Transportation Research Part E 84 (2015) 73–87

Contents lists available at ScienceDirect

Transportation Research Part E

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

Optimal allocation of protective resources in urban rail transit networks against intentional attacks

Jian Gang Jin [a], Linjun Lu [a,*], Lijun Sun [b], Jingbo Yin [a]

[a] School of Naval Architecture, Ocean & Civil Engineering, and State Key Laboratory of Ocean Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[b] Future Cities Laboratory, Singapore-ETH Centre, Singapore 138602, Singapore

ARTICLE INFO

Article history:
Received 4 July 2015
Received in revised form 25 September 2015
Accepted 23 October 2015

Keywords:
Urban rail transit
Public transport
Network interdiction
Multilevel programming
Resource allocation

ABSTRACT

This paper advances the field of network interdiction analysis by introducing an application to the urban rail transit network, deploying protective resources against intentional attacks. The resource allocation problem for urban rail transit systems is considered as a game between two players, the attacker interdicting certain rail stations to generate greatest disruption impact and the system defender fortifying the network to maximize the system's robustness to external interdictions. This paper introduces a game-theoretic approach for enhancing urban transit networks' robustness to intentional disruptions via optimally allocating protection resources. A tri-level defender–attacker–user game-theoretic model is developed to allocate protective resources among rail stations in the rail transit network. This paper is distinguished with previous studies in that more sophisticated interdiction behaviors by the attacker, such as coordinated attack on multiple locations and various attacking intensities, are specifically considered. Besides, a more complex multi-commodity network flow model is employed to model the commuter travel pattern in the degraded rail network after interdiction. An effective nested variable neighborhood search method is devised to obtain the solution to the game in an efficient manner. A case study based on the Singapore rail transit system and actual travel demand data is finally carried out to assess the protective resources' effectiveness against intentional attacks.

1. Introduction

The urban rail transit systems have been developed as the backbone of public transportation system in many large cities over the world. The dependence on the rail system keeps growing while the system itself is becoming to be potential targets for certain terrorists. Even limited random disruptions (e.g., random failures) of urban rail transit system can lead to widespread travel delay, not to mention intentional terrorist attacks. Security from terrorist attacks in cities rose to the forefront of political discourse and debate, particularly in the aftermath of 911 (Loukaitou-Sideris et al., 2006). Table 1 lists incidents of terrorist attacks on urban rail transit systems in recent years all over the world. Most of the terrorist attacks happen on working days and in megacities with high population density, generating massive economic loss and casualties. Besides, terrorist attacks have turned out to be more sophisticated and coordinated by multiple attackers. Taking the 2010 Moscow rail transit system bombing as an example, at the time of the attacks, two interchange stations were attacked by two individuals during the morning rush hour when estimated 500,000 people were commuting through the rail transit system. Urban rail transit

[*] Corresponding author.
E-mail addresses: jiangang.jin@sjtu.edu.cn (J.G. Jin), linjunlu@sjtu.edu.cn (L. Lu), sunlijun@u.nus.edu (L. Sun), jingboyin@sjtu.edu.cn (J. Yin).

http://dx.doi.org/10.1016/j.tre.2015.10.008
1366-5545/© 2015 Elsevier Ltd. All rights reserved.

Table 1
Urban rail transit terrorist attacks in recent years.

Date	Attack mode	Country	City	Casualties
1995.3.20 (Mon)	Poison gas	Japan	Tokyo	12 deaths, 5000 injuries
1995.7.25 (Tue)	Bombing	France	Paris	8 deaths, 117 injuries
1996.6.11 (Tue)	Bombing	Russia	Moscow	4 deaths, 7 injuries
1996.12.3 (Fri)	Bombing	France	Paris	4 deaths, 86 injuries
2000.11.20 (Mon)	Bombing	Germany	Dusseldorf	9 injuries
2001.9.2 (Sun)	Arson	Canada	Montreal	40 injuries
2003.2.18 (Tue)	Arson	Korea	Taegu	198 deaths, 147 injuries
2004.1.5 (Mon)	Arson	China	Hong Kong	None
2004.2.6 (Fri)	Bombing	Russia	Moscow	40 deaths, 134 injuries
2004.3.11 (Thur)	Bombing	Spain	Madrid	92 deaths, 1500 injuries
2004.8.31 (Thur)	Bombing	Russia	Moscow	10 deaths, 40 injuries
2005.7.7 (Thur)	Bombing	Britain	London	56 deaths, 720 injuries
2005.7.21 (Thur)	Bombing	Britain	London	1 injury
2010.3.29 (Mon)	Bombing	Russia	Moscow	40 deaths, 102 injuries
2011.4.11 (Mon)	Bombing	Belarus	Minsk	12 deaths, 200 injuries

Data source: from online news report and data in Ou (2014).

systems in cities have turned to be attractive targets by terrorists, because their efficiency would spread a contaminant among large numbers of people quickly over large distances (Brown et al., 2005) and the resulted service suspension would cause substantial travel delay and confusion among commuters (Jin et al., in press).

The robustness of the urban rail transit systems to external disruptions due to intentional attacks can be greatly enhanced by implementing counterterrorism measures. For example, most large cities in China, such as Beijing and Shanghai, have taken strict security check measures by deploying staff and screening detectors at the entrance of major rail transit stations. Given limited amount of protective resources, it is a critical challenge to determine the allocation of those resources among the entire rail transit network with specific consideration of intentional attacks, particularly if multiple locations are interdicted by coordinated attackers. The resource allocation problem for the urban rail transit systems can be considered as a game between the system operator (i.e., defender) and the attacker (Brown et al., 2005; Cappanera and Scaparra, 2011; Perea and Puerto, 2013). Specifically, the attacker aims to generate greatest disruption impacts via interdicting certain components (e.g., stations) of the system while the defender aims to maximize the system's robustness to external disruptions.

This paper introduces a game-theoretic approach for enhancing urban rail transit networks' robustness to intentional attacks via optimally allocating protection resources. With this objective, we developed a tri-level defender–attacker–user game-theoretic model that optimally allocates protective resources for urban rail transit systems. In the first level, the system defender allocates protective resources among vulnerable stations with the objective of minimizing the maximal potential disruption impacts that can be achieved by attackers. In the second level, the attacker responds correspondingly and interdicts rail stations in order to cause maximal travel delay for rail system users. Different attacking strategies are specifically considered in the game by modeling various attacking intensities, such as in-flow, out-flow, through capacity reductions for rail stations. With both of the defending and attacking patterns, the third level models the system users' behavior and assigns them to alternative paths once the original path is affected. In order to tackle the nonlinear property of the model, an effective nested variable neighborhood search method is devised. The contribution of this study lies in the following aspects:

- Propose a tri-level defender–attacker–user game-theoretic model that optimally allocates protective resources for urban rail transit system against intentional attacks;
- Consider the features of sophisticated attacking behavior and the characteristics of commuter flows in the rail network. The proposed model is capable of modeling multiple attacking locations as well as various attacking intensities while the commuter flow is modeled as a multi-commodity flow problem in the third level.
- Demonstrate the practical significance of the proposed model. A case study based on the Singapore rail transit system and actual travel demand data shows that the worst-case disruption impact achieved by the attack can be significantly mitigated by allocation of protective resources over critical interchange rail stations.

The remainder of this paper is organized as follows. Section 2 reviews relevant papers in the literature and highlights the research gap. A tri-level game-theoretic programming model is developed in Section 3 and a nested variable neighborhood search solution method is proposed in Section 4. Section 5 carries out a case study based on the Singapore rail transit network. Finally, conclusions are drawn in Section 6.

2. Literature review

Recently, research topics related to the robustness of urban rail transit systems to disruptions, including *disruption preventive planning* and *post-disruption response recovery planning*, are receiving more attention. Some disruption preventive planning methodologies and techniques have been proposed for enhancing the urban rail transit system's robustness to disturbances. De-Los-Santos et al. (2012) proposed passenger robustness measures to disruptions in a rail transit network for cases with and without bus bridging interruptions. Jin et al. (2014) investigated the resilience of urban rail systems to random disruption, and proposed to enhance the resilience by leveraging on public bus services. A two-stage stochastic programming model is developed to determine the optimal integration with bus services. As a complementary approach, post-disruption recovery focuses on devising responsive measures that alleviate the consequences of realized disruptions. Meyer and Belobaba (1982) examined the contingency planning processes relevant to rail transit systems and identified important characteristics in the planning process. Darmanin et al. (2010) proposed a disruption recovery strategy based on using existing bus routes buses for the Melbourne metro system. Kepaptsoglou and Karlaftis (2009) studied the bus bridging problem on the degraded urban rail transit network in the event of unexpected operational disruptions, and proposed a methodological framework for determination of bus routes and allocation of bus resources. Focusing on a similar problem, Jin et al. (in press) developed an optimization-based approach, combining column generation and path-based network flow techniques, to determine simultaneously the bus bridging routes and the allocation of available vehicle resources.

In contrast to handling disruptions due to random failures, the problem of fortification against malicious and intentional attacks in the context of urban rail transit systems is not well addressed yet. Brown et al. (2005) proposed a defender–attacker model that optimally deploys limited NBC sensors in Washington DC rail transit system with the objective of minimizing the worst-case detection time. Laporte et al. (2010) investigated the strategic railway transit network design problem in the presence of link failures, and proposed a non-cooperative two-player zero-sum game with perfect information. Similarly, Perea and Puerto (2013) focused on the strategic railway network design problem against intentional attacks. The authors also proposed a mathematical programming model that optimizes the allocation of security resources over the network, which shares some features with our study. However, in this paper we focus on the urban rail transit network which exhibits more complex network topology and undertakes greater inter-line commuter transfer flows. Besides, we specifically model the sophisticated interdiction behaviors by the attacker - multiple interdiction sites and various interdiction intensities.

Except for the urban rail transit system, the network interdiction and fortification problem has also been studied in the literature for other types of infrastructure systems that takes in the form of networks, such as telecommunication network, water supply network, grid network, and other types of transportation networks. However, the specific flow pattern varies among different types of networks, and the interdiction can be distinguished by the location where the network flow is disabled, i.e., node and arc. Qiao et al. (2007) studied the security resource allocation problem for water supply networks, and developed a hybrid method based on max–min linear programming, hydraulic simulation and genetic algorithms to maximize the network's resilience to physical attacks. The underlying network interdiction was based on that in Wood (1993) which identifies a set of arcs to incur most transportation capacity reduction from source to sink. Investigating the power network fortification problem, Yao et al. (2007) presented a tri-level optimization model that captures the interaction between the network defender and attacker. The authors considered both nodes (i.e., power generators) and arcs (i.e., power lines) as the attackable components in the power network in order to identify critical network components to defend possible terrorist attacks. Scaparra and Church (2008) investigated the most cost-effective way of allocating protective resources among facilities of an existing but vulnerable infrastructure system so that the impact of the most disruptive attack to r unprotected facilities is minimized. The authors focused on protection nodes (i.e., facilities) of the network, and developed a bi-level formulation based on p-median location model. Murray-Tuite and Fei (2010) analyzed the terrorist risk in a transportation network and presented a simulation methodology, which tackles the defender–attacker game by decomposing the interaction into a sequential simulation modules. The authors mainly focused on critical infrastructures (e.g., airport and government installations) as the attackable nodes in the transportation network, and considered link capacity reduction as the consequence of node failures. Focusing on the shortest-path network, Cappanera and Scaparra (2011) introduced a game-theoretic approach and developed a tri-level formulation to identify the arcs in the network to harden with the objective of minimizing the shortest path in the worst-case disruptions. Only the shortest path for the given origin–destination pair was considered. Chen et al. (2011) considered a two-player game in the context of minimum cost network design problem, in which the network operator designs the network while the attacker destroys certain arcs in the network. The network design focused on constructing arcs in such a way that the cost of a feasible flow on the residual network during disruption is minimized. Faturechi and Miller-Hooks (2014) proposed a comprehensive framework for quantitatively assessing system performance measures in the presence of uncertain events, component failure, or other disruptions/disasters for civil infrastructure systems. A general optimization model was developed to determine an optimal allocation of limited resources to preparedness and response options. It is observed from the literature that protective resources are allocated to system components, either nodes or links, that are accessible to attackers and vulnerable to disruptions. The attackable components varies among different types of infrastructure systems, while the methodologies for allocating protective resources are universal and applicable to each other.

According to the literature review, protecting the urban rail transit network against intentional attacks with consideration of the passenger flow characteristics as well as attacker's various attacking strategies has practical significance and is worth research efforts. To the best of our knowledge, more sophisticated attacking behavior, such as multiple attacking locations and intensities, is seldom considered in the defender-attack game. Besides, the commuter flow with multiple origin–destination in the rail network needs to be handled by more complex network flow methodologies than that with single origin–destination studied in Cappanera and Scaparra (2011). In this paper, we advance the disruption preventive planning research for the urban rail transit system by introducing a three-player (i.e., defender–attacker–user) game, in which the attacker aims to maximize disruption impacts via interdicting rail stations in the network, the defender aims to minimize the worst-case disruption impacts achieved by the attacker while the system users fulfill the travel demand in the residual rail network. To address the problem, we developed a game-theoretical tri-level model allocating protective resources among the rail network with the goal of identifying cost-effective ways to secure the network against intentional attacks. Different attacking intensity is specifically considered and the multiple origin–destination commuter flow is modeled. To solve the model, we designed an effective heuristic method based on the variable neighborhood search algorithm. A case study on the Singapore rail transit system demonstrates the effectiveness of investing protective resources.

3. A tri-level programming model

3.1. Problem description

The resource allocation problem for the urban rail transit systems is tackled as a game involving three parties, the system defender as the leader, potential attackers as the follower, and rail transit system riders as the system user, as shown in Fig. 1. Without prior knowledge of the exact disruptions made by attackers, the system defender strategically allocates protective resources among the entire rail transit network aiming to maximize the system's robustness to external attacks. We model the available protective resources (e.g., security staff, security screening equipment) as a discrete set, denoted as $S = \{1, 2, \ldots, \bar{s}\}$. Given the required amount of each protection resource associated with rail stations, the challenge for the system defender is to identify those critical system components (e.g., rail stations and rail links) to fortify subject to the total amount of protective resources available. In this paper, we focus on protecting rail stations, since they are easily accessible by the public while the rail links are not. The objective of the protective resource allocation is to minimize the worst-case disruptive impacts that can be achieved by the attacker.

Given the protection configuration by the system defender, the attacker intentionally interdicts certain rail stations among the entire network with the objective of generating greatest disruption impacts. In order to model different attacking strategies by the attacker, we consider various attacking intensities measured by the percentage of capacity reduction for rail stations, including the rail station's in-flow, out-flow and through capacities. In this paper, we are interested in understanding the attacking behavior by those rational and tactful attackers whose objective is to maximize the disruption impacts. The decisions made by the attacker include the selection of rail stations to interdict, and the corresponding attacking intensities. From the attackers' perspective, the disruption impacts consist of the travel inconvenience to the system users as well as the response recovery cost for the system operator. Similar to the defender's resource constraint, the interdiction can only be carried out within certain budget by the attacker. In this paper, we consider multiple attacking intensities to model sophisticated interdiction behaviors of the attacker, while protection resources are allocated without differentiating protection levels. This is due to the fact that the system defender, as the leader of the game, possesses no perfect information about the interdiction pattern, and thus tends to fully protect critical stations. However, knowing the exact protection information, the attacker is able to conduct coordinated interdiction actions, such as multiple sites and intensities.

In the lowest level, the rail transit system riders, as the user, have to respond correspondingly in the event of disruptions, either taking the shortest path from origin to destination if it is not affected by the disruption or using an alternative path in case disruption occurs along the original path. Fig. 2 presents an illustrative example of an urban rail transit system with two lines. In the example, the system riders take the original path indicated by red arrows from Station 1 to 2 under normal conditions, while the alternative path indicated by the dark arrows will be employed once the rail station along the original path is attacked during disruption. In this paper, we measure the performance of the rail transit system as the total travel cost of

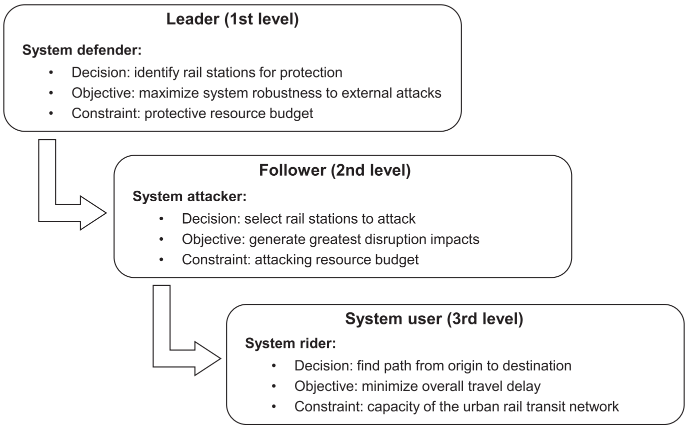
Leader (1st level)
System defender:
• Decision: identify rail stations for protection
• Objective: maximize system robustness to external attacks
• Constraint: protective resource budget
Follower (2nd level)
System attacker:
• Decision: select rail stations to attack
• Objective: generate greatest disruption impacts
• Constraint: attacking resource budget
System user (3rd level)
System rider:
• Decision: find path from origin to destination
• Objective: minimize overall travel delay
• Constraint: capacity of the urban rail transit network

Fig. 1. A tri-level game-theoretic framework for the resource allocation problem.

all system riders. The travel cost can be measured by travel time and/or travel distance. Thus, the travel inconvenience caused by disruptions can be measured by the difference of the overall system performance before and after the disruption.

Therefore, the challenge for the rail transit system operator is to well understand the potential attacking patterns and their associated disruption impacts, and in turn to allocate protective resources correspondingly. With this objective, we introduce a tri-level defender–attacker–user game-theoretic model for enhancing urban transit network's robustness to intentional disruptions via optimally allocating protective resources.

3.2. Network representation

The urban rail transit system can be represented as a graph $G(\mathcal{N}, \mathcal{A})$ with rail stations defined as the node set $\mathcal{N}$ while rail links indicated by the arc set $\mathcal{A}$. Based on the defined rail transit network, alternative path $\mathcal{K}_w$ that can be possibly employed by origin–destination (OD) pair $w \in \mathcal{W}$ under disruptive conditions should be pre-generated for the mathematical model formulation. In this paper, we set the alternative path set $\mathcal{K}_w$ to include the k shortest paths whose journey time does not exceed the original time by a certain limit. The shortest path set K_w can be obtained by the method developed by Yen (1971) and the sequential integer programming method developed by Jin et al. (2014).

Before presenting the tri-level programming model, we first introduce the mathematical notations as follows:

Sets:
$\mathcal{W}$: set of origin–destination (OD) pairs
$\mathcal{S}$: set of protective resources, $\{1, 2, \ldots, \bar{s}\}$
$\mathcal{M}$: set of attacking intensities, $\{1, 2, \ldots, \bar{m}\}$
$\mathcal{N}$: set of nodes representing rail stations in the urban rail transit network
$\mathcal{A}$: set of arcs representing rail links in the urban rail transit network
$\mathcal{K}_w$: set of feasible paths in the urban rail transit network for OD pair $w \in \mathcal{W}$

Parameters (user level):
t_w^k: the travel time of path $k \in \mathcal{K}_w$ of OD pair $w \in \mathcal{W}$
$\tilde{t}_w$: the travel time of OD pair $w \in \mathcal{W}$ under normal condition
p_w: the penalty of OD pair $w \in \mathcal{W}$ if the travel demand cannot be fulfilled under disruption
D_w: travel demand of OD pair $w \in \mathcal{W}$
θ_{wa}^k: 1 if arc $a \in \mathcal{A}$ is used by the path $k \in \mathcal{K}_w$ of OD pair $w \in \mathcal{W}$; 0 otherwise
ρ_{ima}: percentage of capacity reduction of the connecting arc $a \in \mathcal{A}$ if node $i \in \mathcal{N}$ is attacked by intensity $m \in \mathcal{M}$
δ_{wi}^1: 1 if node $i \in \mathcal{N}$ is the origin of OD pair $w \in \mathcal{W}$; 0 otherwise
δ_{wi}^2: 1 if node $i \in \mathcal{N}$ is the destination of OD pair $w \in \mathcal{W}$; 0 otherwise
φ_{im}^1: percentage of in-flow capacity reduction of node $i \in \mathcal{N}$ if it is attacked by intensity $m \in \mathcal{M}$
φ_{im}^2: percentage of out-flow capacity reduction of node $i \in \mathcal{N}$ if it is attacked by intensity $m \in \mathcal{M}$
q_a: the capacity of arc $a \in \mathcal{A}$ (i.e., hourly maximum amount of commuters that can be carried)
q_i^1: the commuter in-flow capacity for node $i \in \mathcal{N}$
q_i^2: the commuter out-flow capacity for node $i \in \mathcal{N}$
$H(\mathbf{y})$: total disruption impact for the system users given interdiction pattern $\mathbf{y}$

Parameters (attacker level):
r_{im}: the recovery effort associated with station $i \in \mathcal{N}$ if it is attacked by intensity $m \in \mathcal{M}$
d_{im}: the required amount of attacking effort to attack node $i \in \mathcal{N}$ by intensity $m \in \mathcal{M}$
T: total amount of attacking efforts
$G_1(\mathbf{z})$: disruption impact for the system users achieved by the attacker given protection pattern $\mathbf{z}$
$G_2(\mathbf{z})$: response recovery efforts for the system defender achieved by the attacker given protection pattern $\mathbf{z}$

Parameters (defender level):
c_{is}: the required amount of protection resource $s \in \mathcal{S}$ at node $i \in \mathcal{N}$ should it be selected for protection
Q_s: total amount of protection resource $s \in \mathcal{S}$

Decision variables:
x_w^k: $\geqslant 0$. The commuter flow of OD pair $w \in \mathcal{W}$ on path $k \in \mathcal{K}_w$
y_{im}: $\in \{0, 1\}$. 1 if node $i \in \mathcal{N}$ is attacked at intensity level $m \in \mathcal{M}$; 0 otherwise
z_i: $\in \{0, 1\}$. 1 if node $i \in \mathcal{N}$ is protected by the defender; 0 otherwise

3.3. User-level model

The user-level model is to assign the travel demand on the urban rail transit network given the interdiction pattern $\mathbf{y}$ by the attacker. Under the disruptive condition, the system riders will find corresponding routes to fulfill their travel demand with least travel delay. The user-level model can be formulated as follows:

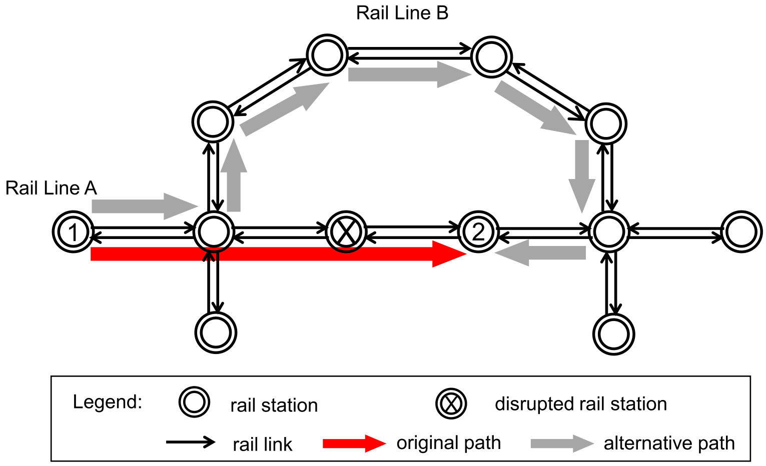

Fig. 2. An illustrative example of the rail transit network representation.

$$H(\mathbf{y}) = \min_{\mathbf{x}} \left\{ \sum_{w\in\mathcal{W}}\sum_{k\in\mathcal{K}_w} (t_w^k - \tilde{t}_w) x_w^k + \sum_{w\in\mathcal{W}} p_w \left(D_w - \sum_{k\in\mathcal{K}_w} x_w^k \right) \right\} \tag{1}$$

$$\text{s.t.} \sum_{k\in\mathcal{K}_w} x_w^k \leqslant D_w \quad \forall w\in\mathcal{W} \tag{2}$$

$$\sum_{w\in\mathcal{W}}\sum_{k\in\mathcal{K}_w} \theta_{wa}^k x_w^k \leqslant \left(1 - \sum_{i\in\mathcal{N}}\sum_{m\in\mathcal{M}} \rho_{ima} y_{im} \right) q_a \quad \forall a\in\mathcal{A} \tag{3}$$

$$\sum_{w\in\mathcal{W}}\sum_{k\in\mathcal{K}_w} \delta_{wi}^1 x_w^k \leqslant \left(1 - \sum_{m\in\mathcal{M}} \varphi_{im}^1 y_{im} \right) q_i^1 \quad \forall i\in\mathcal{N} \tag{4}$$

$$\sum_{w\in\mathcal{W}}\sum_{k\in\mathcal{K}_w} \delta_{wi}^2 x_w^k \leqslant \left(1 - \sum_{m\in\mathcal{M}} \varphi_{im}^2 y_{im} \right) q_i^2 \quad \forall i\in\mathcal{N} \tag{5}$$

$$x_w^k \geqslant 0 \quad \forall w\in\mathcal{W},\ \forall k\in\mathcal{K}_w \tag{6}$$

Objective function (1) minimizes the overall travel delay for commuters whose demand can be fulfilled by alternative paths, measured as difference of total travel time under disruptive and normal conditions. For those commuters who are no longer able to reach destination, a penalty is put in the objective function as the second term. Constraint (2) ensures that the total travel flow along all feasible paths between a particular OD pair w does not exceed the original demand. Constraint (3) guarantees that, for each arc, the total commuter flow that passes through the arc respects the residual capacity under disruptive condition. Similarly, Constraints (4) and (5) impose the restriction of the in-flow and out-flow capacity for each node, respectively.

3.4. Attacker-level model

In the attacker-level model, the attacker aims to maximize the disruption impacts $H(\mathbf{y},\mathbf{z})$ for the system users by finding the optimal attacking nodes and the corresponding attacking intensity, given resource protection decision $\mathbf{z}$ by the defender. The response recovery effort for the system defender is also considered as the second objective. The model can be formulated as follows:

$$G_1(\mathbf{z}) = \max_{\mathbf{y}} H(\mathbf{y}) \tag{7}$$

$$G_2(\mathbf{z}) = \max_{\mathbf{y}} \sum_{i\in\mathcal{N}}\sum_{m\in\mathcal{M}} r_{im} y_{im} \tag{8}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}}\sum_{m\in\mathcal{M}} d_{im} y_{im} \leqslant T \tag{9}$$

$$\sum_{m\in\mathcal{M}} y_{im} \leqslant 1 \quad \forall i\in\mathcal{N} \tag{10}$$

$$y_{im} \leqslant 1 - z_i \quad \forall i\in\mathcal{N},\ \forall m\in\mathcal{M} \tag{11}$$

$$y_{im} \in \{0,1\} \quad \forall i\in\mathcal{N},\ \forall m\in\mathcal{M} \tag{12}$$

Objective function (7) maximizes the travel inconvenience to system users and objective function (8) maximizes response recovery effort for the system defender. Constraint (9) imposes the attacking budget for the attacker. Constraint (10) ensures that at most one attacking intensity should be selected for each node. Constraint (11) guarantees that only those nodes which are not fortified by the defender can be interdicted.

3.5. Defender-level model

At the upper level, the defender optimally allocates protective resources to rail stations. The upper level model can be formulated as follows:

$$\min_{\mathbf{z}} \; G_1(\mathbf{z}) \tag{13}$$

$$\min_{\mathbf{z}} \; G_2(\mathbf{z}) \tag{14}$$

$$\text{s.t.} \sum_{i \in \mathcal{N}} c_{is} z_i \leqslant Q_s \quad \forall s \in \mathcal{S} \tag{15}$$

$$z_i \in \{0, 1\} \quad \forall i \in \mathcal{N} \tag{16}$$

The defender determines the optimal protection pattern with the objective of minimizing the system performance deterioration achieved by the attacker $G_1(\mathbf{z})$ and $G_2(\mathbf{z})$, represented by the two objective functions (13) and (14). Constraint (15) states that the total allocated resource should not exceed the upper limit.

3.6. Weighted-sum bi-objective model

Given the above bi-objective defender–attacker–user game-theoretic model, we employ the weighted-sum method to transform it to a single-objective optimization model. The two objectives, travel inconvenience $H(\mathbf{y})$ and disruption recovery effort $\sum_i \sum_m r_{im} y_{im}$, are firstly normalized by constants C_1 and C_2, respectively, and then combined by a weight parameter $\alpha (0 < \alpha < 1)$ as a single objective. C_1 represents the maximal travel inconvenience that can be possibly achieved by the attacker. The worst case where all travel demand cannot be fulfilled is used to estimate C_1, which is calculated as follows:

$$C_1 = \sum_{w \in \mathcal{W}} p_w D_w \tag{17}$$

Similarly, C_2 represents the worst-case disruption recovery effort that is caused by the attacker's interdiction. The following integer linear programming model (18)–(20) is used to obtain C_2.

$$C_2 = \max_{\mathbf{y}} \sum_{i \in \mathcal{N}} \sum_{m \in \mathcal{M}} r_{im} y_{im} \tag{18}$$

$$\text{s.t.} \sum_{i \in \mathcal{N}} \sum_{m \in \mathcal{M}} d_{im} y_{im} \leqslant T \tag{19}$$

$$y_{im} \in \{0, 1\} \quad \forall i \in \mathcal{N}, \; \forall m \in \mathcal{M} \tag{20}$$

Therefore, the overall tri-level defender–attacker–user game-theoretic model is summarized as follows:

$$\min_{\mathbf{z}} \left\{ \max_{\mathbf{y}} \left\{ \frac{\alpha}{C_1} \min_{\mathbf{x}} \left\{ \sum_{w \in \mathcal{W}} \sum_{k \in \mathcal{K}_w} (t_w^k - \tilde{t}_w) x_w^k + \sum_{w \in \mathcal{W}} p_w \left(D_w - \sum_{k \in \mathcal{K}_w} x_w^k \right) \right\} + \frac{1-\alpha}{C_2} \sum_{i \in \mathcal{N}} \sum_{m \in \mathcal{M}} r_{im} y_{im} \right\} \right\} \tag{21}$$

$$\text{s.t.} \quad (2)\text{—}(6), \; (9)\text{—}(12), \; (15) \text{ and } (16)$$

4. Nested variable neighborhood search algorithm

As the complexity of the problem precludes solving the non-linear tri-level optimization model directly, we develop a nested variable neighborhood search algorithm to find the best defending and attacking patterns for both the defender and attacker. The outer level variable neighborhood search procedure focuses on searching for the optimal defending solution from the system defender's perspective. Nested in the out lever procedure, the inner level variable neighborhood search procedure is conducted for finding the optimal attacking solutions from the attacker's viewpoint.

4.1. Solution representation and initial solution

A solution to the overall tri-level defender–attacker–user model is encoded by two strings, the defending solution $S_d : (d_1, d_2, \ldots, d_k)$ representing the rail stations $(d_1, d_2, \ldots, d_k)$ that are fortified by the system defender, and the attacking solution $S_a : (a_1, a_2, \ldots, a_n; l_1, l_2, \ldots, l_n)$ indicating the rail stations $(a_1, a_2, \ldots, a_n)$ that are selected for interdiction by the attacker as well as the corresponding attacking intensity levels $(l_1, l_2, \ldots, l_n)$.

The initial solution is randomly generated in the following way. Firstly, we define set $N' \subseteq N$ consisting of those rail stations considered in the generation of defending and attacking solutions, while those rail stations in $N \setminus N'$ are assumed to be unlikely to be attacked, and thus do not need to be protected. The definition of the set N' reflects the protection strategy of the system defender. For example, N' can be defined as the set of those interchange rail stations considering that interchange stations are where large amount of passengers transfer, and interdicting them leads to greatest disruption impacts from the whole network perspective. Note that $|N'|$ determines the size of the neighborhood search space. With more rail stations included in set N', larger search space can be explored at the expense of more computational efforts. Therefore, the set N' should be defined in such a way that balances the tradeoff between computational efficiency and solution quality. Secondly, the defender solution S_d starts with an empty set, and inserts elements from $N' \setminus S_d$ one by one while respecting the protection budget constraint (15) until no rail station can be further added. Similarly, the attacking solution S_a is also randomly generated by adding elements from $N' \setminus (S_a \cup S_d)$ one by one while satisfying the attacking budget constraint (9). For each generated element a_i, the corresponding attacking intensity l_i is also randomly assigned.

4.2. Fitness evaluation

With the above designed solution representation, each candidate solution (S_d, S_a) can be translated into the decision variables $\mathbf{y}$ and $\mathbf{z}$ corresponding to the defending and attacking decisions. Thus, the tri-level defender–attacker–user model reduces to the single level model (1)–(6) involving only the flow assignment decision variable $\mathbf{x}$. Considering that the user-level model is a linear programming model which can be solved efficiently by commercial solvers, we employ CPLEX to solve it. With all the decision variables determined, the fitness of each candidate solution (S_d, S_a) can be obtained by the calculating the objective function (21).

4.3. Neighborhood structure

Neighborhood solutions for both of the defending and attacking solutions are generated according to the following five neighborhood structures. Denote $N(S, j)$ as the jth neighborhood space for solution S.

- $N(S, 1)$: 1 to 1 swap operation. Randomly select one element in S_d for the current defending solution (or S_a for the attacking solution) and one element in $N' \setminus S_d$ (or $N' \setminus (S_a \cup S_d)$), and swap the two elements;
- $N(S, 2)$: 1 insertion operation. Randomly select one element in $N' \setminus S_d$ for the defending solution (or $N' \setminus (S_a \cup S_d)$ for the attacking solution), and add it to S_d (or S_a);
- $N(S, 3)$: 1 deletion operation. Randomly delete one element in S_d for the defending solution (or S_a for the attacking solution);
- $N(S, 4)$: 1 to 2 swap operation. Randomly select one element in S_d for the defending solution (or S_a for the attacking solution) and two elements in $N' \setminus S_d$ (or $N' \setminus (S_a \cup S_d)$), and swap them;
- $N(S, 5)$: 2 to 1 swap operation. Randomly select two elements in S_d for the defending solution (or S_a for the attacking solution) and one element in $N' \setminus S_d$ (or $N' \setminus (S_a \cup S_d)$), and swap them.

Note that the attacking intensity decision is not explored by the neighborhood structures, as it will be improved by a local search routine in the inner level variable neighborhood search procedure.

4.4. Outer level variable neighborhood search procedure

The outer level variable neighborhood search procedure is employed to optimize the defending pattern from the system defender's perspective, as is summarized in Algorithm 1. In this procedure, the defined five distant neighborhoods are explored in sequence in order to improve the fitness of the defending solution.

The variable search procedure for optimizing defending pattern starts with exploring the first neighborhood structure. In each iteration, a new defending solution is randomly generated by shaking the current incumbent solution in the jth neighborhood space. The corresponding attacking solution is generated by the inner level variable neighborhood search procedure. The pair of defending and attacking solutions (S_d, S_a) is subsequently improved by a local search step employing the first neighborhood structure. Note that the feasibility of the generated neighborhood solutions are guaranteed by checking the defending and attacking budget constraints. In case the fitness of the neighborhood solution S'_d is improved (i.e., lower than the fitness of the current defending solution S_d), S_d is updated by S'_d and the neighborhood structure is reset to the first one.

Regarding the stopping conditions, the local search step terminates once maximum $NoIter1$ iterations are conducted or the best solution does not get improved for $NoImpr1$ consecutive iterations, while the outer level variable neighborhood search terminates until all the five neighborhood structures are explored.

Algorithm 1. Variable neighborhood search for optimizing defending pattern

```
Input: $G(\mathcal{N},\mathcal{A})$ and all parameters
Output: optimal defending solution $S_d$ and attacking solution $S_a$
generate initial defending solution $S_d$ and initial attacking solution $S_a$;
evaluate fitness of initial solution $f(S_d, S_a)$;
$j \leftarrow 1$;
Repeat
    $S'_d \leftarrow Neighborhood(S_d, j)$;   // shaking defending solution by jth neighborhood structure
    $S'_a \leftarrow VNS(S'_d)$;   // variable neighborhood search for attacking solution
    Repeat// local search for $S'_d$
        $S''_d \leftarrow Neighborhood(S'_d, 1)$;   // shaking by the 1st neighborhood structure
        $S''_a \leftarrow VNS(S''_d)$;
        evaluate the fitness of solution $(S''_d, S''_a)$;
        update $S'_d$;
    Until the stopping condition is met
    If fitness $f(S'_d, S'_a) < f(S_d, S_a)$
        $j \leftarrow 1$;   // reset to initial neighborhood structure
        $S_d \leftarrow S'_d, S_a \leftarrow S'_a$;   // update defending and attacking solutions
    Else
        $j \leftarrow j + 1$;   // move to the next neighborhood structure
    End if
Until $j > 5$
```

4.5. Inner level variable neighborhood search procedure

The inner level variable neighborhood search procedure is employed to optimize the interdiction pattern from the system attacker's perspective, as is summarized in Algorithm 2. Similarly, the defined five distant neighborhoods are explored in sequence in order to improve the fitness of the attacking solution.

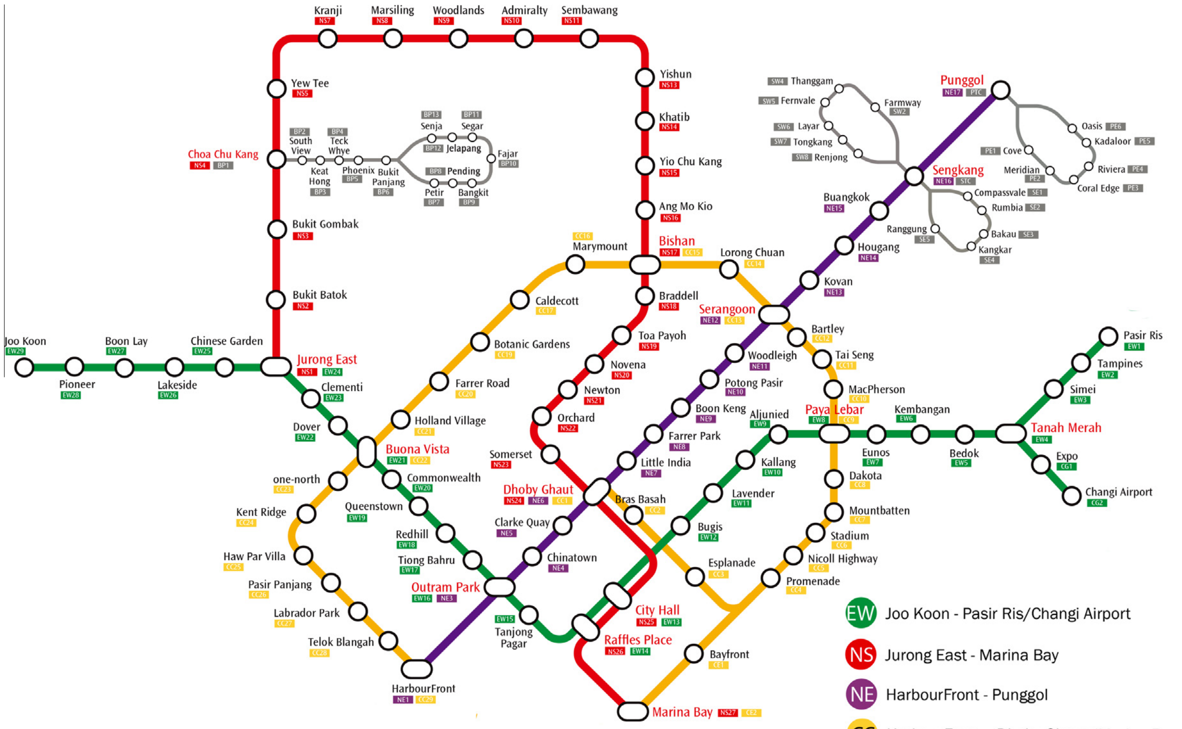

Fig. 3. The urban transit rail network of Singapore.

With given defending solution S_d, the variable search procedure for optimizing attacking pattern starts with exploring the first neighborhood structure. In each iteration, a new attacking solution is randomly generated by shaking the current incumbent solution in the *j*th neighborhood space, which is subsequently improved by a local search step. An additional local search step $IntensitySearch(S_a)$ is employed to find the best attacking intensities corresponding to the identified attacking stations, subject to the attacking budget constraint. In case the fitness of the neighborhood solution S'_a is improved (i.e., higher than the fitness of the current defending solution S_a), S_a is updated by S'_a and the neighborhood structure is reset to the first one.

Regarding the stopping conditions, the local search step for the optimizing neighborhood solutions terminates once maximum *NoIter*2 iterations are conducted or the best solution does not get improved for *NoImpr*2 consecutive iterations. Similarly, the local search step for optimizing attacking intensity terminates once maximum *NoIter*3 iterations are conducted or the best solution does not get improved for *NoImpr*3 consecutive iterations. The inner level variable neighborhood search terminates until all the five neighborhood structures are explored.

Algorithm 2. Variable neighborhood search optimizing attacking pattern

```
Input: $G(\mathcal{N},\mathcal{A})$ and all parameters
Output: optimal attacking solution $S_a$
generate initial attacking solution $S_a$ based on given defending solution $S_d$;
evaluate fitness of initial solution $f(S_d, S_a)$;
$j \leftarrow 1$;
Repeat
    $S'_a \leftarrow Neighborhood(S_a, j)$;   // shaking attacking solution by jth neighborhood structure
    Repeat// local search procedure for $S'_a$
        $S''_a \leftarrow Neighborhood(S'_a, 1)$;   // shaking by the 1st neighborhood structure
        $S''_a \leftarrow IntensitySearch(S''_a)$;   // local search for attacking intensity
        update $S'_a$;
    Until the stopping condition is met;
    If fitness $f(S_d, S'_a) > f(S_d, S_a)$
        $j \leftarrow 1$;   // reset to initial neighborhood structure
        $S_a \leftarrow S'_a$;   // update attacking solution
    Else
        $j \leftarrow j + 1$;   // move to the next neighborhood structure
    End if
Until $j > 5$
```

5. Case studies

In this section we test the performance of the tri-level defender–attacker game-theoretical model by studying a case study based on the Singapore rail transit network, as shown in Fig. 3. The nested variable neighborhood search algorithm is coded in C++ and CPLEX 12.6 is used as the linear programming solver. Computational experiments are conducted on a PC with 3.4 GHz Inter Core i7 PC with 8 GB RAM.

Table 2
Description of the transit rail system and parameters of the model and algorithm.

Rail system	• EW,NS,NE Lines: 6 cars per train; capacity of 1920 passengers; 3 min interval at peak period • CC Line: 3 cars per train; capacity of 931 passengers; 3 min interval
Model input	• Attack effort: 100 for all stations • Recover effort: 100 for Dhoby Ghaut station; 60 for other interchange stations; and 30 for non-interchange stations • Protection resource: 100 for Dhoby Ghaut station; 70 for other interchange stations; and 40 for non-interchange stations • Attacking intensity: full attack ($\varphi^1_{im} = 1,\ \varphi^2_{im} = 1,\ \rho_{ima} = 1,\ \forall i, m, a$; and 100% attack effort, recovery cost and protection resource required); partial attack ($\varphi^1_{im} = 0.5,\ \varphi^2_{im} = 0.5,\ \rho_{ima} = 0.5,\ \forall i, m, a$; and 50% attack effort, recovery cost and protection resource required) • Penalty for unserved commuters: $p_w = 50$ min • Weight parameter in the objective function: $\alpha = 0.5$
Solution algorithm	• Outer-level: $NoIter1 = 100;\ NoImpr1 = 10;$ • Inner-level: $NoIter2 = 100;\ NoImpr2 = 10;\ NoIter3 = 50;\ NoImpr3 = 5;$

5.1. Case study

The urban rail transit network of Singapore in 2013 consists of four intertwined rail lines (EW, NE, NS, CC) and 90 stations, with 15 among them being interchange stations. The travel demand data was obtained by the automatic fare collection system recording the origin, destination and timestamp information of all personnel trips. The OD demand during the morning peak period (8–9 am) is used as the model input. Table 2 summarizes the descriptions of the rail transit system, and the parameter settings of the model as well as the nested variable neighborhood search algorithm. Note that the attack efforts, recovery cost and protection resource parameters are normalized on a scale from 0 to 100, and two attacking intensities (i.e., full attack and 50% partial attack) are considered.

5.2. Impact of interchange and non-interchange stations

We first examine the effectiveness of the set N' which is employed for generating defending and attacking decisions in the solution approach. The following three strategies are compared:

- Strategy 1: defining N' as the set of non-interchange stations. Only non-interchange stations can be interdicted by the attacker while the defender employs no fortification;
- Strategy 2: defining N' as the set of interchange stations. Both of the defender and attacker focus on interchange stations for fortification and interdiction;
- Strategy 3: defining N' to include all stations. Both of the defender and attacker explore all rail stations for fortification and interdiction decision.

Strategy 1 is to assess the maximal disruption impacts that can be achieved by the attacker via interdicting only those non-interchange stations. Strategy 2 explores the defender–attacker's game on those interchange stations, while all stations are considered in Strategy 3. Fig. 4(a) compares for the above three strategies the solution quality which is assessed by the objective function (21). Note that the budget of protection resource is set to be 250. As can be seen, under Strategy 1 interdicting only those non-interchange stations even without any fortification by the defender, the attacker cannot achieve as much disruption impact as that by interdicting those interchange ones under Strategy 2. Thus, interchange stations are more likely to be interdicted by intelligent and intentional attackers, and should be given higher priority when allocating protective resources from the defender's perspective. It is also observed that inclusion of non-interchange stations, as in Strategy 3, does not yield improvement in solution quality, as compared to that of Strategy 2. Fig. 4(b) compares the computational efficiency of Strategies 2 and 3. Note that the optimal solution of Strategy 2 is given as the initial solution for Strategy 3, and the nested variable neighborhood search algorithm is further conducted to explore the benefits of including non-interchange stations. The obtained results demonstrate that the objective function value does not get improved while it consumes substantial amount of additional computational efforts. Therefore, we employ Strategy 2 and only consider interchange stations in the following computational experiments.

5.3. Impact of number of OD pairs

As the efficiency of solving the user-level model is highly influenced by the number of OD pairs, it is necessary to find a suitable amount of OD demand that balances solution quality and computational time. We first rank the total amount of 6689 OD pairs according to the hourly demand ranging from highest to lowest demand – 1264 to 1. The cumulative percentage of travel demand with the number of OD pairs is presented in Fig. 5(a). As can be seen, the travel demand is highly concentrated a small group of OD pairs: top 32 OD (0.48%) pairs take up 10% demand; top 86 OD (1.29%) pairs take up 20% demand; top 166 OD (2.48%) pairs take up 30% demand. Fig. 5(b) summarizes the solution quality as is calculated by the objective function (21) and computational times of the model with various amount of OD demand as the input. Note that the protection resource budget and the attacking effort budget are set to be 250 and 200, respectively. We observe that introduction of additional OD demand does not yield a significant decrease in the objective function value. Besides, the interdiction and fortification decisions remain to be those stations with high priority (as in Fig. 6), without significant change under different amount of OD demand. Therefore, with consideration of both the solution quality and computational efficiency, we employ the top 86 OD pairs (20% demand) in the user-level model in the following computational experiments.

5.4. Effectiveness of protective resources

To assess the effectiveness of allocating protective resource to the rail transit system, we compare the characteristics of the solutions under the protection situation against that without any protective resources. Table 3 summarizes the results of the tri-level game-theoretic model given different budgets of defending and attacking resources. As can be seen, increasing the defending budget yields incremental improvements on the objective function value (i.e., the weighted combination of disruption recovery efforts and commuters' inconvenience) for the system defender. From the attacker's perspective, greater disruption impacts can be achieved with more attacking budget. The results of protection decisions indicate those stations

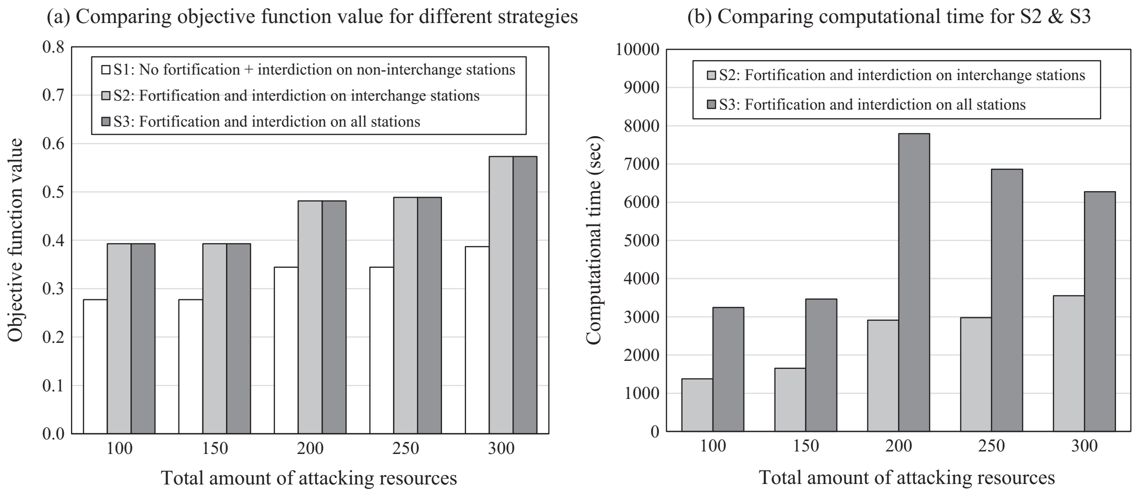

Fig. 4. Solution quality and computational efficiency comparison for different strategies.

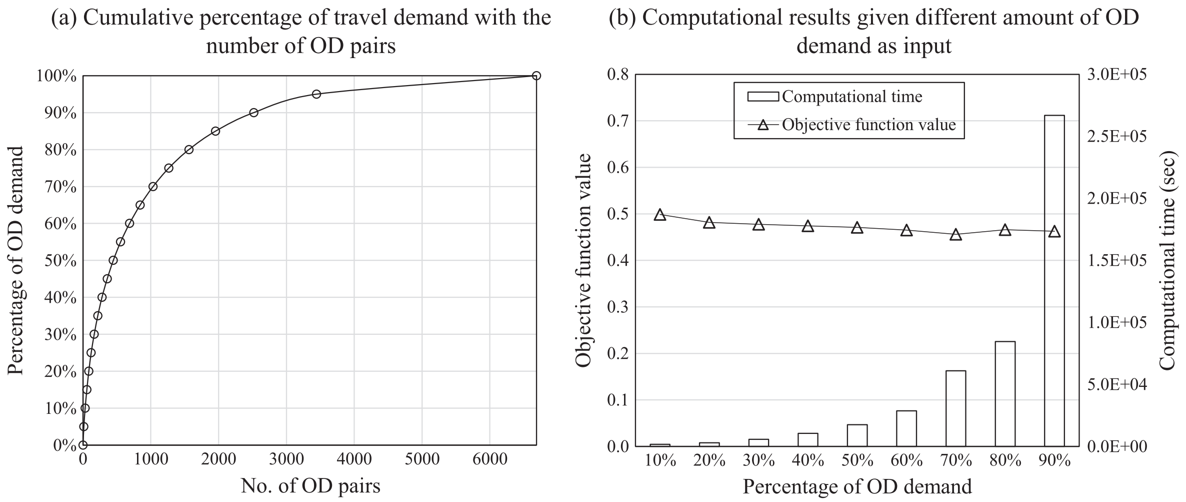

Fig. 5. Sensitivity analysis of amount of OD demand.

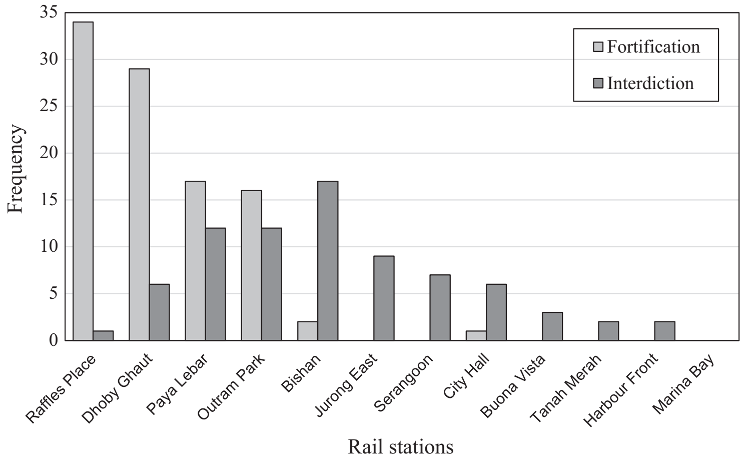

Fig. 6. Frequency with which each station appears in a fortification and interdiction set.

Table 3
Results given various defending and attacking resource budgets.

Protection budget		$Q_s = 0$	$Q_s = 100$	$Q_s = 200$	$Q_s = 300$	$Q_s = 400$
Objective function value	$T = 100$	0.575	0.568	0.401	0.393	0.381
	$T = 200$	0.667	0.596	0.523	0.482	0.451
	$T = 300$	0.754	0.672	0.664	0.573	0.512
Protection decision	$T = 100$	none	[CC1]	[EW14, CC1]	[EW8, EW14, CC1]	[EW8, EW14, EW16, NS17, CC1]
	$T = 200$	none	[CC1]	[EW14, CC1]	[EW14, EW16, CC1]	[EW8, EW14, EW16, NS17, CC1]
	$T = 300$	none	[EW14]	[EW8, EW14]	[EW14, EW16, CC1]	[EW8, EW13, EW14, NS17, CC1]
Attacking decision	$T = 100$	[[CC1],[1]]	[[EW14],[1]]	[[EW8],[1]]	[[EW16],[1]]	[[NE12],[1]]
	$T = 200$	[[EW14, EW16], [1,1]]	[[EW14, EW21], [1,1]]	[[EW13, EW16], [1,1]]	[[EW8, NE12], [1,1]]	[[EW13, NE12], [1,1]]
	$T = 300$	[[EW8, EW16, CC1], [1,1,1]]	[[EW13, EW16, NS27], [1,1,1]]	[[EW16, CC1, NE12], [1,1,1]]	[[EW8, EW24, NS17], [1,1,1]]	[[EW4, EW24, NE12], [1,1,1]]

Note: Attacking intensity index: 1 (full attack); 0 (50% partial attack).
Rail station: EW4(Tanah Merah); EW8(Paya Lebar); EW13(City Hall); EW14(Raffles Place); EW16(Outram Park); EW21(Buona Vista); EW24(Jurong East); NS17(Bishan); CC1(Dhoby Ghaut); NS27(Marina Bay); NE12(Serangoon).

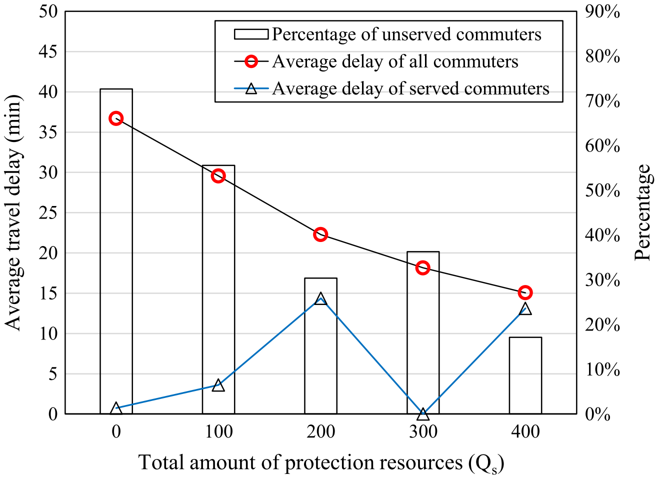

Fig. 7. Sensitivity analysis of budgets of protection resources.

{Dhoby Ghaut, Raffles Place, Paya Lebar, Outram Park} which should be given higher priorities than others when allocating protective resources. Note that those stations with higher priority for protection coincide to a large extent with those selected by the attacker for interdiction. With highest priority stations protected by the defender, the attacker will turn to the remaining stations with subsequent priority. It is also observed that the attacker prefers to focus on those selected stations and conduct greatest attacking intensity, as such attacking pattern gives rise to greater disruption impact.

In order to examine the resource allocation priority among all the rail stations, we solve the game-theoretical model with different budgets of fortification and interdiction resources, Q_s and T ranging in the sets $\{160, 190, 220, 250, 280, 310, 340\}$ and $\{100, 150, 200, 250, 300\}$, respectively. The obtained results indicate that the optimal fortification and interdiction patterns are quite similar to each other, with some key stations occurring in most of the 35 combinations. Fig. 6 presents the frequency with which each interchange rail station appears in the fortification and interdiction patterns. The stations are ordered according to the total frequency of appearing in the fortification and interdiction sets, which indicates the relative priority of stations in terms of protective resource allocation. It is observed that the frequency distribution of stations appearing in interdiction set shows a certain degree of lag behind that of stations appearing in the fortification set. This is exactly because of the effectiveness of protecting the rail stations against intentional attacks: with stations of higher priority fortified, the attacker has to turn to other stations of relative lower priority. Note that the station with the highest fortification frequency (Raffles Place) is an interchange station connecting two lines and associated with the highest inflow and outflow volume, while the station connecting three lines (Dhoby Ghaut) ranked second. It can be concluded that protective resources should be allocated to the rail network with consideration of rail stations' connectivity in the network as well as the in- and out-flow volume.

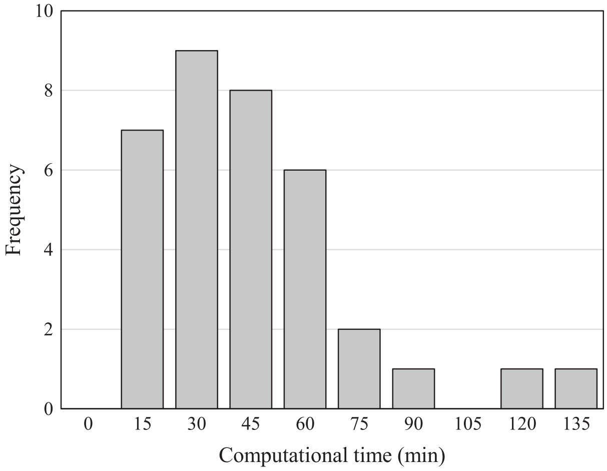

Fig. 8. Distribution of computational times with various fortification and interdiction budgets.

We now investigate the distribution of the objective function value over its components (delays to commuters, percentage not served, and response recovery effort). Fig. 7 presents the sensitivity of the protective resource's effectiveness (average delay of all commuters, average delay of served commuters, and percentage of unserved commuters) to the protective resource budgets, with 0 representing the solution that is fully open to interdiction (i.e., not protected by the defender). Note that the attacking budget is fixed to 200. The response recovery effort turns out to all be 120 under the five protection budgets. As can be seen, investing protective resources to the transit network clearly yields a significant decrease in the average travel delay of all commuters: from 36.7 to 15.1 min (or 59%). Similarly, the percentage of commuters whose travel demand cannot be fulfilled also decreases significantly: from 72.6% to 17.2%. Note, however, that the average delay of served commuters does not exhibit a clear relationship with the protection budget. This is due to the fact that the objective function of the user-level model combines the delay to served commuters and penalty for unserved commuters by a given weight parameter, and the optimal solution balances the two components. It is also observed that commuters are able to reach their final destination by making a detour if the interdicted stations are located in well-connected area, such as the CBD area with intertwined rail lines and multiple interchange stations (e.g., City Hall, Raffles Place, Outram Park, Dhoby Ghaut). However, in case that the interdicted stations are on the periphery of the rail network (e.g., Paya Lebar, Serangoon), those commuters who originally pass by the stations may not get their travel demand fulfilled.

5.5. Computational performance

Fig. 8 presents the histogram for computational times of 35 test instances given various budgets of fortification and interdiction resources. As can be seen, most of the test instances can be solved within 60 min by the proposed nested variable neighborhood search algorithm. Considering that the protective resource allocation is a decision-making problem at the strategic level, the computational efforts required by the solution approach is acceptable. We remark that the computational efficiency can be further improved by reducing the number of rail stations considered for the generation of defending and attacking solutions, and aggregating OD pairs with similar travel flow pattern.

6. Conclusions

This paper has examined the optimal allocation of protective resource in urban rail transit networks against intentional interdiction by attackers. The problem is considered as a game involving three players: the system defender deploying protective resources among vulnerable stations with the objective of minimizing the worst-case disruption impacts, the attacker interdicting rail stations in order to cause maximal recovery efforts for system defender as well as travel delay for system user, and the system user (i.e., commuters) fulfilling the travel demand in the degraded rail network. A tri-level defender–attacker–user game-theoretic model is developed and solved by a nested variable neighborhood search method.

A real-world case study based on the Singapore rail transit network and travel demand data demonstrates that the worst-case disruption impact due to intentional attacks can be significantly mitigated by deploying protective resources over critical interchange rail stations. It is also found that attackers tend to interdict those stations with large transfer and in-and-out commuter flow, and prefer to conduct greatest interdiction intensity on those selected stations. From the system defender's perspective, it is more effective if protective resources are allocated to those stations with high network connectivity and large in-and-out commuter flow. With greater network connectivity, commuters are able to reach their final destination by making detours and thus the disruption impacts can be alleviated significantly.

For future research, we are interested in considering multiple protection levels for the system defender in order to model more complex interaction of the defender–attacker game. Another promising research topic is to design effective post-disruption recovery actions (e.g., running shuttle bus services) in order to support real-time decision making for emergency response.

Acknowledgments

This research was supported by the Shanghai Philosophy and Social Sciences Foundation (2014EGL008), and the National Research Foundation Singapore through the Future Cities Laboratory. It is partially supported by the National Natural Science Foundation of China (51508325, 71401101), and the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry, China.

References

Brown, G., Carlyle, M., Salmeron, J., Wood, K., 2005. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. Tutorials Oper. Res.: Emerg. Theory Meth. Appl., 102–123

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

Chen, R.L.-Y., Cohn, A., Pinar, A., 2011. An implicit optimization approach for survivable network design. In: 2011 IEEE Network Science Workshop (NSW). IEEE, pp. 180–187.

Darmanin, T., Lim, C., Gan, H.-S., 2010. Public railway disruption recovery planning: a new recovery strategy for metro train Melbourne. In: Proceedings of the 11th Asia Pacific Industrial Engineering and Management Systems Conference, vol. 7.

De-Los-Santos, A., Laporte, G., Mesa, J.A., Perea, F., 2012. Evaluating passenger robustness in a rail transit network. Transport. Res. C: Emerg. Technol. 20 (1), 34–46.

Faturechi, R., Miller-Hooks, E., 2014. A mathematical framework for quantifying and optimizing protective actions for civil infrastructure systems. Comput.-Aided Civil Inf. Eng. 29 (8), 572–589.

Jin, J.G., Tang, L.C., Sun, L., Lee, D.-H., 2014. Enhancing metro network resilience via localized integration with bus services. Transport. Res. E: Logist. Transport. Rev. 63, 17–30.

Jin, J.G., Teo, K.M., Odoni, A.R., 2015. Optimizing bus bridging services in response to disruptions of urban transit rail networks, Transport. Sci., in press. http://dx.doi.org/10.1287/trsc.2014.0577.

Kepaptsoglou, K., Karlaftis, M., 2009. The bus bridging problem in metro operations: conceptual framework, models and algorithms. Public Transport 1 (4), 275–297.

Laporte, G., Mesa, J.A., Perea, F., 2010. A game theoretic framework for the robust railway transit network design problem. Transport. Res. B: Meth. 44 (4), 447–459.

Loukaitou-Sideris, A., Taylor, B.D., Fink, C.N., 2006. Rail transit security in an international context lessons from four cities. Urban Aff. Rev. 41 (6), 727–748.

Meyer, M.D., Belobaba, P., 1982. Contingency planning for response to urban transportation system disruptions. J. Am. Plann. Assoc. 48 (4), 454–465.

Murray-Tuite, P.M., Fei, X., 2010. A Methodology for assessing transportation network terrorism risk with attacker and defender interactions. Comput.-Aided Civil Inf. Eng. 25 (6), 396–410.

Ou, W., 2014. Analysis of the Urban Rail Transit Network Survivability Under the Terrorist Attacks, Master's thesis, Southwest Jiaotong University.

Perea, F., Puerto, J., 2013. Revisiting a game theoretic framework for the robust railway network design against intentional attacks. Eur. J. Oper. Res. 226 (2), 286–292.

Qiao, J.H., Jeong, D., Lawley, M., Richard, J.P.P., Abraham, D.M., Yih, Y., 2007. Allocating security resources to a water supply network. IIE Trans. 39 (1), 95–109.

Scaparra, M.P., Church, R.L., 2008. A bilevel mixed-integer program for critical infrastructure protection planning. Comput. Oper. Res. 35 (6), 1905–1923.

Wood, R.K., 1993. Deterministic network interdiction. Math. Comput. Modell., 0895-7177 17 (2), 1–18.

Yao, Y., Edmunds, T., Papageorgiou, D., Alvarez, R., 2007. Trilevel optimization in power network defense. IEEE Trans. Syst. Man Cybernet. C: Appl. Rev. 37 (4), 712–718.

Yen, J.Y., 1971. Finding the K shortest loopless paths in a network. Manage. Sci. 17 (11), 712–716.