Civil Engineering Infrastructures Journal xx,xx
DOI: 10.22059/ceij.2024.378678.2086

Optimal protection-response strategies for urban metro stations against malicious attacks through a game theory approach

Aref Babazadeh, Navid Khademi, Arian Behmanesh

School of Civil Engineering, College of Engineering, University of Tehran, Tehran, Iran.

Received: 16/08/2024

Revised: 09/01/2025

Accepted: 01/02/2025

Abstract

This paper introduces a defender-attacker-defender model grounded in game theory to determine optimal strategies for protecting urban rail systems against deliberate attacks on Metro stations. The model integrates four key players in a quad-level framework: the system manager, who allocates limited security resources; the attacker, who targets the most vulnerable station to maximize disruption; the system operator, who implements strategies to mitigate the impact of attacks; and the public transit passengers, whose travel behavior influences the overall network performance. The study explores four scenarios based on varying levels of protection (full or partial) and operator intelligence (intelligent or non-intelligent). Each scenario is analyzed using a tailored algorithm and applied to the public transit network of Shiraz, Iran, as a case study. The findings reveal that an intelligent operator, capable of anticipating the attacker's moves, significantly mitigates the attack's impact. Furthermore, distributing the security budget across all stations rather than focusing on a select few provides superior protection. This model offers a robust framework for developing effective defense strategies against intentional attacks on urban rail infrastructure.

Keywords: Metro system security; Game theory; Semi-flexible bus system; Bus bridging; Network vulnerability.

1. Introduction

The rail transportation system serves as the primary mode of transportation for passenger movement. The occurrence of an unforeseen disturbance within this system can yield significant consequences for the transportation network, including increased travel costs, decreased passenger satisfaction, and weakened trust in the system (Khademi et al., 2021). These repercussions have the potential to extend to subordinate transportation systems and permeate the entirety of the transportation network, providing the rationale behind prioritizing rail systems as a higher target for intelligent attackers compared to other systems. Hence, spotting and safeguarding this critical infrastructure holds significant importance and has strategic implications for nations.

The United States government safeguards critical transportation infrastructure through the "Transportation Systems Sector-Specific Plan". Developed under the National Infrastructure Protection Plan framework, this plan identifies major threats such as terrorism, cyber-attacks, and information piracy, aiming to protect the sector from such risks (CISA, 2015). Similarly, the European Union (EU) has long been engaged in safeguarding essential infrastructure, including railways, from potential terrorist activities and cyber-attacks. This effort began with initiatives like the 2008 European Critical Infrastructure Directive and has evolved into the 2022 CER Directive "on the resilience of critical entities," which emphasizes enhancing the resilience of critical infrastructure across EU member states (Pursiainen & Kytömaa, 2023).

Threats to transportation infrastructure are generally classified into two categories: (1) unintentional threats caused by human errors or natural disasters, and (2) intentional threats caused by terrorist attacks or aggressive interventions, often executed intelligently to maximize damage and disrupt system efficiency (Khademi et al., 2018). Railway systems are more susceptible to damage than other transportation systems due to their open nature, the absence of robust security measures comparable to those in airports, and the large number of users they accommodate (Strandh, 2017). In addition to strategies for preventing threats or improving resilience, it is crucial to develop methods for mitigating the damage caused by intelligent terrorist attacks (Bababeik et al., 2018). Incidents such as the Madrid train bombings in 2004, the London subway attacks in 2005, and the St. Petersburg subway assaults in 2017 illustrate strategic acts of terrorism targeting rail transportation infrastructure with the intent to inflict destruction and disruption (Strandh, 2017).

On June 7, 2017, a terrorist attack by ISIS targeted the administrative building of the parliament and the "Baharestan" Metro station in Tehran (see Figure 1), causing significant disruption. The absence of preventative measures led to the station's closure for 12 hours, affecting approximately 30,000 passengers and causing secondary repercussions on the entire Metro network and the overall transportation system of Tehran.

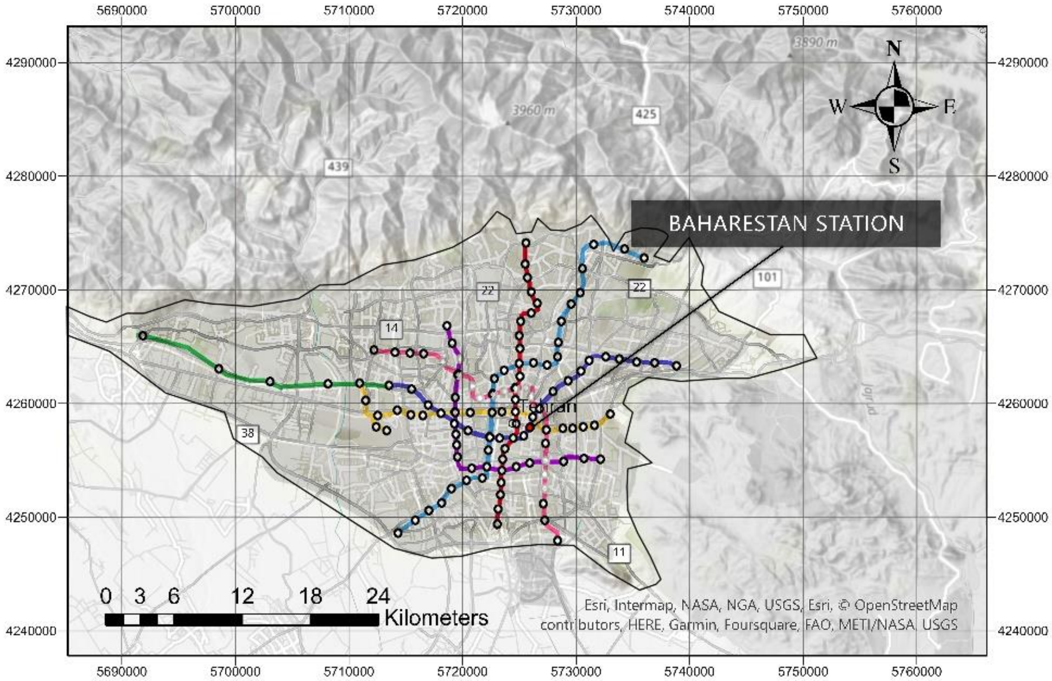

Figure 1. Tehran Metro network and the location of Baharestan station

Protecting critical infrastructure from intentional and intelligent assaults presents unique challenges compared to safeguarding against unintentional attacks. Traditional methodologies such as risk analysis and reliability may not suffice for effectively predicting the dangers associated with intelligent attacks, as these methods assume constant threat levels. In contrast, intelligent attackers adapt and modify in response to defensive measures (Li et al., 2019). Therefore, adopting a more effective approach, such as game theory, is imperative for accurately modeling the actions of an intelligent attacker accurately (Brown et al., 2006).

The utilization of defender-attacker-defender models, which fall under the category of optimization problems rooted in game theory, offers the potential to yield a near-optimal defense plan (Alderson et al., 2011). Researchers have solved the tri-level problem of allocating defense resources to implement optimal protection tactics against intelligent attackers (Alderson et al., 2011; Brown et al., 2006; Sarhadi et al., 2014). However, no studies have yet explored optimal defense mechanisms for safeguarding passenger rail transportation system components. Most previous research assumes that safeguarding system components renders them resistant to attacks, but this assumption neglects the ability of public transit system operators to predict intelligent attacks and engage in an interactive game with the attacker.

To address these challenges, this study introduces a quad-level defender-attacker-defender model tailored for public transportation systems, specifically passenger rail networks. Building on previous tri-level defense models applied to private transportation systems, our approach integrates not only the attacker and system manager but also public transit operators and passengers. This inclusion enables the modeling of dynamic operator responses, such as bus rerouting and fleet adjustments, which are critical in mitigating the impacts of disruptions. Furthermore, the study pioneers the concept of partial protection, where the defense budget is distributed across stations, reflecting realistic constraints and enhancing strategic flexibility. By employing game theory, the model effectively captures the adversarial interactions between intelligent attackers and defenders, offering innovative insights into optimizing protection strategies for public transit systems.

This article aims to develop a model that identifies vulnerable metro stations in a passenger rail transportation system to mitigate the risks associated with intelligent threats, such as terrorist attacks. By incorporating the travel time index as a metric for assessing the susceptibility of the public transit system, the model facilitates the efficient allocation of the protection resources. Optimizing travel time can contribute to multiple objectives, including enhancing safety, fostering economic growth, and improving infrastructure utilization (Afandizadeh et al., 2024). This strategic allocation seeks to reduce the likelihood of attacks on critical stations and minimize the impact of any potential disruptions. A quad-level model grounded in defender-attacker-defender game theory is employed to achieve this objective.

While current public transportation defense models often assume that no higher-level agent can anticipate lower-level agents' actions, our study highlights the need for models that account for intelligent attackers capable of adapting their strategies. By incorporating partial protection strategies and varying levels of agent intelligence, our approach not only addresses these gaps but also provides innovative and practical solutions for enhancing the security of public transportation systems.

2. Background

The safety and resilience of metro networks are critical issues in urban transportation research. Studies have used various methods and theories to assess vulnerabilities to disruptions. Zhu et al. (2018) showed that targeted attacks on nodes with high betweenness centrality can severely impact metro network functionality. Their findings emphasized the importance of implementing protection strategies focused on loop lines and transfer stations to improve network robustness. Similarly, Xu et al. (2019) developed a new analytical framework to assess the vulnerability of subway networks. Their findings revealed that although these networks are highly resistant to random failures, they are particularly vulnerable to intentional attacks on key hub stations.

Wang et al. (2017) expanded the understanding of metro network robustness by conducting a global analysis of 33 metro systems. They revealed that resilience is not solely determined by network topology but also by the strategic placement of transfer stations and the provision of alternative routes. These findings underscore the importance of planning for redundancy in transportation networks to mitigate potential disruptions.

Building on these studies, Xu and Chopra (2023) investigated the impact of interconnectedness on the resilience of multimodal public transportation systems. They found that integrating bus and metro networks through inter-layer coupling enhances overall system robustness by reducing topological vulnerabilities and increasing attack tolerance. This integration is particularly advantageous in geographically constrained urban environments, such as mountain cities, where it fosters a safe-to-fail system design. Ma et al. (2020) further advanced this perspective by developing a robust model for a dual-layer Bus-Subway network. Their findings indicated that resilience can be significantly improved by increasing station capacities and addressing cascading failure mechanisms, providing actionable insights for designing more robust multi-modal transportation systems.

Implementing integrated planning for rail and bus transportation systems significantly enhances the efficiency and adaptability of public transit systems, thereby promoting urban sustainability (Yang & Liang, 2023). Bus systems, designed to operate within a city's street network, offer a flexible transportation option that is not restricted to fixed routes, unlike rail systems. This flexibility allows buses to serve as viable alternatives to rail systems during emergencies by navigating safe, alternative routes. Strategies such as the semi-flexible bus system and bus bridging system can mitigate disruptions in the rail network.

2.1. Semi-flexible Bus System

Semi-flexible transportation systems combine traditional and on-demand system attributes, typically involving predetermined routes and timetables while allowing some level of flexibility (Yoon et al., 2022). According to Errico et al. (2013), these systems can be classified based on their structure. This study focuses on the route deviation method, where vehicles operate along a predetermined route and timetable but are able to detour temporarily to accommodate passenger pickups or drop-offs before resuming their original route. This system is particularly effective in managing increased travel demand during rail system crises, such as terrorist attacks.

Mehran et al. (2020) provides analytical models to compare the operational costs of regular bus and semi-flexible transit systems, emphasizing the importance of demand type and usage area. Vansteenwegen et al. (2022) examined the effectiveness of a demand-responsive semi-flexible feeder bus system in scenarios where deviations occur at one or two stations. Mishra and Mehran (2023) explored optimizing service headway and slack time for route deviation, providing insights into operational costs, user costs, and service benefits. Their research assessed the impacts of factors such as vehicle capacity, demand levels, route deviation limits, and weather conditions on system efficiency and cost-effectiveness.

This study investigates the role of semi-flexible bus transportation systems in managing passenger demand during rail transportation crises, focusing on criteria for establishing new bus stops near disrupted Metro stations to transition remaining rail system passengers to the existing urban bus network.

2.2. Bus bridging

Bus bridging is frequently employed to accommodate rail network passengers during planned or unforeseen interruptions. This approach involves establishing temporary bus services to connect affected Metro stations with nearby stations in the public transit network. Unlike the semi-flexible bus system, bus bridging primarily serves as a temporary measure designed to address rail transportation infrastructure impairments during maintenance and repairs.

Numerous studies have explored restoring interrupted rail systems through bus bridging. Currie and Muir (2017) concluded that bus bridging could efficiently meet demand during disruptions when other forms of urban transportation are insufficient. Jingfeng et al. (2017) introduced passenger flow management and bus bridging strategies to mitigate subway overcrowding. Zhang et al. (2024) proposed an optimized bus bridging route design that considers the number of stations and available resources. Yang et al. (2018) assessed the impact of bus bridging lines during rail disruptions. Liang et al. (2019) developed a robust, flexible bus bridging system to mitigate rail transportation network disruptions. Aboudina et al. (2021) proposed a detailed methodology for deploying shuttle bus services during metro disruptions, emphasizing maximizing the efficiency of shuttle service.

This study evaluates the effectiveness of bus bridging in assisting passengers stranded at disrupted Metro stations, establishes temporary bus routes to connect these stations to nearby public transit stations, and addresses the regulation of bus frequency to ensure a consistent schedule.

2.3. Tri-level programing model

Game theory has been extensively developed in transportation studies to predict network damage from attacks and formulate reactive and proactive strategies. This methodology employs either two-level (defender-attacker) models or tri-level (defender-attacker-defender) optimization models to identify system vulnerabilities or strategize optimal safeguarding. The existing two-level attacker-defender model, commonly referred to as the "interdiction model," has been modified to incorporate a tri-level defender-attacker-defender model for determining the optimal defense strategy (Brown et al., 2006).

2.3.1. Defender-attacker-defender models

The defender-attacker-defender model is a tri-level optimization problem that aims to identify the most critical assets within a transportation system. By considering a restricted defense budget, this model can provide a near-optimal defensive strategy. The two-level attacker-defender model is theoretically embedded in the tri-level defense design model of defender-attacker-defender (Yamany et al., 2020). In this tri-level problem, the attacker's potential benefits are minimized by the high-level defender adopting optimal defense strategies.

In a road transportation system, private car users are low-level defenders, adjusting their travel strategy to reduce incurred costs when an attack disrupts the system. In public transit systems, system operators are low-level defenders who can implement short-term changes to the network's structure to devise the most effective countermeasures against assaults and mitigate system damage. Finally, the high-level defender is the system manager or owner, who assesses the actions of the attacker and the low-level defender and implements the most effective defensive tactics within budgetary constraints to minimize the costs resulting from potential attacks.

Numerous studies have investigated the application of tri-level models grounded in game theory to develop optimal defense mechanisms against intentional attacks. Brown et al. (2008) proposed a tri-level model to identify the optimal defense strategy for safeguarding important national organizations against attacks, considering financial limitations. Sarhadi et al. (2014) introduced a tri-level game framework involving a network manager, an attacker, and a network operator to assess the vulnerability of specific rail-truck intermodal terminals to terrorist threats. Yang et al. (2018) proposed a three-player game including the urban rail transport network manager, the attacker, and the operator to address safeguarding the connectivity of the rail system with the public transit network. Chen et al. (2018) applied game theory to examine how players' behavior affects decision-making in strategic investment scenarios.

2.4. Research gap and contribution

Tri-level defender-attacker-defender models based on game theory are recognized for their ability to yield near-optimal defense strategies and have predominantly been applied to private transportation networks. Researchers like Brown et al. (2008), Alderson et al. (2011), and Zhang et al. (2018) have explored tri-level resource allocation to determine the best defensive strategies against intelligent attacks on these networks. Similar tri-level defense models have been applied to cargo transport systems, such as the work by Sarhadi et al. (2014) on rail intermodal terminal networks and Chen et al. (2018) on container transportation networks, to counter unforeseen attacks and identify optimal defensive strategies. However, in contrast to private transportation systems, public networks allow the operator at the lowest level to implement temporary coping strategies that improve the functionality of the disrupted network.

To the best of our knowledge, no existing studies have addressed the optimal defense design for public transportation systems with a focus on passengers. Our study introduces a game-theory-based defense model specifically designed to protect passenger rail systems and mitigate the effects of disruptions caused by intelligent attacks to Metro stations. Game theory was chosen for its ability to model strategic interactions between rational entities (Khalid et al., 2023), which is central to this study's objective of analyzing intentional attacks on urban rail systems. Unlike risk assessment frameworks (Akinrolabu et al., 2019) or simulation modeling (Bešinović, 2020), game theory explicitly captures the dynamic interplay between attackers and defenders, enabling the design of optimal strategies under varying scenarios. Additionally, while graph theory (Pirbhulal et al., 2021) and machine learning (Talpur & Gurusamy, 2022) are valuable for other contexts, they lack the capacity to address the adversarial and decision-based nature of this problem. In our proposed model, the network operator at the lowest level solves a bi-level bus frequency setting problem, effectively transforming the problem into a quad-level game theory model. This model includes not only the system manager and the attacker but also the users and operators. It employs a congested transit assignment model as the lower-level problem within the frequency setting model, distinguishing it from the uncongested assignment models commonly found in existing literature. Moreover, we address the proposed defense model with varying levels of agent intelligence, including their ability to anticipate the behavior of higher-level actors before taking action.

The proposed approach also provides the operator with practical improvement strategies for the public transport network following the deactivation of a station. The operator is empowered to adjust the bus network, whether through fleet relocation or route deviation, to minimize the impacts of disruption. While few previous studies have mathematically examined bus bridging or semi-flexible bus systems— which are often described only qualitatively—our model incorporates these strategies directly into the operator's problem, enabling precise network adjustments in response to an attack.

The ultimate objective of optimal defense models in transportation systems is to identify and prioritize system components vulnerable potential threats and determine optimal budget allocation for their protection. Previous studies on defense models typically assumed that any protected component would be immune to attacks if the system manager employed protective strategies, a concept referred to as "full protection". Our study introduces the concept of "partial protection," where the level of protection—and consequently, the probability of a successful attack—is directly proportional to the budget allocated to a Metro station. This approach offers a wider range of defensive strategies and transforms the leader-follower game between the system manager and the attacker into a non-cooperative zero-sum game, potentially resulting in more effective protection outcomes.

3. Methodology

Consider a hypothetical small public transit system depicted in Figure 2(a). This system consists of a one-directional street with 5 nodes and 4 links, allowing mobility exclusively by walking or utilizing bus and subway transit. There is a bus route at ground level that includes stops at nodes 1, 2, 4, and 5. Additionally, there is an underground Metro line running beneath this street, which has three stations that emerge at street level at nodes 1, 3, and 5. Because the bus, Metro, and street routes overlap, as is common in real-world scenarios, the transit routes are expanded by incorporating route and station data from subway and bus lines, so that the transit system is represented as an equivalent graph called a “transit network” (Spiess & Florian, 1989). The transit network corresponding to the aforementioned small transit system is shown in Figure 2(b). This representation depicts all potential movements a passenger may have within the transit system illustrated in Figure 2(a), including walking, boarding, in-vehicle, and alighting movements.

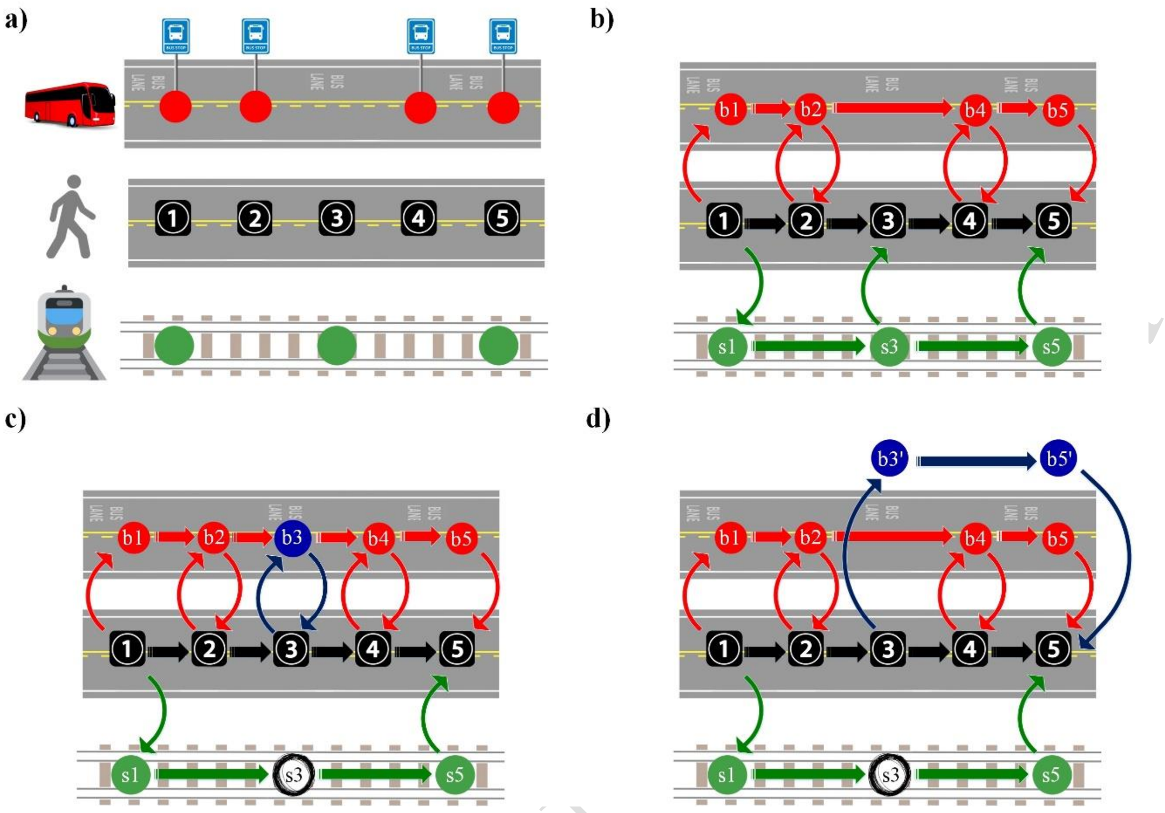

Figure 2. **(a)** A hypothetical public transit system; **(b)** The public transit network for this hypothetical system; **(c)** The operator's strategy to modify the transit network by creating a new bus stop; and **(d)** The operator's strategy to modify the transit network by creating a new bus line

As mentioned above, in the proposed model of this research, three players —the system manager, the attacker, and the operator— engage in a three-person game. Assuming that the Metro station s3, as shown in Figure 2(b), is targeted by an attacker, this station should be eliminated from the transit network to prevent passengers from disembarking there. The low-level defender (operator) can effectively respond to the attack and mitigate the increase in travel time resulting from the attack by removing the station s3 from the Metro network. This disruption can be compensated for by utilizing the potential of the existing bus network and implementing an optimal coping strategy. Figures 2(c) and 2(d) depict two examples of strategies that the operator can employ to enhance the damaged network. The first strategy, as depicted in Figure 2(c), involves establishing a new bus station at node 3 to cater to the remaining subway passengers at this station. The second approach, illustrated in Figure 2(d), involves establishing a bus bridge between nodes 3 and 5. This enables the passengers from Metro station s3 to utilize this new line to reach their destination.

3.1. Formulation of the quad-level game

3.1.1. Passengers and operator

The operator is at the lowest level of the game (the third level). Using the existing bus system, the operator can improve the total travel time of the public transit system (including the rail and bus network) in the event of an attack that results in the destruction of a Metro station. The operator's coping strategies against terrorist attacks on Metro stations are classified into three categories:

1. Redistributing the existing bus fleet between lines and resetting the frequency of existing bus lines without changing the number of lines or their routes.
2. Adding a new bus line to the network connecting the nearest bus station to the attacked Metro station, or creating a new bus line linking the attacked Metro station and other Metro stations, and accordingly resetting the frequency of the bus lines.
3. Altering the route of one of the existing bus lines towards the target Metro station to cover the passengers from that station and then rescheduling the bus lines.

The operator solves the problem of adjusting bus line frequencies for any given state of the public transit system by using an improved version of the method developed by Constantin and Florian (1995). The mathematical model of the operator's (OP) problem is as follows:

$$OP\left\{\begin{array}{l} FS(x,w)\left\{\begin{array}{l}\min\limits_{F}\ TC = \sum\limits_{a\in A} h_a . t_a(x_a) . x_a \ + \sum\limits_{p\in P} w_p \\ \text{s.t.} \\ \qquad \sum\limits_{l\in L} F_l . T_l(x) \le N_b \\ \qquad \underline{F} \le F_l \le \overline{F} \qquad \forall\, l\in L\end{array}\right. \\ TA(F)\left\{\begin{array}{l} \min\limits_{x,w} Z = \sum\limits_{a\in A}\int_0^{x_a} h_a . t_a(u)\, du \ + \sum\limits_{p\in P} w_p \\ \text{s.t.} \\ \qquad \sum\limits_{a\in A_n^+} x_a - \sum\limits_{a\in A_n^-} x_a = d_p \qquad \forall\, n\in N \\ \qquad x_a \le F_a . w_p \quad \forall\, a\in A , p\in P \\ \qquad x_a \ge 0 \qquad \forall\, a\in A\end{array}\right.\end{array}\right. \tag{1}$$

The problem OP is a bi-level programming model where the upper-level problem FS is the frequency setting (FS) problem which aims to determine the frequency vector $F = (F_l)$ by minimizing the total travel time (TC) of the passengers (sum of the passengers' travel times on links and waiting times at stations), considering that the passenger flows x_a and the waiting times w_p are the solution of the lower-level transit assignment (TA) problem TA for any given F. The first constraint of the problem FS applies the limitation of the existing bus fleet, and the second constraint specifies the upper and lower limits for the bus line frequencies. All mathematical notations used in the model above and the subsequent relationships are provided in Appendix 1.

Constantin and Florian (1995) used the TA model by Spiess and Florian (1989) as the lower-level problem of their FS model. This represents an uncongested model where the travel times $t_a(x_a)$ are fixed values, so the capacity of the bus line is not considered. In contrast, the proposed model OP is a congested model, where $t_a(x_a)$ being a function of x_a. This allows passenger flows to be restricted below the line capacities by imposing the following penalty function to the travel times $t_a(x_a)$ of in-vehicle links using the following penalty function:

$$\tau_a(x_a)\begin{cases} \dfrac{\rho}{1-\dfrac{x_a}{c_a}} & if\ \dfrac{x_a}{c_a} < 1-\rho \\ \alpha\dfrac{x_a}{c_a}-\beta & if\ \dfrac{x_a}{c_a} > 1-\rho \end{cases} \tag{2}$$

where c_a is the capacity of link a, ρ is a small parameter, and α and β are positive values selected to ensure the penalty function $\tau_a(x_a)$ becomes continuously differentiable (we use $\rho = 0.005$, $\alpha = 200$, and $\beta = 198$). It can be easily seen that τ_a increases slowly when $\frac{x_a}{c_a}$ approaches 0.995 and then abruptly increases. Due to this function, the line travel times T_l (i.e., the sum of in-vehicle travel times of each line $l \in L$) are also functions of link flow vector $x = (x_a)$.

It is worth mentioning that the problem OP can be solved considering both the attacker's and the operator's strategies. The transit network can be adjusted for any attack by removing boarding and alighting links at the target station. To do this, while keeping the problem's general form, a binary parameter $h = (h_a)$ has been added to the frequency setting model FS to allow for changes in the disrupted transit network structure at each stage of the attacker and operator's game. After the attacker selects the target Metro station, $h_a = BN$ (BN is a large number) is set for the boarding and alighting links connected to that station, and $h_a = 1$ for other links in the transit network. Consequently, the travel times for the boarding and alighting links at the disrupted station become very large, making the flow on these two links zero in the final solution of the OP problem. Any strategy j of the attacker is distinguished with a specific vector $h_j = (h_{aj})$. To cope with this attack, the notation h_a in both FS and TA models should be replaced with h_{aj}. Additionally, each coping strategy of the operator, such as adding a bus line or a bus station, is applied by using the corresponding bus set L_k and station set P_k instead of the sets L and P within the models.

The mathematical model of the operator's problem is in the following form

$$ET_j = \min_{k\in K_j}\{ET_{j,k}\} \tag{3}$$

where

$$ET_{j,k} = TC_{j,k} - TC_0 \tag{4}$$

$ET_{j,k}$ is the attacker's gain (i.e., the increase in passenger travel time) from attack j, considering the operator's coping strategy $k \in K_j$ that aims to mitigate the negative effect of the attack; $TC_{j,k}$ is the objective function value of the FS problem with $h = h_j$, $L = L_k$ and $P = P_k$; TC_0 is the objective function value of the same problem for the system in its normal (not attacked) state. ET_j represents the minimized expected travel time increase, indicating the effectiveness of the operator’s strategy in minimizing the attacker’s gain.

In this article, we consider two perspectives on the operator's performance in mitigating the impact of Metro station destruction and responding to threats from the attacker. In the first perspective, the operator lacks information on the attacker's intentions and can only devise a defensive plan after the target station is attacked and destroyed. In the second perspective, the operator demonstrates intelligent behavior by skillfully managing the attacker's choices and accurately anticipating the attacker's actions before the attack. In both approaches, the operator solves the OP problem. However, the key difference is that in the first approach, the interaction between the attacker and the operator is modeled as a leader-follower game, while in the second approach, the operator engages in a non-cooperative, two-player game with the attacker. In Section 3.2, scenarios based on whether the operator is intelligent or not are defined, and the solution methods for the defense design problem at each stage of the game between the operator and the attacker are explained.

An iterative method is used to solve the OP problem. Starting from an initial feasible F, the TA model is solved for x and w. Then, with these variables fixed, the FS problem is solved to find a new F. This process continues sequentially until a convergence condition is met.

3.1.2. Attacker

The attacker plays in the middle level (second level) of the game and possesses the ability to increase the travel time of the public transit system as much as possible by making smart attacks on a Metro station. It is important to highlight that the attacked line became completely inoperative in cases where an attacker deliberately damaged a section of the line through acts of sabotage, such as detonating a bomb inside a train carriage or near the rails. However, based on available evidence, stations are frequently the focus of terrorist attacks. Therefore, this article assumes that the attacker's objective is to maximize the overall travel time in the public transit system by targeting the most crucial Metro station in the rail system and making it inoperable. In this scenario, passengers are unable to use the target station to access the Metro line; however, the line remains operational, and the fleet continues to travel along the predetermined route without stopping at that station.

The mathematical model of the attacker's problem is in the following form

$$ET^i = \max_{j\in M-M_i}\{ET_j\} = \max_{j\in M-M_i}\min_{k\in K_j}\{ET_{j,k}\} \tag{5}$$

where $M \subset P$ is the set of Metro stations, $M_i \subset M$ is the set of Metro stations protected by the system manager’s defense strategy i; and K_j is the set of operator's coping strategies (such as adding a bus line or station, adjusting bus line frequencies, and rescheduling bus routes) in response to the attack on station $j \in M_i$. ET^i represents the maximum gain the attacker can achieve (i.e., the increase in passenger travel time) after accounting for the operator's optimal coping strategies across all unprotected stations.

During each phase of the game, the system manager determined the defense strategy $i \in I$ to enhance the protection level of the Metro stations within the allocated budget, where I is the set of all feasible strategies of the system manager (i.e., all subsets of Metro station set M). Subsequently, the attacker selected a strategy $j \in M - M_i$ to target the Metro stations, aiming to cause the largest possible increase in travel time for the public transit system. In the same way, the operator follows a coping strategy $k \in K_j$ to mitigate the negative effect of the attack by the attacker.

3.1.3. Manager

The system manager, positioned at the highest level of the game (the first level), strategically selected crucial Metro stations to enhance the level of protection within the constraints of the budget limit. The objective was to minimize the cost to the system in the event of a targeted attack on a Metro station. In general, it was presumed that the system manager possessed a high level of intelligence and could accurately anticipate the actions and choices of both the operator and the attacker. Consequently, the game between the system manager and the other players was always structured as a leader-follower game.

The mathematical model of the manager's problem is as

$$ET = \min_{i \in I}\{ET^i\} = \min_{i \in I} \max_{j \in M - M_i}\{ET_j\} = \min_{i \in I} \max_{j \in M - M_i} \min_{k \in K_j}\{ET_{j,k}\} \qquad (6)$$

ET represents the minimum gain for the attacker (i.e., the smallest increase in passenger travel time) under the system manager's best protective strategy against the attacker's worst-case strategy of targeting one of the unprotected stations. All other notations remain as previously defined.

According to Eq. 6, during each phase of the game, the system manager selects one or more stations to protect from terrorist attacks, taking into account the available budget. By analyzing the behavior of the operator and the attacker and predicting the increase in system travel time under each protective scenario, the manager seeks to minimize the maximum travel time imposed on the public transit system, thereby achieving the most optimal outcome.

This research assumes that the system manager can implement protective measures in two distinct ways:

– *Full protection:* In this scenario, the system manager allocates the existing budget to various crucial stations to eliminate the possibility of attacks on those stations. As a result, the attacker can only target vulnerable stations and cause damage to them. The main goal of the system manager is to identify the most critical stations within the railway network in in case of sabotage attacks and implement comprehensive measures to safeguard them, thereby minimizing the extent of disruption caused by such attacks.

- *Partial protection:* In this approach, the system manager allocates the budget across all stations to enhance their protection levels and minimize the potential impact of an attack on the rail network by reducing the likelihood of its success. In this case, the attacker can target any of the Metro stations, but the probability of a successful attack on each station depends on the amount spent on its protection. The system manager's main objective is to determine the most effective level of protection for each station and to optimally distribute the budget to achieve this goal.

Finally, the quad-level game in this article is created with the following assumptions:

- The system manager has a limited budget to protect Metro stations from terrorist attacks. Allocating this budget reduces the probability of an attack on the stations.
- The attacker targets only one Metro station, aiming to disrupt its entire operation upon a successful attack.
- If a Metro station is attacked, passengers will be unable to board or alight at that station.
- In addition to the rail transportation system, there is a bus transportation system that can serve as an alternative in the event of an attack or damage to the rail network. This system can efficiently transport displaced passengers ensuring the uninterrupted operation of the public transit network.
- The operating costs of the operator's protection strategies and the bus fleet capacity limitation are excluded.
- The number of buses in the network is constant. Consequently, it is not possible to increase the number of buses in the public transit system during the disruption, and the operator can only relocate the fleet among existing or newly established lines.

3.2. Suggested scenarios and solution algorithms

In Section 3.1, the problem of determining the optimal defense strategy against terrorist attacks on Metro stations is introduced as a complex four-player game involving the system manager, the attacker, the operator, and the transit passengers. The game is structured as a hierarchical, multi-level optimization model, where the system manager serves as the ultimate decision-maker. At the subsequent levels, the attacker and the operator are engaged in a competitive interaction: the attacker aims to disrupt the public transit system by increasing passenger travel time, while the operator aims to counteract these disruptions by minimizing network delays, taking into account the behavior of the passengers. The effectiveness of the system manager's protection strategy is crucial in shaping the outcomes of this dynamic interaction.

This paper examines four distinct scenarios within the defender-attacker-defender framework, considering two modes of protection employed by the system manager and two intelligence levels for the operator's responses (refer to Table 1). These scenarios provide a comprehensive analysis of the strategic interactions between the players and underscore the importance of adaptive defense strategies in the face of intelligent adversaries.

In scenarios 1 and 2, the allocation of protection budget to Metro stations is carried out in a manner that ensures complete protection, effectively making it impossible for an attack to be attempted on those stations. Consequently, the likelihood of an assailant attacking the protected stations is considered to be zero (full protection). However, in scenarios 3 and 4, the likelihood of attacking Metro stations is influenced by the amount of budget allocated to their protection (partial protection). As a result, it remains possible to target stations that are protected, except for those that have received sufficient budget to achieve full protection.

In scenarios 1 and 3, it is assumed that the operator cannot anticipate the attacker's actions before the assault (unintelligent operator). This implies that the attacker can predict the operator's coping strategy. However, in scenarios 2 and 4, it is assumed that the operator can anticipate the attacker's behavior before the attack (intelligent operator). In these scenarios, while the attacker is aware of the operator's strategies to counter the attack on each station, they cannot predict with certainty the operator's specific countermeasures at the time of the attack.

Table 1
Defense scenarios based on player behave in the defender-attacker-defender game

Scenario	Protection type		Players	
		Operator	Attacker	Manager
			Intelligence against	
1	Full protection	-	Operator	Operator and Attacker
2	Full protection	Attacker	Operator	Operator and Attacker
3	Partial protection	-	Operator	Operator and Attacker
4	Partial protection	Attacker	Operator	Operator and Attacker

3.2.1. Scenario 1: Full protection with unintelligent operator

In this scenario, the quad-level problem is structured as two leader-follower games: one between the system manager and the attacker, and the other between the attacker and the operator. The system manager is fully aware of both the attacker’s and the operator’s behaviors, while the attacker understands the operator’s actions. Initially, the manager selects combinations of Metro stations for full protection within the constraints of the budget and evaluates the potential reactions of both the attacker and the operator. The attacker, aware of the operator’s limitations, then targets the most vulnerable stations based on the manager’s defense strategies and anticipates the operator’s response. The operator, unable to foresee the attacker’s plans, reacts post-attack by evaluating available tactics and selecting the most effective strategy for each attacked station. Through iterative analysis, the manager identifies the stations most at risk and prioritizes them for full protection.

At the lowest level, the operator evaluates the impact on travel time in the public transit network by solving the OP problem using Eq. 4, considering the destruction of Metro station j and the implementation of the chosen strategy. Eq. 3 calculates the minimum possible increase in travel time after the destruction of Metro station j and the application of the operator's optimal strategy. For each protection scenario i, the manager aims to achieve the minimum increase in travel time across the network by fully protecting a selected set of stations. Naturally, for those stations that are fully protected ($j \in M_i$), this increase in travel time is effectively zero.

At the middle level, the attacker determines the maximum potential increase in travel time on the public transit network using Eq. 5, considering the optimal coping -strategy for each station. At the highest level, the system manager uses Eq. 6 to find the minimum possible increase in travel time resulting from an attack on the most vulnerable station, while considering the most effective coping strategy.

3.2.2. Scenario 2: Full protection with intelligent operator

In this scenario, the quad-level problem is formulated as a leader-follower game between the system manager and the other players, with a non-cooperative zero-sum game between the attacker and the operator. The system manager is aware of the behaviors of both the attacker and the operator. Additionally, both the attacker and the operator can anticipate each other's actions in advance. Initially, the manager operates similarly to Scenario 1, selecting combinations of Metro stations to fully protect. Then, the attacker and operator engage in a non-cooperative, zero-sum game to evaluate the effectiveness of the manager's defense strategies. This interaction helps determine the probability of the attacker attacking each unprotected station. By analyzing various station sets and considering potential attacks on vulnerable stations, the manager ultimately selects the set that minimizes the anticipated increase in travel time for the public transit system caused by an attack, thereby identifying the optimal stations for full protection.

At the start of the game between the attacker and the operator, for each protection strategy i, the attacker sets the probability of attacking the protected stations to zero, and the probability of attacking the unprotected stations to an equal value of $q_j^1 = 1/(m - m_i))$, where $m = |M|$ is the total number of Metro stations, and $m_i = |M_i|$ is the number of stations that can be fully protected within the available budget (total budget index units). The operator calculates the change in travel time on the public transit network and identifies the smallest increase in travel time following the destruction of Metro station j by solving the OP problem using Eqs. 3 and 4.

During each phase of the game between the lowest and the middle levels, and for a given protection scenario i, the operator first estimates the expected increase in network travel time resulting from an attack on each station without implementing any coping strategy, $\widehat{\overline{ET}}_j^i$, using Eq. 7:

$$\widehat{\overline{ET}}_j^i = q_j^i.\overline{ET}_j \tag{7}$$

where $\overline{ET}_j$ represents the increase in network travel time if the attacker targets station j and the operator does not implement a copying strategy. The attacker then, recognizing that the operator will apply the optimal coping strategy to the most critical station, estimates the expected increase in network travel time due to the destruction of this critical station, considering the operator's optimal strategy, $\widehat{ET}_j^i$, using Eq. 8:

$$\widehat{ET}_j^i = q_j^i . ET_j \tag{8}$$

At the end of each phase of the game, the attacker compares the values of $\widehat{ET}_j^i$ for the critical station with $\widehat{\widehat{ET}}_j^i$ for the other stations. Based on this comparison, the attacker selects the station with the highest priority for the next attack. The probability of attacking the unprotected stations is then updated using Eq. 9:

$$q_j^i = \frac{t}{t+1} \times q_j^i + \frac{1}{t+1} \times \tilde{q}_j^i \tag{9}$$

In this equation, $\tilde{q}_j^i$ an auxiliary variable that, during each phase of the game between the attacker and the operator, is assigned a value of one for the station identified as the highest priority target for the next attack and a value of zero for all other stations.

After determining the final attack probability vector at the end of the game, the attacker calculates the expected increase in travel time caused by the destruction of Metro stations for each protection scenario i, considering the implementation of the optimal strategy for each station, using Eq. 10:

$$\widehat{ET}^i = \sum_j \widehat{ET}_j^i = \sum_j q_j^i . ET_j \tag{10}$$

where $\widehat{ET}^i$ represents the maximum expected increase in network travel time that the attacker anticipates, given the system manager's protection of station set i.

Finally, at the highest level, the manager employs Eq. 11 to determine the minimal anticipated increase in travel time within the public transit network resulting from an attack, while taking into account the operator's optimal strategy to mitigate the impact:

$$ET = \min_i \{\widehat{ET}^i\} = \min_i \sum_j \widehat{ET}_j^i = \min_i \sum_j q_j^i . ET_j \tag{11}$$

3.2.3. Scenario 3: Partial protection with unintelligent operator

In this scenario, the quad-level problem is structured as a non-cooperative, zero-sum game between the system manager and the attacker, with a leader-follower game between the attacker and the operator. The manager’s actions are unpredictable to the attacker, and the manager, in turn, cannot fully anticipate the attacker's behavior. However, the attacker has full knowledge of the operator's likely responses. Initially, the manager and the attacker engage in a non-cooperative, zero-sum game to determine the probability of a successful attack on each station, based on the optimal distribution of the protection budget. The manager allocates the protection budget across all Metro stations. After observing this budget allocation, the attacker selects potential stations for attack and evaluates the operator's possible responses. The operator then counters the attacks by selecting the most effective strategies to mitigate disruption at each targeted station. Similar to Scenario 1, at the lowest level of the game, the operator calculates the increase in travel time on the public transit network following the destruction of a Metro station j by implementing the optimal strategy for that station, using the OP problem and Eqs. 3 and 4.

In this article, instead of using the actual protection budget in the equations, a protection budget index is employed. The protection budget index for each station is defined as the ratio of the allocated protection budget for that station to the full protection budget required for a single station. Since the allocated budget for any station cannot exceed the full protection budget, the protection budget index for all Metro stations will always be a value between zero and one.

To calculate the probability of an attacker's success in targeting the stations, it is necessary to define a relationship between the protection budget index allocated by the manager to each station and the probability of success in attacking that station. This relationship should satisfy the following conditions:

- As the protection budget for a station increases, the probability of the attacker's success decreases.
- The maximum protection budget for each station is equal to the cost of complete protection, which is equivalent to one unit of the budget index.
- If no budget is allocated for station protection, the probability of the attacker's success in destroying it is one.
- If one unit of the budget index is allocated to protect the station, the probability of the attacker succeeding in destroying it is zero.
- As the station protection budget index increases from 0 to 1, the probability of the attacker’s success decreases rapidly at first; however, the rate of decrease gradually slows until it reaches zero.

In this article, the relationship between the protection budget index and the probability of a successful attack on each station $j \in M$ is suggested as follows:

$$r_j = 1 - \sqrt{1 - \left(c_j - 1\right)^2} \qquad 0 \le c_j \le 1,\ 0 \le r_j \le 1 \tag{12}$$

where c_j and r_j denote the protection budget index allocated to station j, and r_j represents the probability of a successful attack on that station. This equation, incorporating the characteristics outlined above, effectively models the relationship between the probability of the attacker's success and the protection budget index of the station.

At the start of the game between the manager and the attacker, the manager distributes the available budget evenly among all Metro stations. The defense strategy ii provides the manager with a budget sufficient to fully protect m_i stations out of a total of $m = |M|$ stations (i.e., the total units of the protection budget index available to the manager is equal to m_i). Thus, in the first iteration of the partial protection scenario, the manager distributes this budget equally among all m stations. Denoting by c_j^{ii} the protection budget index assigned to Metro station j in iteration ii of the game, we set $c_j^1 = \frac{m_i}{m}$ for all $j \in M$.

In each phase of the game, the attacker calculates the probability of a successful attack on each Metro station (r_j^{ii}) based on the budget allocated to them using Eq. 12 and then computes the anticipated increase in travel time on the public transit network after destroying Metro station j, considering the likelihood of a successful attack while the operator implements the optimal strategy. This is done using Eqs. 13 and 14:

$$\widehat{ET}_j^{ii} = r_j^{ii}.ET_j \tag{13}$$

$$\widehat{ET}^{ii} = \max_j\{\widehat{ET}_j^{ii}\} \tag{14}$$

where $\widehat{ET}_j^{ii}$ represents the expected increase in network travel time in iteration ii of the game between the attacker and the manager, considering an attack on Metro station j and the implementation of the operator's optimal coping strategy, and $\widehat{ET}^{ii}$ denotes the maximum expected increase in network travel time in iteration ii if the attacker targets the most critical Metro station.

After identifying the critical station at the end of each phase of the game, the manager updates the protection budget indices for the stations using Eq. 15:

$$c_j^{ii} = \frac{ii}{ii+1} \cdot c_j^{ii} + \frac{1}{ii+1} \cdot \tilde{c}_j^{ii} \tag{15}$$

In this equation, $\tilde{c}_j^{ii}$ is an auxiliary variable set to one for the critical station and zero for all other stations during each phase of the game between the manager and the attacker. Considering that the budget index for station protection cannot exceed 1, at each stage of the game, if any of the c_j^{ii} values surpass 1, the vector (c_j^{ii}) for $j \in M$ is modified again using Eqs. 16 and 17:

$$c_{max}^{ii} = \max_j\{c_j^{ii}\} \tag{16}$$

$$c_j^{ii} = \begin{cases} 1 & if \quad c_j^{ii} > 1 \\ c_j^{ii} + \dfrac{c_{max}^{ii} - 1}{j - 1} & if \;\; 0 \leq c_j^{ii} \leq 1 \end{cases} \tag{17}$$

Through iterative adjustments, where the manager refines the budget distribution among the stations in each step, the protection budget vector converges to an optimal allocation. At the end of the game, the final values for each station's protection budget index c_j and the probability of a successful attack r_j are determined. The final expected increase in travel time due to the destruction of Metro stations, under the optimal partial protection strategy, is calculated using Eq. 18:

$$\widehat{ET} = \; r_j . ET_\mathrm{j} \tag{18}$$

which will be the same for all Metro stations

3.2.4. Scenario 4: Partial protection with intelligent operator

In this scenario, the quad-level problem is structured as two non-cooperative, zero-sum games: one between the system manager and the attacker, and the other between the attacker and the operator. Neither the manager nor the attacker can fully predict the other's behavior, and the attacker cannot fully anticipate the operator's responses. Initially, the attacker and the manager engage in a two-player game to determine the probability of a successful attack on each station, based on the distribution of the protection budget. In this game, different levels of protection are defined for each station, and the protection budget is allocated to minimize the likelihood of a successful attack. Then, considering the partial protection strategy selected by the manager, the attacker and operator engage in a two-player game to determine the probability of an attack on each station and the expected maximum damage resulting from this attack. As a result, the station that causes the most damage to the system, despite the operator’s coping strategy, becomes the attacker’s final target. The operator calculates the increase in travel time on the public transit network and the minimum increase in travel time after the destruction of Metro station j, implementing the optimal strategy for that station by solving the OP problem using Eqs. 3 and 4.

At the start of the game between the attacker and the operator, for each defense strategy ii, the attacker sets the probability of attacking all Metro stations equally to $q_j^1 = 1/m$. In each phase of this game, considering the manager's defense strategy ii, the operator first estimates the expected increase in network travel time resulting from an attack on each station without implementing any coping strategy, $\widehat{\widehat{ET}}_j^{ii}$, using Eq. 19:

$$\widehat{\widehat{ET}}_j^{ii} = r_j^{ii} . q_j^{ii} . \overline{ET}_j \tag{19}$$

where q_j^{ii} is the probability of the attacker targeting station j and r_j^{ii} is the probability of the attacker succeeding if station j is attacked. Then, the attacker, considering that the operator will employ the best coping strategy for the most critical station, estimates the expected increase in network travel time due to the destruction of this critical station, while considering the operator's optimal coping strategy, $\widehat{ET}_j^{ii}$, using Eq. 20:

$$\widehat{ET}_j^{ii} = r_j^{ii} . q_j^{ii} . ET_j \tag{20}$$

At the end of each phase of the game between the attacker and the operator, the attacker compares the values of $\widehat{ET}_j^{ii}$ for the critical station with $\widehat{\widehat{ET}}_j^{ii}$ for the other stations. Based on this comparison, the attacker selects the station with the highest priority for the next attack and updates the probabilities of attacking each Metro station using Eq. 21:

$$q_j^{ii} = \frac{t}{t+1} \times q_j^{ii} + \frac{1}{t+1} \times \tilde{q}_j^{ii} \tag{21}$$

where $\tilde{q}_j^{ii}$ is an auxiliary variable that is set to one for the station with the highest priority for the attacker and zero for the other stations during each phase of the game. At the end of the game, the final probabilities of attacking the stations are determined.

At the start of the game between the system manager and the attacker, similar to Scenario 3, the available budget is evenly distributed among all Metro stations. As a result, in the first iteration of the game, the protection budget index for all Metro stations is $c_j^1 = \frac{m_i}{m}$. The attacker then uses Eq. 12 to calculate the probability of a successful attack on each station in the first iteration (r_j^1) and proceeds to engage with the operator.

In each phase of the game between the manager and the attacker, the attacker identifies the most critical station for the attack by considering the final attack probabilities and the probability of success in attacking at each station in that phase. The expected increase in travel time for the public transit network, in the event of an attack on the critical station, is estimated using Eq. 22:

$$\widehat{ET}^{ii} = \max_j\left\{\widehat{ET}_j^{ii}\right\} = \max_j\left\{r_j^{ii}.\,q_j^{ii}.\,ET_j\right\} \tag{22}$$

After identifying the critical station at the end of each phase of the game between the manager and the attacker, the manager updates the protection budget indices for the stations using Eq. 15. If necessary, the manager further adjusts the budget index vector using Eqs. 16 and 17. As previously mentioned, $\tilde{c}_j^{ii}$ in Eq. 15 is an auxiliary variable set to one for the critical station and zero for the other stations. If the protection budget index for any station exceeds one, the budget index vector is recalculated using Eqs. 16 and 17.

As the game between the manager and the attacker progresses, each phase is repeated with the updated protection budget index vector, and the game between the attacker and the operator is played again. Ultimately, at the end of the game, the final values for each station's protection budget indexc_j, the probability of a successful attack r_j, and the probability of attacking each station q_j are determined. The expected increase in travel time, considering the optimal coping strategy, is then calculated using Eq. 23:

$$\widehat{ET} = \sum_j r_j.\,q_j.\,ET_{\mathrm{j}} \tag{23}$$

4. Case study

4.1. Scope of study

In this article, the public transit network of Shiraz city is used as a case study. Shiraz, the capital of Fars province, is located in southern Iran. According to the latest census conducted in

2021, the city has a population of approximately 1,565,572, making it the fifth most populous city in Iran. Shiraz's public transit system consists of 63 bus lines and one Metro line. This Metro line, spanning 24.5 kilometers, includes 22 stations and serves around 3.7 million passengers annually throughout the city. Figure 3 illustrates the Shiraz rail transport network, highlighting the line and station locations.

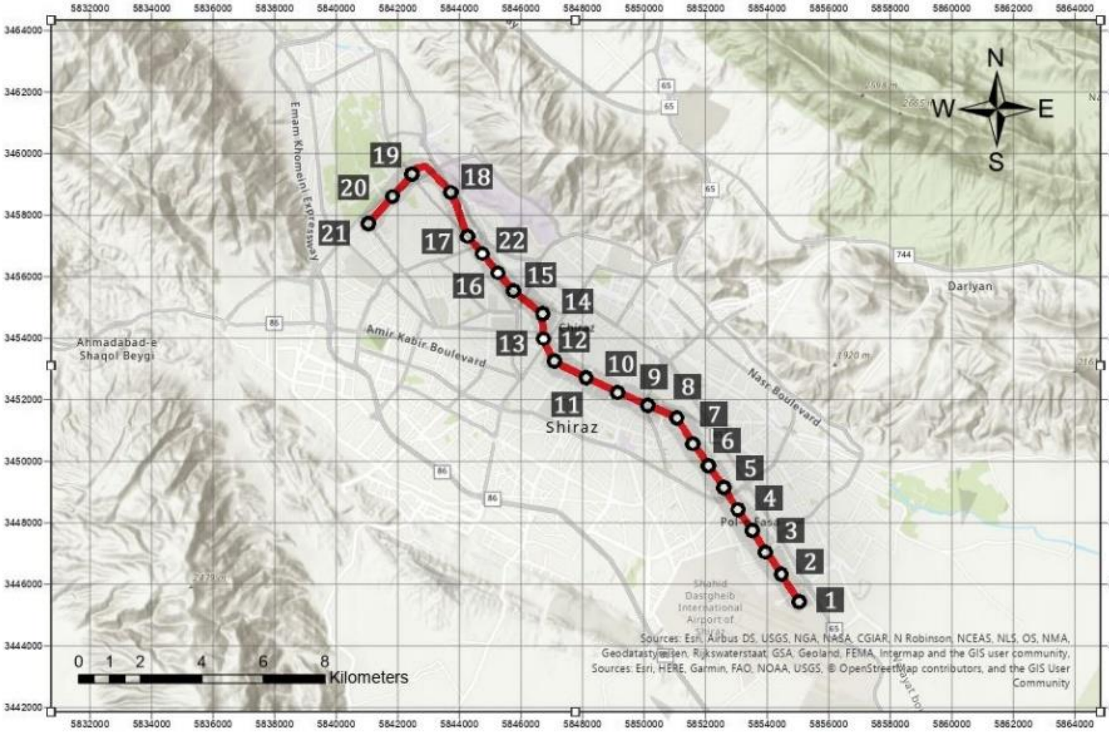
N
S
W
E
Emam Khomeini Expressway
Amir Kabir Boulevard
Nasr Boulevard
Shiraz
Ahmadabad-e Shaqol Beygi
Darlyan
Shahid Dastgheib International Airport of Shiraz
0 1 2 4 6 8
Kilometers
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
Sources: Esri, Airbus DS, USGS, NGA, NASA, CGIAR, N Robinson, NCEAS, NLS, OS, NMA, Geodatastyrelsen, Rijkswaterstaat, GSA, Geoland, FEMA, Intermap and the GIS user community,
Sources: Esri, HERE, Garmin, FAO, NOAA, USGS, © OpenStreetMap contributors, and the GIS User Community

Figure 3. Shiraz Metro line

4.2. Principal assumptions

Any of the 22 Shiraz Metro stations could be the target of a terrorist attack. As noted in Section 3.1, the system manager has a restricted budget for station security, which can be allocated across Metro stations in various ways. In the event of a terrorist assault on any of these stations, the operator will employ a variety of strategies to serve the remaining passengers while mitigating the effects of the attack. The additional assumptions for solving the problem are as follows:

1. The protection cost for all Metro stations is assumed to be identical.
2. The system manager has sufficient budget to fully protect four stations. This budget can be allocated to four stations in the full protection approach or distributed among all stations in the partial protection approach. Instead of using the actual protection budget assigned to each station, the protection budget index of that station is used to solve the problem. The

protection budget index is defined as the ratio of the budget allocated to a station to the full protection budget of that station.

3. The relationship between the protection budget index and the probability of an attacker's success in targeting a station is assumed as Eq. 12.
4. The bus fleet is assumed to be fixed. In other words, in case of an attack on a Metro station, the operator's coping strategies for modifying the bus network are limited to the following:
   - Relocating the fleet between bus lines by adjusting their frequencies.
   - Connecting the disrupted station to the bus network or linking it to t adjacent Metro stations with a bus bridge, followed by adjusting bus lines frequencies.
   - Deviating existing bus lines from their main routes to cover the disrupted station and readjusting the frequencies of bus lines.

According to the structure of the public transit network in Shiraz city, the strategies outlined in Table 2 are considered the operator's coping strategies. Notably, in strategy (i), the operator does not alter the bus network structure, such as by deviating existing routes or creating new ones. Instead, the operator reallocates the fleet among existing bus lines to improve the public transit network’s performance after an attack.

Table 2
Operator strategies to cope with the attack in Shiraz Metro stations

Disrupted Metro station	Operator’s coping strategies			
	(i) Moving the fleet between lines	(ii) Connecting to the existing bus lines or connecting to other Metro stations		(iii) Deviating the routes of existing bus lines
		Bus lines connected to disrupted station	Metro stations connected disrupted station	Bus lines deviated towards the disrupted station
1	No change	35-48-71-32	2	35-48-71-32
2	No change	28-71-32-35	1-3	28-71-32-35
3	No change	48-71-32-35	2-4	48-71-32-35
4	No change	48-71-20-35-27	3-5	48-71-20-35-27
5	No change	32-20-35-48-27	4-6	32-20-35-48-27
6	No change	48-20-35-27	5-7	48-20-35-27
7	No change	27-20-51-58-7	6-8	27-20-51-58-7
8	No change	27-7-51-58-71	7-9	27-7-51-58-71
9	No change	2-73	8-10	2-73
10	No change	2-7-51-58-71-35	9-11	2-7-51-58-71-35
11	No change	2-16-21-51-18-71	10-12	2-16-21-51-18-71
12	No change	2-73-9	11-13	2-73-9
13	No change	73-5-21-18-9	12-14	73-5-21-18-9
14	No change	73-5-21-18-10	13-15	73-5-21-18-10

15	No change	21-18-9	14-16	21-18-9
16	No change	54-9-22	15-22	54-9-22
22	No change	54-22	16-17	54-22
17	No change	54	18-22	54
18	No change	60-50-37-22	17-19	60-50-37-22
19	No change	22	18-20	22
20	No change	54-50-37	19-21	54-50-37
21	No change	38	20	38

4.3. Results

The operator's OP problem was implemented in C++ to efficiently handle the complexity of bus network adjustments. Meanwhile, the attacker's problem (Eq. 5) and the system manager's problem (Eq. 6), along with the detailed execution of the game dynamics between the three players, were coded in MATLAB. The algorithms developed for solving the optimal defense model, particularly tailored to each defensive scenario discussed in Section 3, are thoroughly detailed in Appendix 2. These algorithms offer a step-by-step approach for addressing the unique challenges posed by Metro station attacks, providing a robust framework for implementing the defense strategies outlined in this study.

4.3.1. Scenario 1: Full protection - Non-intelligent operator

In this scenario, assuming the budget to fully protect four Metro stations is in position, the system manager will have $\binom{22}{4} = 7315$ defense strategies. In each defense strategy, there are 18 unprotected Metro stations, and the attacker will choose one of them to attack. As a result, there were $7315 \times 18 = 131670$ defense-attack situations in this scenario. To deal with each of the 18 possible attacking plans, the operator has a number of available strategies (according to Table 2).

The results of the analysis of scenario 1 in the Shiraz network show that the optimal strategy of the system manager is to protect stations number 4, 5, 15 and 17. As a result of applying this strategy, the attacker chooses to attack Metro station number 19 as the best attack strategy. The operator also minimizes the effects of this attack by creating a bus connection between this station and bus line number 22. The final results are shown in Table 3.

The analysis of Scenario 1 for the Shiraz network reveals that the optimal strategy for the system manager is to protect stations 4, 5, 15, and 17. With this strategy in place, the attacker is most likely to target Metro station 19 as the optimal attack strategy. The operator minimizes the effects of this attack by creating a bus connection between this station and bus line 22. The final results are shown in Table 3.

Table 3
Analysis results of scenario 1 for Shiraz public transit network

Optimal strategies of players	Network travel time before the attack (hours)	Network travel time after attack (hours)	Increase in network travel time after attack (hours)	Percentage increase in network travel time after attack
Protection set: 4-5-15-17 Target station: 19 Coping strategy: Connecting Metro station 19 to bus line 22	42142.148	Regardless of the manager's protection strategy and the operator's coping strategy		
		43742.344	1600.196	3.8
		Considering the manager's protection strategy and the operator's optimal coping strategy		
		42308.358	166.210	0.4

4.3.2. Scenario 2: Full protection - Intelligent operator

In this scenario, assuming that the budget for the full protection of four Metro stations is available, the system manager has $\binom{22}{4} = 7315$ defense strategies. The key difference between this scenario and Scenario 1 is the intelligence of the operator over the attacker, leading to a two-player game between the operator and the attacker to determine the optimal attack strategy and the operator's optimal coping strategy.

The analysis of Scenario 2 for the Shiraz network shows that the optimal strategy for the system manager is to protect stations 4, 8, 10, and 11. In this scenario, station 2 has the highest probability of being targeted. In the event of an attack on this station, the operator minimizes the impact of the disruption by creating a bus connection line between this station and bus line 28. The final results are presented in Table 4. As can be seen, if the operator acts intelligently in response to the attacker, the manager's defense strategy (protection set) and the attacker's attack strategy change significantly, leading to a reduction in the impact of disruptions caused by terrorist attacks on Metro stations.

Table 4
Analysis results of scenario 2 for Shiraz public transit network

Optimal strategies of players	Network travel time before the attack (hours)	Network travel time after attack (hours)	Increase in network travel time after attack (hour)	Percentage increase in network travel time after attack
Protection set: 4-8-10-11 Target station: 2 Coping strategy: Connecting Metro station 2 to bus line 28	42142.148	Regardless of the manager's protection strategy and the operator's coping strategy		
		43742.344	1600.196	3.8
		Considering the manager's protection strategy and the operator's optimal coping strategy		
		42254.936	112.788	0.3

4.3.3. Scenario 3: partial protection – non-intelligent operator

In this scenario, a budget equivalent to the cost of fully protecting four Metro stations is available, but the operator aims to optimally distribute this budget among the Metro stations to minimize the effects of station disruption while reducing the likelihood of an attacker successfully targeting the stations.

The analysis of Scenario 3 for the Shiraz network provides the final value of the protection budget index for different Metro stations, as shown in Table 5. The protection budget index refers to the specific proportion of the total available protection budget allocated to each station. This is expressed as a fraction of the full protection budget required for one station, with values ranging from 0 (no protection) to 1 (full protection). The highest protection budget indices are assigned to stations 15 and 17, with 0.4262 and 0.4245 units of budget index, respectively, while the lowest protection budget indices are allocated to stations 3 and 11, with 0.0001 units of budget index (almost zero).

Table 6 shows the final probability of the attacker succeeding in attacking the Metro stations, based on the protection budget index of each station. The application of this scenario results in the effect of disruption across all stations being equal in terms of increasing network travel time. In the event of an attack on any station, 44,521 hours will be added to the total network travel time. Table 7 presents the final results of this scenario. As observed, distributing the protection budget among all Metro stations reduces the overall impact of disruptions caused by terrorist attacks on the Metro stations.

Table 5
Protection budget index for Shiraz Metro Stations in scenario 3

Metro Station	1	2	3	4	5	6	7	8	9	10	11
Protection budget index	0.0383	0.1926	0.0001	0.3635	0.3364	0.034	0.0803	0.2432	0.2605	0.321	0.0001
Metro Station	12	13	14	15	16	17	18	19	20	21	22
Protection budget index	0.2297	0.005	0.2364	0.4262	0.2216	0.4245	0.1556	0.3179	0.3043	0.0556	0.042

Table 6
Attack success probability for Shiraz Metro stations in scenario 3

Metro station	1	2	3	4	5	6	7	8	9	10	11
Successful attack probability	0.7258	0.4099	0.9894	0.2287	0.2518	0.7414	0.6074	0.3463	0.3268	0.7484	0.9894
Metro station	12	13	14	15	16	17	18	19	20	21	22
Successful attack probability	0.3623	0.9001	0.3542	0.181	0.3722	0.1822	0.4643	0.2687	0.2816	0.6711	0.7131

Table 7
Analysis results of scenario 3 for Shiraz public transit network

<table>
<tr><th>Optimal strategies of players</th><th>Network travel time before the attack (hours)</th><th>Network travel time after attack (hours)</th><th>Increase in network travel time after attack (hour)</th><th>Percentage increase in network travel time after attack</th></tr>
<tr><td rowspan="4">The distribution of the protection budget index among the stations is according to Table 5.
All stations are equally likely to be attacked.</td><td rowspan="4">42142.148</td><td colspan="3">Regardless of the manager's protection strategy and the operator's coping strategy</td></tr>
<tr><td>43742.344</td><td>1600.196</td><td>3.8</td></tr>
<tr><td colspan="3">Considering the manager's protection strategy and the operator's optimal coping strategy</td></tr>
<tr><td>42186.669</td><td>44.521</td><td>0.1</td></tr>
</table>

4.3.4. Scenario 4: partial protection – intelligent operator

In this scenario, similar to Scenario 3, a budget equivalent to the full protection budget of four Metro stations is available. However, the system manager aims to distribute this budget among the Metro stations in a manner that minimizes the impact of attacks and disruptions.

The analysis of Scenario 4 for the Shiraz network provides the final protection budget index values for different Metro stations, as shown in Table 8. The highest protection budgets are allocated to stations 4 and 10, with 0.3885 and 0.3415 units of budget index, respectively, while the lowest protection budgets are assigned to stations 3, 6, 21, and 22, each with 0.1019 units of budget index. Compared to Scenario 3, the distribution of protection budgets in Scenario 4 is less dispersed. Table 9 presents the probability of the attacker succeeding in attacking the metro stations, based on the protection budget index of each station.

As a result of applying this scenario, the disruption effect on network travel time is equalized across all stations. In the event of an attack on any station, 36.126 hours will be added to the total network travel time. The final results of this scenario are displayed in Table 10. As observed, when the protection budget is distributed among all Metro stations and the operator acts intelligently, the impact of disruptions caused by terrorist attacks on Metro stations can be significantly reduced.

Figure 4 and Table 11 illustrate the impact of disruptions at each station within the Shiraz city transport network on the total travel time for public transit users, as well as the effectiveness of the operator's optimal coping strategy in mitigating the disruption effects of an attack on the Metro stations.

Table 8
Protection budget index for Shiraz Metro Stations in scenario 4

Metro Station	1	2	3	4	5	6	7	8	9	10	11
Protection budget index	0.1293	0.2775	0.1019	0.3885	0.1443	0.1019	0.1068	0.2216	0.1233	0.3415	0.229
Metro Station	12	13	14	15	16	17	18	19	20	21	22
Protection budget index	0.1575	0.1644	0.295	0.1124	0.2195	0.1648	0.1234	0.2078	0.1857	0.1019	0.1019

Table 9
Attack success probability for Shiraz Metro stations in scenario 4

Metro station	1	2	3	4	5	6	7	8	9	10	11
Successful attack probability	0.5081	0.3085	0.5602	0.2087	0.4825	0.5602	0.5503	0.3722	0.5189	0.2473	0.3631
Metro station	12	13	14	15	16	17	18	19	20	21	22
Successful attack probability	0.4612	0.4507	0.2907	0.5394	0.3748	0.4499	0.5187	0.3896	0.4195	0.5602	0.5602

Table 10
Analysis results of scenario 4 for Shiraz public transit network

Optimal strategies of players	Network travel time before the attack (hours)	Network travel time after attack (hours)	Increase in network travel time after attack (hour)	Percentage increase in network travel time after attack
The distribution of the protection budget index among the stations is according to Table 5. All stations are equally likely to be attacked.	42142.148	Regardless of the manager's protection strategy and the operator's coping strategy		
		43742.344	1600.196	3.8
		Considering the manager's protection strategy and the operator's optimal coping strategy		
		42178.274	36.126	0.1

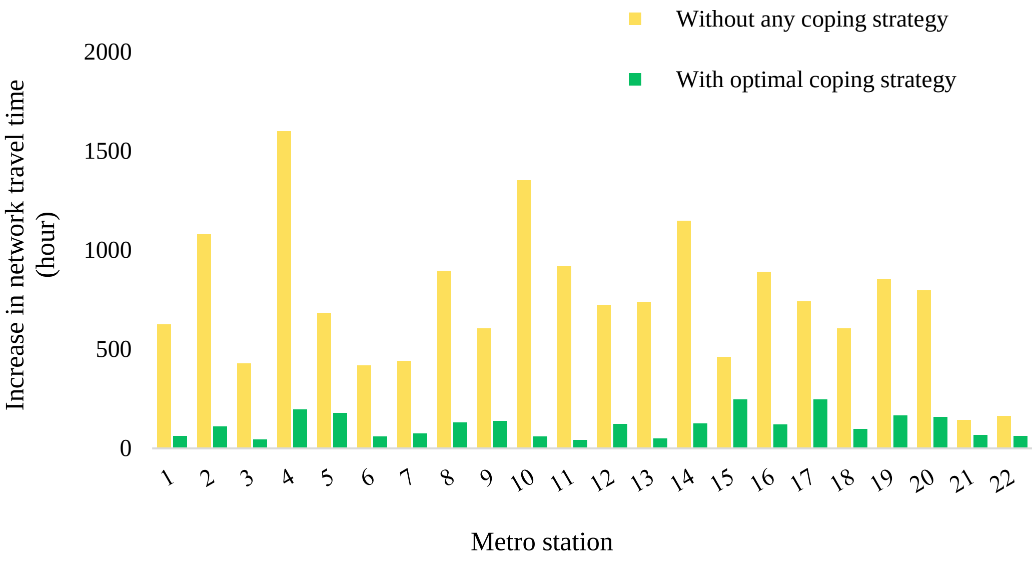

Figure 4. Impact of Metro station disruptions on total travel time of Shiraz transit network with and without the operator's optimal coping strategy

Table 11

Impact of Metro station disruptions on the total travel time of the Shiraz transit network

Metro station	Total travel time without any coping strategy (hours)	Total travel time with optimal coping strategy(hours)	Percentage reduction in network travel time (%)
1	624.844	61.556	90.1
2	1080.000	109.112	89.9
3	427.148	44.276	89.6
4	1600.196	195.442	87.8
5	682.406	177.394	74.0
6	417.656	60.270	85.6
7	439.884	73.620	83.3
8	894.758	129.030	85.6
9	605.492	136.882	77.4
10	1353.610	59.756	95.6
11	919.056	42.204	95.4
12	722.884	123.254	82.9
13	739.392	49.368	93.3
14	1148.234	126.246	89.0
15	460.992	246.804	46.5
16	890.422	120.174	86.5
17	741.978	245.514	66.9
18	605.610	96.314	84.1
19	855.680	166.210	80.6
20	796.320	158.890	80.0
21	141.766	66.636	53.0
22	162.148	62.748	61.3

Finally, Figure 5 illustrates the percentage increase in travel time for Shiraz's public transportation network following a terrorist attack on Metro stations across the four scenarios. The results demonstrate that the operator’s intelligence in anticipating the attacker’s actions significantly reduces the impact of disruptions. This is evident from the lower increase in network travel time in scenario 2 compared to scenario 1, and in scenario 4 compared to scenario 3. Moreover, distributing the protection budget across all stations (partial protection) rather than concentrating it on a few stations further mitigates the impact of attacks, as seen in scenario 3 versus scenario 1, and in scenario 4 versus scenario 2. The percentage effect of the manager's protection strategies and the operator's coping strategies on improving network travel time after a terrorist attack is summarized in Table 12. The findings highlight the advantages of an intelligent operator and an optimally distributed protection budget.

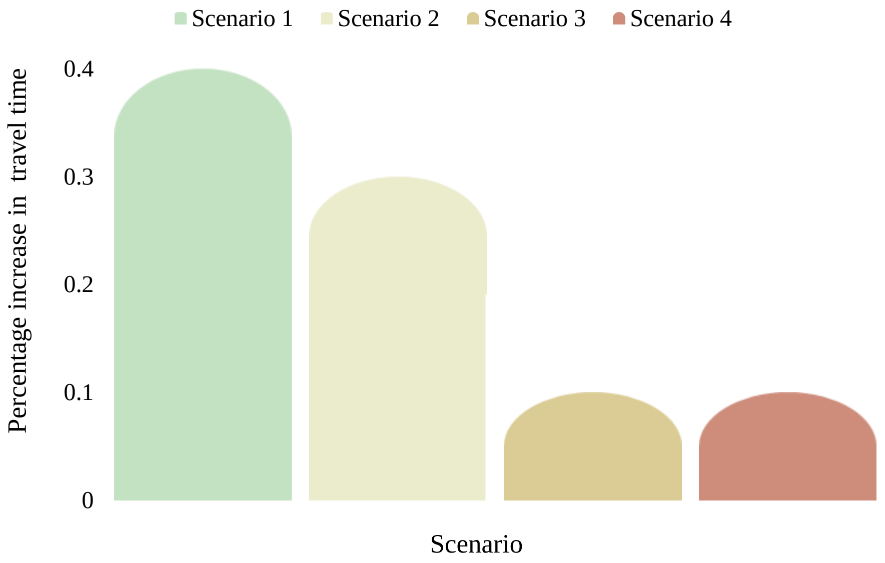

Figure 5. Percentage increase in travel time for Shiraz public transit network due to a terrorist attack on Metro stations in different scenarios

Table 12
Effect of manager’s protection and operator’s response on reducing travel time increase after a Metro station attack in Shiraz

Scenario number	Increase in network travel time without manager's protection strategy and operator's coping strategy (hours)	Increase in network travel time considering manager's protection strategy and operator's coping strategy (hours)	Percentage reduction in network travel time Increase (%)
1	1600.19	166.21	89.6
2	1600.19	112.79	93.0
3	1600.19	44.52	97.2
4	1600.19	36.13	97.7

5. Conclusion, limitations, and further investigations

This paper presented a defender-attacker-defender optimization model to evaluate defense strategies for protecting urban rail systems against intentional destruction of Metro stations. The model's key innovation lies in considering different intelligence scenarios for the attacker and operator, and in simulating the behavior of public transit system users both during and after an attack. This approach led to a quad-level model, incorporating a two-level interactive game between the operator and public transit users aiming to reduce travel time following an attack.

Four scenarios were defined based on the intelligence levels of the players, each accompanied by a practical algorithm for solving the quad-level model. These algorithms were applied to the public transit network of Shiraz, resulting in the determination of optimal protection levels for Metro stations under different scenarios. The results indicate that focusing solely on the most critical Metro stations and allocating the full protection budget to them does not yield an optimal defense design. Instead, distributing the protection budget among all stations (partial protection) and employing a non-cooperative zero-sum game approach between the system manager and the attacker offer more effective results. Furthermore, an intelligent operator can predict the attacker’s behavior, evaluate counterstrategies, and select optimal responses to minimize disruption.

While this study primarily considers travel time as the key metric, future research could explore additional factors such as service downtime, passenger flow disruption, and system recovery time. Incorporating economic elements, including revenue loss and repair costs, could provide a more comprehensive framework for assessing the impact of intentional disruptions on urban rail systems. Additionally, the model assumes rational and deterministic behavior for attackers, defenders, and passengers, whereas real-world behaviors are often influenced by uncertainties, incomplete information, and psychological factors. Enhancing the model with stochastic elements or behavioral game theory could improve its realism.

Another limitation lies in the static nature of the security allocation strategies explored in this study. Extending the model to include adaptive or dynamic strategies would allow for real-time responses to evolving threats, increasing its robustness. Lastly, generalizing the findings to other metro systems with different network structures and socio-political contexts warrants further investigation. Multi-case studies across various metro systems could enhance the applicability and relevance of the proposed framework. Addressing these limitations will enable future research to build upon this study’s foundation, leading to more effective and resilient strategies for urban rail system protection.

Appendix 1: Mathematical Notations

Symbol	Definition
A	The entire set of public transit network links (including both bus and subway modes)
P	The entire set of public transit network stations (including both bus and subway modes)
N	The entire set of public transit network nodes (including both bus and subway modes)
L	The entire set of bus lines
a	A link's number in the public transit network
n	A node's number in the public transit network
p	A station's number in the public transit network
l	A line's number in the public transit network
j	A metro station's number
x_a	Passenger flow on link a (in vehicles per hour)
t_a	Fixed travel time of link a
w_p	Average waiting time of passengers at transit station p
$t_a(x_a)$	Travel time function of link a
$\tau_a(x_a)$	Penalty function of link a
T_l	Travel time of transit line l
F_l	Frequency of transit line l
N_b	Total number of public transit fleet
$\underline{f}$ & $\overline{f}$	Upper and lower limits for the frequency of all bus lines
A_n^-	The set of outbound links from node n in the public transit network
A_n^+	The set of inbound links to node n in the public transit network
d_n	Travel demand from node p to the destination
BN	A very large number
h_a	A binary parameter for link a; $h_a = BN$ if a is a boarding or alighting link connected to the attacked Metro station, and $h_a = 1$ for other links in the transit network; $h = (h_a)$
h_{aj}	The value of h_a when Metro station j is attacked, $h_j = (h_{aj})$
M	The entire set of all Metro stations
m	The number of Metro stations, $m = \|M\|$
I	The set of all defense strategies of manager (i.e., including all subsets of M)

i A defense strategy's number

M_i The set of Metro stations protected by system manager at defense strategy i (i.e., the subset of M corresponding with defense i)

m_i The number of Metro stations protected by system manager in defense strategy i, $m_i = |M_i|$ (equivalent to the total units of budget index in strategy i),

K_j The set of operator's coping strategies to deal with the attack on Metro station j

k_j The number of operator's coping strategy to deal with the attack on Metro station j, $k_j = |K_j|$

k A coping strategy's number

L_k The entire set of bus lines in coping strategy k

P_k The entire set of stations in coping strategy k

ii Repetition counter for the steps in calculating the distribution index of the station protection budget during the manager and attacker game

t Repetition counter for calculating the probability of attacking stations during the attacker and operator game

q_j^i Probability of an attack on Metro station j for defense strategy i

q_j^{ii} Probability of an attack on Metro station j in iteration ii

$\tilde{q}_j^i$ Auxiliary variable for computing q_j^i during the attacker and operator game

$\tilde{q}_j^{ii}$ Auxiliary variable for computing q_j^{ii}during the attacker and operator game

q_j Final probability of an attack on Metro station j

r_j Final probability of the attacker's success in attacking Metro station j

c_j Final Index of protection budget allocated to Metro station j

$\tilde{c}_j$ Auxiliary variable for computing c_j

c_j^{ii} Index of protection budget allocated to Metro station j in iteration ii

$\tilde{c}_j^{ii}$ Auxiliary variable for computing c_j^{ii}

r_j^{ii} Probability of success in attacking Metro station j in iteration ii

c_{max}^{ii} The highest budget index allocated to a Metro station in iteration ii

TC The total travel time of passengers in the public transit network

TC_0 The total travel time of passengers in the public transit network in the absence of an attack

$TC_{j,k}$ The total travel time of passengers in the public transit network when the attacker targets Metro station j and the operator implements coping strategy k

ET The minimum increase in public transit network travel time across all of the manager's protection strategies when the attacker targets the most critical station and the operator implements the best coping strategy.

ET^i The highest increase in the public transit network travel time when the most critical station within protection set M_i is targeted and the operator implements the best coping strategy

ET_j The lowest increase in the public transit network travel time when the attacker targets Metro station j and the operator implements the best coping strategy.

$\overline{ET_j}$ Added travel time in the public transit network when Metro station j is targeted and the operator implements no coping strategy

ET_j^i The lowest increase in public transit network travel time for protection set M_i when Metro station j is targeted and the operator implements the best coping strategy.

$ET_{j,k}$ Added travel time in the public transit network when Metro station j is targeted and the operator implements coping strategy k

$\widehat{ET}$ The minimum expected increase in public transit network travel time among all protection strategies when the most critical station is targeted and the operator implements the best coping strategy

$\widehat{ET}^i$ The highest expected increase in public transit network travel time for protection set M_i when the most critical station is targeted and the operator implements the best coping strategy

$\widehat{ET}^{ii}$ The highest expected increase in public transit network travel time in iteration ii when the most critical station is targeted and the operator implements the best coping strategy

$\widehat{\widehat{ET}}_j^i$ Expected increase in public transit network travel time for protection set M_i when Metro station j is targeted and the operator implements no coping strategy

$\widehat{\widehat{ET}}_j^{ii}$ Expected increase in public transit network travel time in iteration ii when Metro station j is targeted and the operator implements no coping strategy

$\widetilde{ET}_j^i$ Auxiliary value for computing $\widehat{\widehat{ET}}_j^i$

$\widetilde{ET}_j^{ii}$ Auxiliary value for computing $\widehat{\widehat{ET}}_j^{ii}$

Appendix 2: Solution Algorithm for Protection Scenarios 1–4

Step 0: Solve the OP problem for the existing public transport network and obtain the value of $TC0$.

Step 1: For each $j \in \{1, \dots, m\}$, do:

- **Step 1-1**: Set $h_a = BN$ for boarding and alighting links at station m_j and $h_a = 1$ for other links.
- **Step 1-2**: Solve the sub-problem (1) of the OP problem and obtain TC_j and $\overline{ET_j} = TC_j - TC_0$.
- **Step 1-3**: For each $k \in K_j$, Modify the disrupted network structure based on the coping strategy k, solve the OP problem to obtain $TC_{j,k}$, and compute $ET_{j,k} = TC_{j,k} - TC_0$.
- **Step 1-4**: Compute $ET_{\mathrm{j}} = \min_k \{ET_{\mathrm{j},k}\}$.

Step 2: Determine m_i based on the protection budget. Set $i = 1$ and $ii = 1$.

Step 3: (For Scenarios 1 and 2) Identify the i-th set of protected Metro stations M_i.

Step 4: (For Scenarios 3 and 4) For each $j \in \{1, \dots, m\}$, set $c_j^{ii} = \frac{m_i}{m}$.

Step 5: For each $j \in \{1, \dots, m\}$:

- (For Scenario 2) If $j \in M_i$, set $q_j^i = 0$, otherwise set $q_j^i = 1/(m - m_i)$. Set $t = 1$.
- (For Scenario 4) Set $q_j^{ii} = 1/m$.

Step 6: (For Scenarios 3 and 4) For each $j \in \{1, \dots, m\}$, compute $r_j^{ii} = 1 - \sqrt{1 - \left(c_j^{ii} - 1\right)^2}$.

Step 7: For each $j \in \{1, \dots, m\}$:

- (For Scenario 1) If $j \in M_i$, set $ET_j^i = 0$, otherwise set $ET_j^i = ET_j$.
- (For Scenario 2) Compute $\widehat{ET}_j^i = q_j^i . ET_j$.
- (For Scenario 3) Compute $\widehat{ET}_j^{ii} = r_j^{ii} . ET_j$.
- (For Scenario 4) Compute $\widehat{ET}_j^{ii} = r_j^{ii} . q_j^{ii} . ET_j$.

Step 8: For each $j \in \{1, \dots, m\}$:

- (For Scenario 2) Compute $\widehat{\widehat{ET}}_j^i = q_j^i . \overline{ET}_j$.
- (For Scenario 4) Compute $\widehat{\widehat{ET}}_j^{ii} = r_j^{ii} . q_j^i . \overline{ET}_j$.

Step 9:

- (For Scenario 2)
  - **Step 9-1**: For station j with the highest $\widehat{\widehat{ET}}_j^i$, set $\widetilde{ET}_j^i = \widehat{ET}_j^i$, and for other stations set $\widetilde{ET}_j^i = \widehat{\widehat{ET}}_j^i$.
  - **Step 9-2**: For station j with the highest $\widetilde{ET}_j^i$, set $\tilde{q}_j^i = 1$, and for other stations set $\widetilde{q}_j^i = 0$.
  - **Step 9-3**: For each $j \in \{1, \dots, m\}$: If $j \in M_i$, set $q_j^i = 0$, otherwise set $q_j^i = \frac{t}{t+1} q_j^i + \frac{1}{t+1} \tilde{q}_j^i$.
- (For Scenario 4)
  - **Step 9-1**: For station j with the highest $\widehat{\widehat{ET}}_j^{ii}$, set $\widetilde{ET}_j^{ii} = \widehat{ET}_j^{ii}$, and for other stations set $\widetilde{ET}_j^{ii} = \widehat{\widehat{ET}}_j^{ii}$.
  - **Step 9-2**: For station j with the highest $\widetilde{ET}_j^{ii}$, set $\widetilde{q}_j^{ii} = 1$, and for other stations set $\widetilde{q}_j^{ii} = 0$.
  - **Step 9-3**: For each $j \in \{1, \dots, m\}$, set $q_j^{ii} = \frac{t}{t+1} q_j^{ii} + \frac{1}{t+1} \tilde{q}_j^{ii}$.

Step 10: (For Scenarios 2 and 4) If convergence conditions met, go to Step 11, otherwise set $t = t + 1$ and go to Step 7.

Step 11:

- (For Scenario 1) Set $ET^i = \max_j \left\{ET_j^i\right\}$.
- (For Scenario 2) Set $\widehat{ET}^i = \sum_j \widehat{ET}_j^i$.
- (For Scenarios 3 and 4) Set $\widehat{ET}^{ii} = \max_j \left\{\widehat{ET}_j^{ii}\right\}$.

Step 12: (For Scenarios 1 and 2) If all possible protection sets have been reviewed, go to Step 15 for Scenario 1 and Step 14 for Scenario 2. Otherwise, go to Step 13.

Step 13: (For Scenarios 1 and 2) Set $t = t + 1$.

- (For Scenario 1) Go to Step 7.
- (For Scenario 2) Go to Step 5.

Step 14: (For Scenario 2) For each $j \in \{1, \dots, m\}$, set $q_j = q_j^i$ and obtain the final attack probability vector (q_j).

Step 15:

- (For Scenario 1) Set $ET = \min_i \{ET^i\}$.
- (For Scenario 2) Set $\widehat{ET} = \min_i \{\widehat{ET}^i\}$.

Step 16:

- (For Scenario 1) Identify the set *i* with the minimum ET^i as the optimal set of stations to be protected by the system manager.
- (For Scenario 2) Identify the set *i* with the minimum $\widehat{ET}^i$ as the optimal set of stations to be protected by the system manager.

Step 17: (For Scenarios 3 and 4)

- **Step 17-1**: For station j with the highest $\widehat{ET}_j^{ii}$, set $\tilde{c}_j^{ii}$, and for other stations set $\tilde{c}_j^{ii} = 0$.
- **Step 17-2**: For each $j \in \{1, \dots, m\}$, set $c_j^{ii} = \frac{ii}{ii+1} c_j^{ii} + \frac{1}{ii+1} \tilde{c}_j^{ii}$.
- **Step 17-3**: Set $c_{max}^{ii} = \max_j \{c_j^{ii}\}$.
- **Step 17-4**: If $c_{max}^{ii} > 1$, then for each $j \in \{1, \dots, m\}$:
  - If $c_j^{ii} = c_{max}^{ii}$, set $c_j^{ii} = 1$.
  - Otherwise, set $c_j^{ii} = c_j^{ii} + \frac{c_{max}^{ii} - 1}{\mathrm{j}-1}$.

Step 18: (For Scenarios 3 and 4) If the convergence condition is met, go to Step 19. Otherwise, set $ii = ii + 1$ and go to Step 6.

Step 19: (For Scenarios 3 and 4) For each $j \in \{1, \dots, m\}$, set $c_j = c_j^{ii}$ and $r_j = r_j^{ii}$. Obtain the final budget allocation vector (c_j) and the final success probability vector (r_j).

Step 20: (For Scenario 4) For each $j \in \{1, \dots, m\}$, set $q_j = q_j^{ii}$ and obtain the final attack probability vector(q_j).

Step 21:

- (For Scenario 3) $\widehat{ET} = r_j . ET_{\mathrm{j}}$.
- (For Scenario 4) Set $\widehat{ET} = \sum_j r_j . q_j . ET_{\mathrm{j}}$.

References

Aboudina, A., Itani, A., Diab, E., Srikukenthiran, S., & Shalaby, A. (2021). "Evaluation of bus bridging scenarios for railway service disruption management: A users' delay modelling tool". *Public Transport*, *13*(3), 457-481. https://doi.org/10.1007/s12469-020-00238-w

Afandizadeh, S., Amoei Khorshidi, N., Mirzahossein, H., & Shakoori, S. (2024). Predicting the Fluctuation of Travel Time Reliability as a Result of Congestion Variations by Bagging-Based Regressors. *Civil Engineering Infrastructures Journal ,57(1)* ,85-101 . https://doi.org/10.22059/ceij.2023.349853.1878

Akinrolabu, O., Nurse, J. R. C., Martin, A., & New, S. (2019). "Cyber risk assessment in cloud provider environments: Current models and future needs". *Computers & Security*, *87*, 101600. https//:doi.org/10.1016/j.cose.2019.101600

Alderson, D., Brown, G., Carlyle, M., & Wood, R. (2011). *"Solving defender-attacker-defender models for infrastructure defense"*. https://doi.org/10.1287/ics.2011.0047

Bababeik, M., Khademi, N., & Chen, A. (2018). "Increasing the resilience level of a vulnerable rail network: The strategy of location and allocation of emergency relief trains". *Transportation Research Part E: Logistics and Transportation Review*, *119*, 110-128. https://doi.org/10.1016/j.tre.2018.09.009

Bešinović, N. (2020). "Resilience in railway transport systems: A literature review and research agenda". *Transport Reviews*, *40*(4), 457-478. https://doi.org/10.1080/01441647.2020.1728419

Brown, G., Carlyle, M., Salmerón, J., & Wood, R. (2006). "Defending critical infrastructure". *Interfaces*, *36*, 530-544. https://doi.org/10.1287/inte.1060.0252

Brown, G. G., Carlyle, W. M., & Wood, R. K. (2008). *"Appendix E: Optimizing department of homeland security defense investments: Applying defender-attacker (-defender) optimization to terror risk assessment and mitigation."*. Department of homeland security bioterrorism risk assessment: A call for change. https://doi.org/10.17226/12206

Chen, H., Lam, J. S. L., & Liu, N. (2018). "Strategic investment in enhancing port–hinterland container transportation network resilience: A network game theory approach". *Transportation Research Part B: Methodological*, *111*, 83-112. https://doi.org/10.1016/j.trb.2018.03.004

CISA. (2015). *Transportation systems sector-specific plan*) .National Infrastructure Protection Plan and Resources, Issue .

Constantin, I., & Florian, M. (1995). "Optimizing frequencies in a transit network: A nonlinear bi-level programming approach". *International Transactions in Operational Research*, *2*(2), 149-164 . https://doi.org/10.1016/0969-6016(94)00023-M

Currie, G., & Muir, C. (2017). "Understanding passenger perceptions and behaviors during unplanned rail disruptions". *Transportation Research Procedia*, *25*, 4392-4402. https://doi.org/10.1016/j.trpro.2017.05.322

Errico, F., Crainic, T. G., Malucelli, F., & Nonato, M. (2013). "A survey on planning semi-flexible transit systems: Methodological issues and a unifying framework". *Transportation Research Part C: Emerging Technologies*, *36*, 324-338. https://doi.org/10.1016/j.trc.2013.08.010

Jingfeng, Y., Jin, J. G., Wu, J., & Jiang, X. (2017). "Optimizing passenger flow control and bus-bridging service for commuting metro lines". *Computer-Aided Civil and Infrastructure Engineering*, *32*. https://doi.org/10.1111/mice.12265

Khademi, N., Bababeik, M., & Fani, A. (2021). "Sparse rail network robustness analysis: Functional vulnerability levels of accidents resulting from human errors". *Journal of Safety Science and Resilience*, *2*(3), 111-123. https://doi.org/10.1016/j.jnlssr.2021.07.001

Khademi, N., Babaei, M., Schmöcker, J.-D., & Fani, A. (2018). "Analysis of incident costs in a vulnerable sparse rail network – Description and Iran case study". *Research in Transportation Economics*, *70*, 9-27. https://doi.org/10.1016/j.retrec.2018.08.010

Khalid, m. n. a., Al-Kadhimi, A., & Mahinderjit Singh, M. (2023). "Recent developments in game-theory approaches for the detection and defense against advanced persistent threats (APTs): A systematic review". *Mathematics*, *11*, 1353. https://doi.org/10.3390/math11061353

Li, W., Li, Y., Tan, Y., Cao, Y., Chen, C., Cai, Y., Lee, K. Y., & Pecht, M. (2019). "Maximizing Network Resilience against Malicious Attacks". *Scientific Reports*, *9*(1), 2261. https://doi.org/10.1038/s41598-019-38781-7

Liang, J., Wu, J., Qu, Y., Yin, H., Qu, X., & Gao, Z. (2019). "Robust bus bridging service design under rail transit system disruptions". *Transportation Research Part E: Logistics and Transportation Review*, *132*, 97-116. https://doi.org/10.1016/j.tre.2019.10.008

Ma, F., Shi, W., Yuen, K. F., Sun, Q., Xu, X., Wang, Y., & Wang, Z. (2020). "Exploring the robustness of public transportation for sustainable cities: A double-layered network perspective". *Journal of Cleaner Production*, *265*, 121747. https://doi.org/10.1016/j.jclepro.2020.121747

Mehran, B., Yang, Y., & Mishra, S. (2020). Analytical models for comparing operational costs of regular bus and semi-flexible transit services. *Public Transport*, *12*(1), 147-169. https://doi.org/10.1007/s12469-019-00222-z

Mishra, S., & Mehran, B. (2023). "Optimal design of integrated semi-flexible transit services in low-demand conditions". *IEEE Access*, *11*, 30591-30608. https://doi.org/10.1109/ACCESS.2023.3260727

Pirbhulal, S., Gkioulos, V., & Katsikas, S. (2021). "Towards integration of security and safety measures for critical infrastructures based on bayesian networks and graph theory: A systematic literature review". *Signals*, *2*, 771-802. https://doi.org/10.3390/signals2040045

Pursiainen, C., & Kytömaa, E .(2023). " From European critical infrastructure protection to the resilience of European critical entities: What does it mean?". *Sustainable and Resilient Infrastructure*, *8*(sup1), 85-101. https://doi.org/10.1080/23789689.2022.2128562

Sarhadi, H., Tulett, D., & Verma, M. (2014). "A defender-attacker-defender approach to the optimal fortification of a rail intermodal terminal network". *Journal of Transportation Security*. https://doi.org/10.1007/s12198-014-0152-4

Spiess, H., & Florian, M. (1989). "Optimal strategies :A new assignment model for transit networks". *Transportation Research Part B: Methodological*, *23*(2), 83-102. https://doi.org/10.1016/0191-2615(89)90034-9

Strandh, V. (2017). "Exploring vulnerabilities in preparedness – rail bound traffic and terrorist attacks". *Journal of Transportation Security*, *10*(3), 45-62. https://doi.org/10.1007/s12198-017-0178-5

Talpur, A., & Gurusamy, M. (2022). "Machine learning for security in vehicular networks: A comprehensive survey". *IEEE Communications Surveys & Tutorials*, *24*(1), 346-379. https://doi.org/10.1109/COMST.2021.3129079

Vansteenwegen, P., Melis, L., Aktaş, D., Montenegro, B. D. G., Sartori Vieira, F., & Sörensen, K. (2022). "A survey on demand-responsive public bus systems". *Transportation Research Part C: Emerging Technologies*, *137*, 103573. https://doi.org/10.1016/j.trc.2022.103573

Wang, X., Koç, Y., Derrible, S., Ahmad, S. N., Pino, W. J. A., & Kooij, R. E. (2017). "Multi-criteria robustness analysis of metro networks". *Physica A: Statistical Mechanics and its Applications*, *474*, 19-31. https://doi.org/10.1016/j.physa.2017.01.072

Xu, J., Song, S., Zhai, H., Yuan, P., & Chen, M. (2019). "A new analytical framework for network vulnerability on subway system". *Concurrency and Computation: Practice and Experience*, *32*. https://doi.org/10.1002/cpe.5508

Xu, Z., & Chopra, S. S. (2023). "Interconnectedness enhances network resilience of multimodal public transportation systems for Safe-to-Fail urban mobility". *Nature Communications*, *14*(1), 4291. https://doi.org/10.1038/s41467-023-39999-w

Yamany, W., Moustafa, N., & Turnbull, B. (2020). *"A tri-level programming framework for modelling attacks and defences in cyber-physical systems"* AI 2020: Advances in Artificial Intelligence, Cham. https://doi.org/10.1007/978-3-030-64984-5_8

Yang, H., & Liang, Y. (2023). "Examining the Connectivity between Urban Rail Transport and Regular Bus Transport". *Sustainability*, *15*(9). https://doi.org/10.3390/su15097644

Yang, Y., Ding, H.-x., Chen, F., & Yang, H.-m. (2018). "An approach for evaluating connectivity of interrupted rail networks with bus bridging services". *Advances in Mechanical Engineering*, *10*(3), 1687814018766927. https://doi.org/10.1177/1687814018766927

Yoon, G., Chow, J. Y. J., & Rath, S. (2022). "A Simulation sandbox to compare fixed-route, semi-flexible transit, and on-demand microtransit system designs". *KSCE Journal of Civil Engineering*, *26*(7), 3043-3062. https://doi.org/10.1007/s12205-022-0995-3

Zhang, C., Bütepage, J., Kjellström, H., & Mandt, S. (2018). "Advances in variational inference". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *PP*. https://doi.org/10.1109/TPAMI.2018.2889774

Zhang, Z., Li, X., Zhang, J., & Shi, Y. (2024). "Optimizing Bus Bridging Service Considering Passenger Transfer and Reneging Behavior". *Sustainability*, *16*(23). https://doi.org/10.3390/su162310710

Zhu, W., Liu, K., Wang, M., & Yan, X. (2018). "Enhancing robustness of metro networks using strategic defense". *Physica A: Statistical Mechanics and its Applications*, *503* ,1081-1091 . https://doi.org/10.1016/j.physa.2018.08.109