time(s) (AVG)
16-1	19	10798.5	1.5	10799.7	10798.5	0.0%	0.0%	1.4
16-2	21	125426.0	4.9	125960.0	125960.0	0.4%	0.4%	2.9
16-3	22	103072.0	2.3	103666.1	103072.0	0.6%	0.0%	4.1
16-4	24	976164.0	1.2	976164.0	976164.0	0.0%	0.0%	3.6
16-5	22	82266.5	5.1	82266.5	82266.5	0.0%	0.0%	4.6
25-1	36	91479.6	9.5	91479.6	91479.6	0.0%	0.0%	7.2
25-2	43	8514070.0	48.1	8514070.0	8514070.0	0.0%	0.0%	25.3
25-3	39	912132.0	115.2	912132.0	912132.0	0.0%	0.0%	59.5
25-4	42	2620880.0	144.8	2644080.0	2644080.0	0.9%	0.9%	34.6
25-5	37	879881.0	60.0	879881.0	879881.0	0.0%	0.0%	15.2
36-1	61	6200620.0	1152.1	6200620.0	6200620.0	0.0%	0.0%	138.9
36-2	62	7192520.0°	10000	7192520.0	7192520.0	0.0%	0.0%	182.2
36-3	62	5085400.0°	10000	4858400.0	4772240.0	-4.5%	-6.2%	288.8
36-4	58	3787020.0	8091.4	3880475.0	3791880.0	2.5%	0.1%	196.2
36-5	60	3941680.0°	10000	3847340.0	3847340.0	-2.4%	-2.4%	228.2
AVG		2701560.6	2642.4	2687990.3	2676300.2	0.3%†	0.1%†	79.5

° Objective value obtained after 10,000 sec.

† The average is computed excluding the cases where the gaps are negative.

Table 4: Computational results ($Q = 15\%$ and $P = 6$)

		SVI-D		GSA-H				
Network name	Number of arcs	Objective value	Computing time(s)	Objective value (AVG)	Objective value(Best)	Gap (AVG)	Gap (Best)	Computing time(s) (AVG)
16-1	19	9256.7	3.0	9261.4	9256.7	0.1%	0.0%	1.6
16-2	21	67021.8	7.2	67021.8	67021.8	0.0%	0.0%	2.1
16-3	22	86701.4	4.3	86701.4	86701.4	0.0%	0.0%	5.7
16-4	24	430400.0	2.6	432855.8	430400.0	0.6%	0.0%	2.6
16-5	22	72928.5	7.4	72928.5	72928.5	0.0%	0.0%	4.2
25-1	36	74847.7	23.9	75364.6	74847.7	0.7%	0.0%	6.5
25-2	43	6206390.0	170.5	6206390.0	6206390.0	0.0%	0.0%	26.9
25-3	39	725125.0	224.3	725125.0	725125.0	0.0%	0.0%	59.0
25-4	42	2029260.0	270.7	2029260.0	2029260.0	0.0%	0.0%	32.6
25-5	37	553016.0	190.9	553016.0	553016.0	0.0%	0.0%	14.7
36-1	61	5758590.0	1876.8	5758590.0	5758590.0	0.0%	0.0%	152.8
36-2	62	6035350.0°	10000	5282835.0	5221890.0	-12.5%	-13.5%	152.9
36-3	62	4814590.0°	10000	3714470.0	3714470.0	-22.8%	-22.8%	349.2
36-4	58	3391630.0°	10000	3188382.5	2937520.0	-6.0%	-13.4%	168.1
36-5	60	3719340.0°	10000	3179980.0	3179980.0	-14.5%	-14.5%	236.6
AVG		2264963.1	2852.1	2092145.5	2071159.8	0.1%†	0.0%†	81.0

° Objective value obtained after 10,000 sec.
† The average is computed excluding the cases where the gaps are negative.

Table 5: Computational results ($Q = 20\%$ and $P = 6$)

The analysis of the tables shows that SVI-D is able to solve to optimality only small and medium problem instances. Within the time allowed, the algorithm does not converge in 7 out of the 10 large instances (networks 36-x). For these instances, the solutions found by the heuristic in a fraction of the time are always superior (in a case more than 20% better). GSA-H is able to identify 9 out of the 12 proven optimal solutions for $Q = 15\%$, and all the proven optimal solutions for $Q = 20\%$. Unlike the exact method, the execution time and the solution quality of the heuristic are not affected by the budget amount. In addition, the quality of the solutions is fairly good across all the iterations, with an iteration average gap (excluding negative gaps) equal to 0.3% when $Q = 15\%$ and 0.1% when $Q = 20\%$. The efficiency of GSA-H in solving these problems is largely due to the use of the auxiliary problem SP2. Solving this problem, in fact, is computationally much easier than solving SP (80% faster on average). The solutions obtained by solving SP2 are often good approximations of the solutions to SP, although there are cases where the objectives of the two problems' optimal solutions differ by as much as 32%.

Overall, GSA-H seems to be both accurate and scalable. In the next section, we will show that this heuristic algorithm can be successfully used to identify cost-efficient protection plans for an even larger, real-size network.

7 Case study

In this section, we present a case study on the Central London Tube. Some of the findings emerging from the case study's analysis are then validated using the random instances presented in the previous section.

The map of the central portion of the London Tube is displayed in Fig. 1. The corresponding network is made of 51 nodes and 70 undirected arcs.

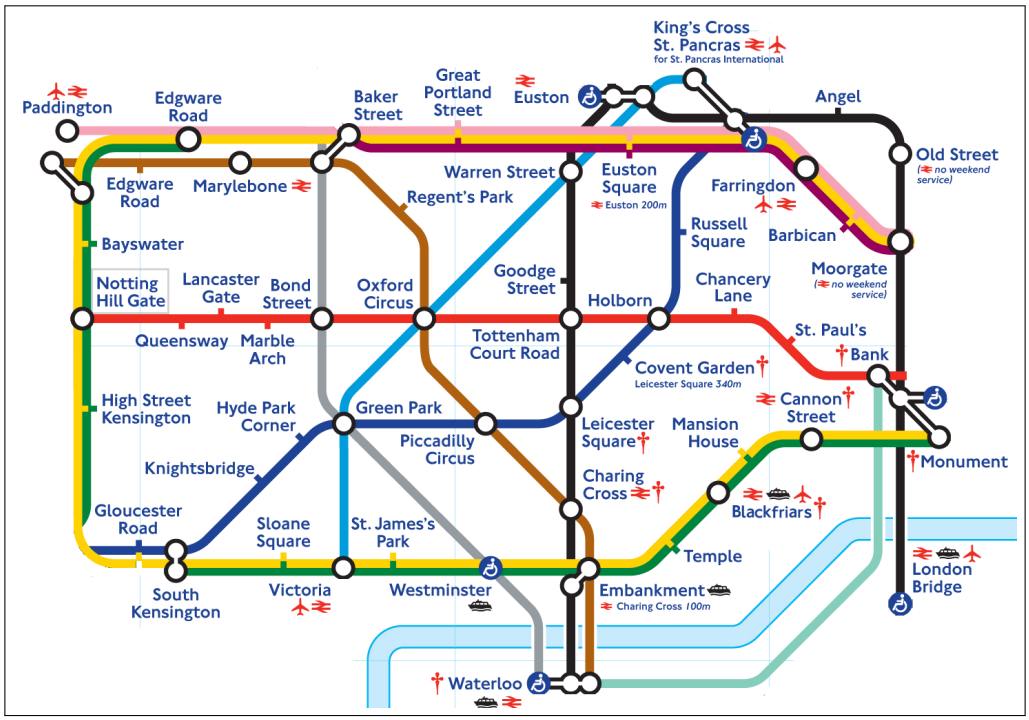


Figure 1: Central London tube map

To set the parameters of the problem, we use the open data available on the Transport For London website (TFL) (www.tfl.gov.uk/info-for/open-data-users). We use the running time between two directly connected stations to set the nominal cost of each arc, which is then used for computing the paths' length. The length of each path includes a 10-minute delay for each line change along the path. The physical distance of a connection is used to estimate its protection cost. This choice is motivated by the fact that typical protection strategies, such as digging draining pits, fortifying water pipes and sewers, and installing video surveillance, are all dependent on the length of the link. TFL also provides information regarding the flow from all the origins to all the destinations. This is used to build the demand matrix. We categorize the stations into three groups based on their sizes: small ($p_i^n = 2$), medium ($p_i^n = 4$) and big ($p_i^n = 6$). The annual flow of passengers is used to identify the category of each station. Namely, a station is *small* if the amount of annual passengers going through

it is less than 25 millions, *medium* if it is between 25 and 50 millions, *big* otherwise. The rest of the parameters are set as explained in the previous section. We analyse different scenarios which vary in terms of protection budget $(0\%, 5\%, 10\%, 15\%, 20\%)$ and amount of disruption resources $(1, 2, 3, 4, 5, 6)$. Algorithm GSA-H is used to solve the problem, if not stated otherwise.

7.1 Impact of the protection budget on the flow loss

The impact of different protection budget levels on the system worst-case flow loss is displayed in Fig. 2. The analysis is performed for six scenarios, which differ in terms of the disruption magnitude, defined by the parameter P.

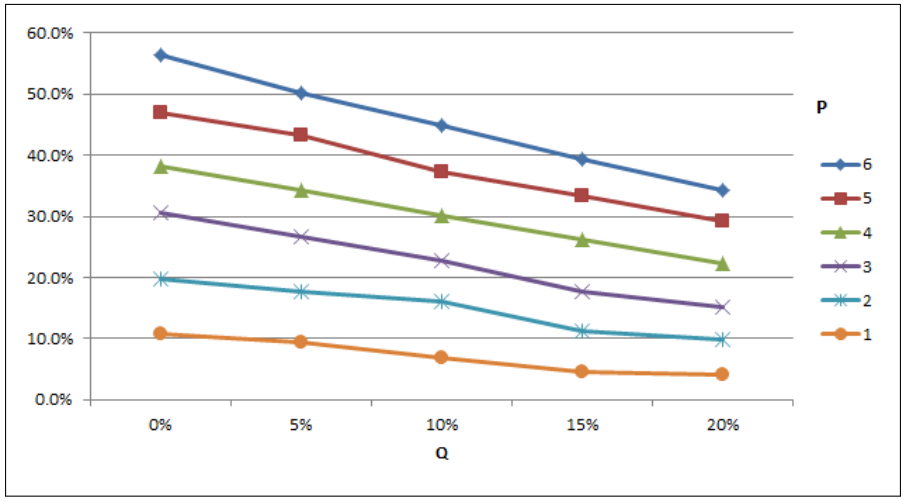


Figure 2: Flow loss for different budget levels and disruption scenarios (London Tube)

Clearly, increasing the protection resources from 0% to 20% can reduce the worst-case flow loss quite significantly, in every disruption scenario. For the largest disruption scenario ($P = 6$), the flow loss drops from more than 56% to about 34%. This means that, without any protection, a *large* disruption can potentially affect more than half of the entire traffic on the network. If 20% of the network is protected in a cost-efficient way, then the worst-case scenario flow loss drops to about one third of the total flow. Generally, all the budget increments prove to have a beneficial impact on the demand losses, although the marginal benefit due to the last increment decreases for small disruption scenarios (i.e., P = 1).

Network	$Q = 0\%$	$Q = 20\%$
16-1	94%	30%
16-2	91%	37%
16-3	82%	37%
16-4	94%	20%
16-5	76%	46%
25-1	95%	23%
25-2	85%	7%
25-3	60%	45%
25-4	70%	20%
25-5	96%	11%
36-1	72%	16%
36-2	64%	15%
36-3	63%	17%
36-4	50%	14%
36-5	55%	13%
AVG	76%	23%

Table 6: Flow loss with no protection and with 20% protection for P = 6 (Random instances)

The impact of protection is even more pronounced when the random instances are considered. For each random instance, Table 6 displays the demand loss when the network is completely unprotected and when 20% of the network is protected, for P = 6. The results highlight that these networks, especially the small ones, are highly vulnerable to disruptions: up to 95% of the flow (76% on average) can be disrupted without protection when only a few assets are disabled. However, a cost efficient protection plan can significantly mitigate the impact of disruption, reducing the flow loss to 23% on average.

7.2 Protection plans analysis

In this section, we analyse the Tube protection plans identified by the model in different scenarios. We consider the same six disruption scenarios used in the previous section and four protection budget levels $(5\%, 10\%, 15\%, 20\%)$. Tables 7 and 8 show the most frequently protected nodes and links of the network across the 24 scenarios.

Station	No. of protections
Westminster	18
Notting Hill	16
St. Paul's	10
Chancery Lane	9
Moorgate	9
Old Street	8
Marble Arch	7
Lancaster Gate	6
Bank/Monument	5
Holborn	3

Table 7: Frequency of protections for stations

Link	No. of protections
Holborn-Tottenham Court Road	24
Chancery Lane-St. Pauls's	24
Bank/Monument-St. Pauls's	24
Bond Street-Mable Arch	23
Chancery Lane-Holborn	23
Oxford Circus-Tottenham Court Road	21
Lancaster Gate-Marble Arch	19
Bond Street-Oxford Circus	19
Notting Hill-Queensway	18
Queensway-Lancaster Gate	18

Table 8: Frequency of protections for links

Table 8 shows that some key links (the first three) appear in every single protection plan. This is a clear evidence of how critical these assets are for the network: independently on the disruption scenario and available protection resources, these links must be protected to minimize the system's losses in case of disruption. Among the stations, Westminster and Notting Hill are clearly the most critical: they are protected in 18 and 16 out of the 24 cases, respectively (Table 7).

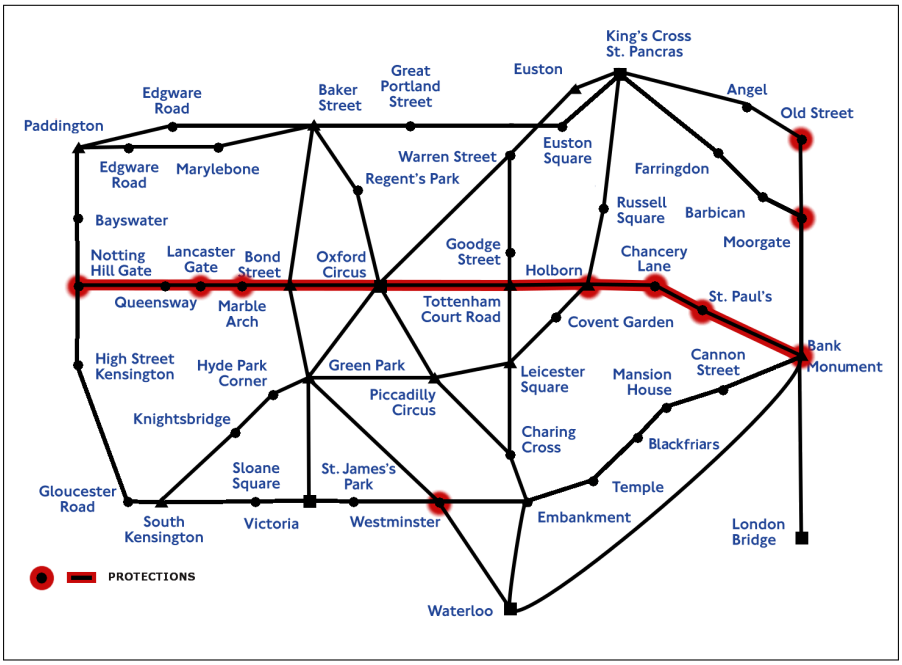
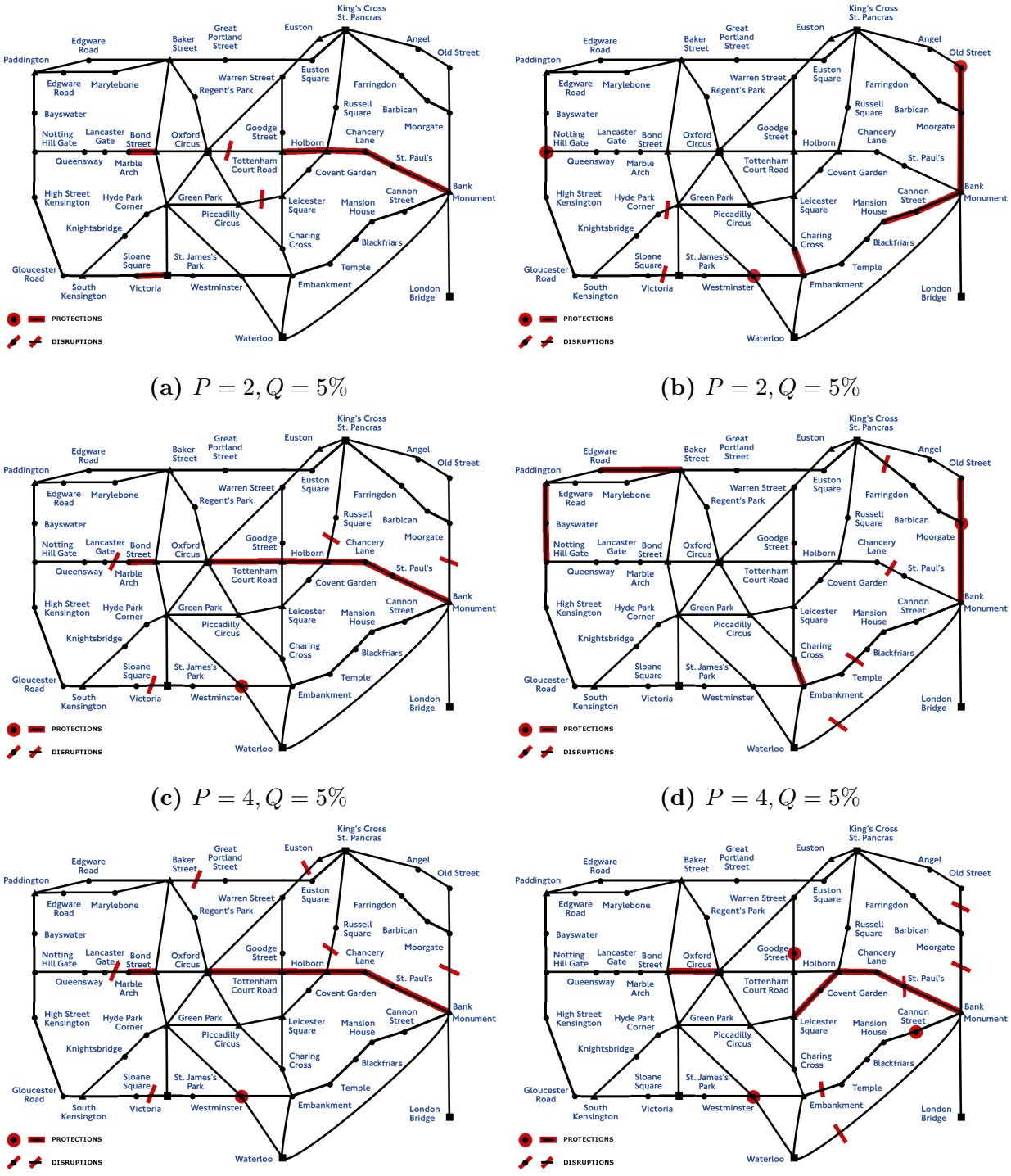


Figure 3: Most frequently protected elements

In Fig. 3 the most frequently protected elements of the network are highlighted. Circles, triangles and squares represent small, medium and big stations, respectively. The figure shows a clear pattern in the protection. All the protected arcs and most of the protected nodes belong to the Central line. This is a plausible result, considering that the Central line is the busiest tube line, with over 260 million annual passengers.

7.3 The importance of considering variable post-disruption demand

To prove the importance of modeling the passenger (user) behaviour in an accurate way when planning protection efforts, we propose a comparison between the solutions obtained with NPVDL and the solutions obtained with the model introduced by Scaparra et al. (2015). We refer to this model as the Network Protection Problem with Constant Demand Loss (NPCDL). Although NPCDL and NPVDL use the same metric to evaluate the impact of a disruption (i.e., the demand loss), the passenger behaviour in NPCDL is modeled in a much more simplistic way by simply discarding, in a pre-computational step, paths that exceeds a given threshold. In the following analysis, we firstly focus on the London Tube. We consider two threshold values to define the acceptable paths: 2 (meaning that a path twice as long as the shortest path or less is considered acceptable) and 1.5 (meaning that a path up to 50% longer than the shortest path is considered acceptable).



(a) $P = 2, Q = 5\%$

(b) $P = 2, Q = 5\%$

(c) $P = 4, Q = 5\%$

(d) $P = 4, Q = 5\%$

(e) $P = 6, Q = 5\%$

(f) $P = 6, Q = 5\%$

Figure 4: Optimal protection plans and post-protection interdictions for NPVDL and NPCDL (London Tube)

In Fig. 4, we display the optimal protection plans and the post-protection, worst-case interdictions identified by the two models (NPVDL and NPCDL with threshold 2) for three

different disruption scenarios ($P = 2, 4, 6$). The optimal solutions were computed by using SVI-D for both problems. For the sake of clarity, this figure displays the results for a protection budget level equal to 5% (protection plans involving fewer elements can be better visualized in the pictures). The pictures in the left column (4a, 4c, 4e) show the NPVDL solutions, whereas the pictures in the right column (4b, 4d, 4f) show the NPCDL solutions. It is evident that the solutions identified by the two models differ quite significantly, both in terms of protected elements and in terms of post-protection, worst-case disruptions. For example, when $P = 2$ and $P = 4$ the protection plans are completely different. Substantial differences were also noted for other values of the parameter Q.

To evaluate the impact that overlooking the user behaviour may have on the evaluation of worst-case demand losses, we use the optimal protection plans identified by NPCDL to compute the worst-case losses in our modelling framework (i.e., when the post-disruption passenger demand varies with the extent of the travel delay according to the pattern of α_r values in Table 2). Note that for budgets larger than 5%, the problems were solved with GSA-H. As noted in the previous section, in fact, the performance of SVI-D deteriorates when the budget increases and the instances with a budget exceeding 5% could not be solved by the exact approach. Table 9 displays the percentage objective function (demand loss) increase for different disruption scenarios and protection budget levels, when the threshold is equal to 2 and 1.5, respectively.

By observing the table, it can be noticed that the solutions found by NPCDL are strongly suboptimal, especially for large values of Q and small disruptions. In this case study, the demand loss increase for both threshold values can be as high as 153% when $Q = 20\%$ and $P = 1$. Although the increase is less substantial for other combinations of the parameters P and Q, in all cases but two, solving the more simplistic NPCDL model results in a misestimation of the real worst-case scenario losses in case of disruption. Note that the negative increase in Table 9, observed when $P = 3$, $Q = 5\%$ and threshold is 1.5, is due to the fact that the heuristic solution to the NPVDL is not the optimal one.

	Threshold=2				Threshold=1.5			
	Q							
P	5%	10%	15%	20%	5%	10%	15%	20%
1	16%	57%	129%	153%	16%	59%	139%	153%
2	12%	12%	58%	71%	11%	10%	49%	85%
3	14%	19%	38%	56%	−1%	16%	48%	99%
4	11%	19%	32%	51%	1%	15%	30%	24%
5	6%	12%	3%	8%	4%	2%	21%	8%
6	4%	9%	7%	16%	0%	5%	11%	16%
AVG	11%	21%	45%	59%	5%	18%	50%	64%

Table 9: Demand loss increase when using NPCDL with threshold 2 and 1.5 (London Tube)

This finding is corroborated by performing the same analysis on the random instances. Average results over the 15 random instances are displayed in Table 10. Even for these instances, worse-case scenario losses can be significantly under-estimated when using NPCDL.

	Threshold=2				Threshold=1.5			
	Q							
P	5%	10%	15%	20%	5%	10%	15%	20%
1	28%	80%	214%	345%	21%	31%	113%	229%
2	59%	161%	289%	631%	46%	142%	254%	564%
3	57%	172%	303%	72%	3%	8%	26%	367%
4	7%	19%	28%	181%	2%	7%	18%	143%
5	21%	61%	19%	155%	17%	53%	10%	15%
6	2%	39%	12%	77%	0%	1%	3%	44%
AVG	29%	89%	144%	244%	15%	40%	71%	227%

Table 10: Average demand loss increase when using NPCDL with threshold 2 and 1.5 (Random instances)

These results show empirically that failure to accurately represent the passenger behaviour into a modeling framework may lead to highly sub-optimal protection strategies, where limited protection resources are not allocated in a cost-effective way.

7.4 Solution analysis with a less delay-sensitive passenger behaviour

In the previous section, we have demonstrated that considering the passenger behaviour is crucial to identify sound protection strategies. In this section, we analyse the sensitivity of our solutions to different values of the parameter α_r, used to capture the passenger behaviour. To this end, we run a new set of experiments where the values of α_r have been changed to the values shown in Tab. 11.

Length increment	$\leq 40\%$	$> 40\%$ and $\leq 70\%$	$> 70\%$ and $\leq 100\%$	$> 100\%$
α_r	1	0.5	0.1	0

Table 11: New values of α as a function of the shortest path increase.

These values indicate that passengers are willing to accept longer travel delays, as compared to the ones used in the previous analysis. For instance, a travel time increase up to 40% does not cause any flow loss, whereas previously a 40% increment would have led to the loss of 50% of the flow.

Tables 12 and 13 show the most frequently protected stations and links, across all the proposed scenarios.

Station	No. of protections
Westminster	15
Notting Hill	15
Old Street	10
Chancery Lane	9
St. Paul's	9
Marble Arch	8
Moorgate	7
Lancaster Gate	6
Bank/Monument	4
Holborn	3

Table 12: Frequency of protections for stations, with new α values.

Link	No. of protections
Bond Street-Mable Arch	24
Chancery Lane-Holborn	24
Chancery Lane-St. Pauls's	22
Holborn-Tottenham Court Road	22
Bank/Monument-St. Pauls's	20
Lancaster Gate-Marble Arch	20
Oxford Circus-Tottenham Court Road	18
Notting Hill-Queensway	18
Queensway-Lancaster Gate	18
Bond Street-Oxford Circus	14

Table 13: Frequency of protections for links, with new α values.

Changing α has an obvious impact on the objective function. There is, in fact, an average 4.4% decrease in the flow loss. Nonetheless, it seems that the protection plans have not changed significantly. Tables 12 and 13 show the same patterns highlighted by Tables 7 and

8. No new element appears in the protection plans and there are only small variations in the frequency of the protected elements. This suggests that, for this particular case, the solutions identified by our model are quite robust to variations of the parameter α. As mentioned in the introduction, estimates of this parameter can be obtained by surveying a sample of the railway system users. A small misestimation of this figure should not have a major impact on the protection strategies identified by the model.

8 Conclusions and future work

In this paper we introduce a new modelling approach for increasing the reliability and security of flow-based networks. Our focus is on passenger railway systems. The proposed approach overcomes some of the limitations of pre-existing models, by capturing the user behaviour in a post-disruption period. Specifically, our model assumes that the demand for service after a disruption depends upon the extent of travel delay of each origin-destination route on the network. Results show that failing to consider the user behaviour may lead to sub-optimal protection plans and an underestimation of disruption consequences.

The inclusion of the post-disruption user behaviour into a mathematical model significantly increases the model complexity and tractability. To identify optimal or near-optimal solutions to the problem, we developed a heuristic solution approach consisting of a greedy construction phase followed by a Simulated Annealing procedure. We also implemented an exact decomposition algorithm based on the concept of Super-Valid Inequalities. Computational tests on some randomly generated networks show that the exact method, although useful to assess the accuracy of the heuristic on small problems, can only tackle networks of modest size. In contrast, the heuristic proves to be both efficient and effective in identifying high quality solutions. The application of the modelling approach to a real rail network (the London tube) provides a practical demonstration of how limited protection resources can be allocated in a cost-efficient way among the most vulnerable assets of a rail system. It also highlights how some key elements must be protected in every disruption scenario to achieve high level of network security. Finally, the case study highlights the fact that neglecting the post-disruption user behaviour may lead to the identification of highly inefficient protection strategies, with worst-case disruption losses 150% higher than those obtained with our model.

Interesting extensions to this work include the introduction of some stochastic elements in the modelling approach so as to allow relaxation of the assumption that interdictions and protections are always successful. Furthermore, our model assumes that the attacker has perfect knowledge of the infrastructure. Stochastic models could also be used to relax this assumption. New models could also be developed to protect infrastructure systems against

both man-made and natural disasters. In the latter case, scenario-indexed models may be more suitable to capture the randomness and likelihood of disruptive events. Another interesting line of research for the future would be the development of similar models for optimising the protection of road networks in addition to rail networks. This would require taking into consideration complex issues such as traffic equilibrium, link congestion and the user imperfect perception of the state of the network (He and Liu, 2012). Extending our model to capture these additional aspects would undoubtedly make the problem more difficult to solve. Therefore, future research should also be directed towards developing some novel and efficient solution approaches.

References

Akgun I., Gumubuga F., and Tansel B. (2015). Risk based facility location by using fault tree analysis in disaster management. *Omega* **52**, 168–179.

Aksen D., Piyade N., Aras N. (2010) The budget constrained r-interdiction median problem with capacity expansion. *Central European Journal of Operations Research* **18(3)**, 269–291.

Aksen D., Akca S., and Aras N. (2014). A bilevel partial interdiction problem with capacitated facilities and demand outsourcing. *Computers & Operations Research* **41**, 346–358.

Azad N., Hassini E., and Verma M. (2016). Disruption risk management in railroad networks: An optimization-based methodology and a case study. *Transportation Research Part B: Methodological* **85**, 70-88.

Balinski M. L.(1965). Integer programming: methods, uses, computations. *Management Science* **12(3)**, 253–313.

Bayrak H., Bailey M. D.(2008) Shortest path network interdiction with asymmetric information. *Networks* **52(3)**, 133–140.

Berman O., Krass D., and Menezes M. B. (2007). Facility reliability issues in network p-median problems: strategic centralization and co-location effects. *Operations Research* **55(2)**, 332–350.

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

Chen Q., Li X., Ouyang Y. (2011). Joint inventory-location problem under the risk of probabilistic facility disruptions. *Transportation Research Part B: Methodological* **45(7)**, 991–1003.

Church R. L., Scaparra M. P., Middleton R. S. (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers* **94**, 491–502.

Church R. L., Scaparra M. P. (2007) Protecting Critical Assets: The r-Interdiction Median Problem with Fortification. *Geographical Analysis* **39(2)**, 129–146.

Cormican K. J., Morton D. P., Wood R. K. (1998) Stochastic network interdiction. *Operations Research* **46(2)**, 184–197.

Council Directive 114/EC (2008). On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF*

Cui T., Ouyang Y., and Shen Z. J. M. (2010). Reliable facility location design under the risk of disruptions. *Operations Research* **58**, 998–1011.

Desai J., and Sen S. (2010). A global optimization algorithm for reliable network design. *European Journal of Operational Research* **200(1)**, 1–8.

Fiumara F. (2015). The Railway Security: Methodologies and Instruments for Protecting a Critical Infrastructure. In *Railway Infrastructure Security*, 25–63. Setola, Sforza, Vittorini, Pragliola Eds. Springer.

Fulkerson D. R., Harding G. C. (1977) Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming* **13(1)**, 116–118.

García-Archilla B., Lozano A. J., Mesa J. A., and Perea F. (2013). GRASP algorithms for the robust railway network design problem. *Journal of Heuristics* **19(2)**, 399–422.

Gong J., Mitchell J. E., Krishnamurthy A., and Wallace W. A. (2014). An interdependent layered network model for a resilient supply chain. *Omega* **46**, 104–116.

Hakimi S. L. (1964). Optimum locations of switching centers and the absolute centers and medians of a graph. *Operations Research* **12(3)**, 450–459.

Hakimi S. L. (1965). Optimum distribution of switching centers in a communication network and some related graph theoretic problems. *Operations Research* **13(3)**, 462–475.

He X., and Liu H. X. (2012). Modeling the day-to-day traffic evolution process after an unexpected network disruption. *Transportation Research Part B: Methodological* **46(1)**, 50–71.

H.R. 3162. (2001) Patriot Act. An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. Available at *http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf*

Israeli E., Wood R. K. (2002) Shortest path network interdiction. *Networks* **40(2)**, 97–111.

Jin J. G., Lu L., Sun L., and Yin, J. (2015) Optimal allocation of protective resources in urban rail transit networks against intentional attacks. *Transportation Research Part E: Logistics and Transportation Review* **84**, 73-87.

Khaled A. A., Jin M., Clarke D. B., and Hoque M. A. (2015) Train design and routing optimization for evaluating criticality of freight railroad infrastructures. *Transportation Research Part B: Methodological* **71**, 71–84.

Kirkpatrick S. (1984). Optimization by simulated annealing: Quantitative studies. *Journal of statistical physics* **34(5-6)**, 975–986.

Laporte G., Mesa J. A., Perea F. (2010) A game theoretic framework for the robust railway transit network design problem. *Transportation Research Part B: Methodological* **44(4)**, 447–459.

Li X., and Ouyang Y. (2010). A continuum approximation approach to reliable facility location design under correlated probabilistic disruptions. *Transportation Research Part B: methodological*, **44(4)**, 535–548.

Liberatore F., Scaparra M. P., Daskin M. S. (2011) Analysis of facility protection strategies against an uncertain number of attacks: the stochastic R-interdiction median problem with fortification. *Computers & Operations Research* **38(1)**, 357–366.

Liberatore, F., Scaparra, M. P., Daskin, M. S. (2012). Hedging against disruptions with ripple effects in location analysis. *Omega* **40(1)**, 21–30.

Lim C., Smith J. C. (2007) Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions* **39(1)**, 15–26.

Losada C., Scaparra M. P., Church R. L., Daskin M. (2012a) The stochastic interdiction median problem with disruption intensity levels. *Annals of Operations Research* **201(1)**, 345–365.

Losada C., Scaparra M. P., O'Hanley J. R. (2012). Optimizing system resilience: a facility protection model with recovery time. *European Journal of Operational Research* **217(3)**, 519–530.

Matisziw T. C., Murray A. T. (2009) Modeling *st* path availability to support disaster vulnerability assessment of network infrastructure. *Computers & Operations Research* **36(1)**, 16–26.

Milmo D. Copper thefts from railways escalating out of control, warns union leader. Available at *http://www.theguardian.com/uk/2011/sep/30/copper-thefts-rail-delays-bob-crow*

Murray A. T., Matisziw T. C., Grubesic T. H. (2007) Critical network infrastructure analysis: interdiction and system flow. *Journal of Geographical Systems* **9(2)**, 103–117.

Myung Y. S., Kim H. J. (2004) A cutting plane algorithm for computing k-edge survivability of a network. *European Journal of Operational Research* **156(3)**, 579–589.

Nielsen L. K., Kroon L., and Maróti G. (2012). A rolling horizon approach for disruption management of railway rolling stock. *European Journal of Operational Research* **220(2)** 496-509.

O'Hanley J. R., Church R. L. (2011). Designing robust coverage networks to hedge against worst-case facility losses. *European Journal of Operational Research* **209(1)**, 23–36.

O'Hanley J. R., Scaparra M. P., and Garcia S. (2013). Probability chains: A general linearization technique for modeling reliability in facility location and related problems. *European Journal of Operational Research* **230(1)**, 63-75.

Peeta S., Salman F. S., Gunnec D., Viswanath K. (2010). Pre-disaster investment decisions for strengthening a highway network. *Computers & Operations Research* **37(10)**, 1708–1719.

Peng P., Snyder, L. V., Lim, A., Liu, Z. (2011). Reliable logistics networks design with facility disruptions. *Transportation Research Part B: Methodological* **45(8)**, 1190–1211.

Perea F., and Puerto J. (2013). Revisiting a game theoretic framework for the robust railway network design against intentional attacks. *European Journal of Operational Research* **226 (2)** 286–292.

Rad M. A., Kakhki H. T. (2013). Maximum dynamic network flow interdiction problem: New formulation and solution procedures. *Computers & Industrial Engineering* **65(4)**, 531–536.

Robinson N. (2014) UK storms destroy railway line and leave thousands without power. Available at *http://www.bbc.co.uk/news/uk-26042990*.

Scaparra M. P., and Church R. (2012). Protecting supply systems to mitigate potential disaster a model to fortify capacitated facilities. *International Regional Science Review* **35(2)**, 188-210.

Scaparra M. P., Starita S., Sterle C. (2015). Optimizing investment decisions for railway systems protection. In *Railway Infrastructure Security*, 215–233. Setola, Sforza, Vittorini, Pragliola Eds. Springer.

Schmitt A. J., Sun S. A., Snyder L. V., and Shen Z. J. M. (2015). Centralization versus decentralization: Risk pooling, risk diversification, and supply chain disruptions. *Omega* **52**, 201–212.

Snyder L. V., Scaparra, M. P., Daskin, M. S., Church, R. L. (2006). Planning for disruptions in supply chain networks. *Tutorials in Operations Research* 234–257.

Snyder L. V., Daskin M. S. (2005). Reliability models for facility location: the expected failure cost case. *Transportation Science* **39(3)**, 400–416.

Starita S., and Scaparra M. P. (2016). Optimizing dynamic investment decisions for railway systems protection. *European Journal of Operational Research* **248(2)**, 543-557.

Wang J. Y., Ehrgott M., and Chen A. (2014). A bi-objective user equilibrium model of travel time reliability in a road network. *Transportation Research Part B: Methodological* **66**, 4–15.

Wollmer R. (1964) Removing arcs from a network. *Operations Research* **12**, 934–940.

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

Zhu Y., Zheng Z., Zhang X., Cai K. (2013). The r-interdiction median problem with probabilistic protection and its solution algorithm. *Computers & Operations Research* **40(1)**, 451–462.