Research Article GU J Sci 36(4): 1601-1623 (2023) DOI: 10.35378/gujs.1103774

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

Providing Homeland Security Strategies Against Interdictions in the City Transportation Network: A case study in Turkey

Ertugrul AYYILDIZ[1, *], Gokhan OZCELIK[1], Cevriye GENCER[2], Emrullah DEMIRCI[2]

[1] *Department of Industrial Engineering, Faculty of Engineering, Karadeniz Technical University, Trabzon, Turkey*
[2] *Department of Industrial Engineering, Faculty of Engineering, Gazi University, Ankara, Turkey*

Highlights

- This paper defines a variation of the shortest path problem (CMSSP).
- The CMSSP is extended within the network interdiction problem framework (CMSSNIP).
- Exact optimization models for the problems are formulated and tested in a case study.

Article Info

Received: 14 Apr 2022
Accepted: 19 Oct 2022

Keywords

Shortest path problem
Network interdiction
Mixed integer programming,
Networks

Abstract

This study defines a capacitated multiple-source multiple-sink shortest path problem and introduces its extension, called the capacitated multiple-source multiple-sink shortest path network interdiction problem (CMSSNIP). CMSSNIP examines the actions of attackers who attempt to maximize the total shortest path of network users trying to reach the crime locations for the aid process after causing an incident in certain regions to provide strategic information for the defense systems of the government. In this context, the exact mathematical model is proposed to ensure useful information about safe routes to network users. In this manner, to the best knowledge of authors, the CMSSNIP consisting of multiple-source nodes and multiple-sink nodes and considering capacity-demand relations between security units and crime locations is studied for the first time. Consequently, a set of scenarios is considered based on the levels of the interdiction budget and the number of crime locations through a real case application to show the applicability of the model. Furthermore, computational experiments are performed to evaluate the performance of the model in networks of different sizes. It is realized that the model provides resilient strategies against interdictions in terms of obtaining the safe shortest paths at the operational level within seconds in the real case applications.

1. INTRODUCTION

In this day and age, we often encounter situations where it is vital to go from one location to another as quickly as possible. This situation is also important in terms of accessibility, time management, cost management sustainability, etc. When determining transportation routes, managers should consider the effects of this decision on environmental, economic, and social sustainability. No obstacles should be ignored to provide a more robust service to these locations that require humanitarian aid. The management of the aid process against terror groups has gained enormous importance for defense systems when considering the increasing number of terror acts in recent years. In particular, conducting aid activities under the destructive and striking effect of terrorist or harmful groups on transportation networks is a vital issue in terms of governments and societies. For situations recorded or known in security intelligence systems, this issue can be handled. For instance, in the eastern part of Turkey, mines and trenches are continually being excavated and placed on the soldiers' paths. These paths are on the shortest paths of the soldiers. With the proposed model, results are produced to support strengthening efforts against possible secretions. As stated in the text, the proposed optimization model considers the assumption that the interdictions are in the shortest route routes of security units. For this purpose, many studies employ different approaches to improve defense systems in the literature [1–5].

*Corresponding author, e-mail: ertugrulayyildiz@ktu.edu.tr

Such a compulsive process involves two opposite sides whose aims are conflicting and corresponds to the network interdiction problem (NIP) in the literature. In the classical NIP, these two sides are called the network user (follower) and attacker (leader). The network user, who wants to benefit from a network, tries to optimize predefined objective functions, such as minimizing the distance traveled along with the network or maximizing the amount of moved material. The attacker attempts to restrict the objective value achieved by the network user by completely incapacitating arcs or nodes, increasing travel times over arcs, or reducing the capacity of arcs or nodes [6]. In shortest path NIP (SPNIP), the network user seeks to transmit flows through the network as efficiently as possible, while the attacker (e.g., smuggler, illegal immigrants, terrorist, enemy) seeks to restrict the reachable objective value of the defender by attacking some links to lower network capacity or increase travel time and cost. In a two-stage game called the SPNIP, the attacker acts first, and the user, who is fully aware of the attacker's actions, acts second. The attacker knows that the user will choose the shortest route between two nodes they are familiar with, so they interdict travel on a subset of arcs by making those arcs more expensive. It is typical to presume that the interdictor has a restricted budget, which limits the amount of potential harm to a network [7, 8].

Many countries are stepping up their efforts to improve national security in an effort to minimize the potential for terrorist threats [1]. This context served as the first presentation and discussion of numerous contemporary homeland security applications, including the network interdiction problem [2]. This study deals with the circumstances in which terrorists try to interdict aid processes to be provided to these locations on a transportation network after taking destructive actions at several locations at the same time to harm the environment or society. Therefore, it is revealed that humanitarian aid activities should be provided from multiple locations to speed up these aid processes under the destructive impact of terrorists. First, we develop an SPINIP optimization model to protect against the loss of a terrorist attack in order to achieve synergy between counterterrorism methods. Furthermore, our approach offers a fresh point of view for decision analysis in counterterrorism. Second, we generate different shortest path problems to enhance bi-level programming model solution techniques. Third, we apply this approach to the Şişli case study in Istanbul and provide the city managers' counterterrorism recommendations. In this regard, the study aims to reveal the likely roads to be interdicted and to determine the safest routes in the presence of the destructive impact of the terrorist trying to interdict them while the aid activities are provided from more than one location. The safest route is the route that provides maximum security against threats. In other words, the paths that are least likely to be attacked and affected by attacks are the safest route. Our objective is to determine this route and make it practical. Of course, here we also consider the constraints here. By doing so, the goal of this study is to provide strategic information for the manager of defense systems of governmental and nongovernmental organizations at the operational level considering the devastating impacts of the terrorist on transportation networks. For this purpose, a capacitated multiple-source multiple-sink shortest path problem (CMSSP), consisting of multiple-source nodes and multiple-sink nodes and considering capacity-demand relations, is presented. In addition, this problem is extended to the capacitated multiple-source multiple-sink shortest path network interdiction problem (CMSSNIP), corresponding to many real-case applications relating to especially terror acts requiring humanitarian aid. In the CMSSNIP, the network user (support teams) wants to minimize the sum of traveled distance between source node(s) and sink node(s) to satisfy the demands, whilst an attacker (a terror group) aims to maximize the total distance of shortest path used by the support teams under a limited interdiction budget. In fact, since the proposed exact optimization model gives the information about the arcs to be interdicted, in this way, the network user can determine the routes to avoid or strengthen clearly. In this way, the network user is now able to develop resilient strategies against attacker. To illustrate the problem, let us consider that the case where we encounter fire at more than one location is caused by terrorist acts. The fire truck(s) will try to reach the corresponding locations in a minimum time by departing from the fire station(s). If we assume that the terror group has an interdiction budget or resource to extend the total minimum time/shortest path used by fire trucks, the problem turns into the CMSSNIP. The proposed mathematical models are tested and explained step by step through an example network to show the applicability. Then, a real case application is conducted in Şişli which is one of the districts with a high crime rate of İstanbul province in Turkey by considering different scenarios. In addition, computational studies are performed to test the model performance in terms of runtime and see the objective function value under varying parameter values regarding the number of source/sink nodes.

The novelties of the study presented are outlined from different perspectives as follows. In terms of research novelty, once the CMSSP is defined, its extension into the NIP framework is investigated for the first time. For the CMSSNIP, the exact mathematical model is presented in general form, considering capacitated multiple-source nodes and multiple-sink nodes that have demands. The main goal of this study is to provide critical information for both governmental organizations and nongovernmental organizations to improve their defense strategies against attacks by obtaining the attacker's interdiction plans through the exact formulation of the attacker proposed in the CMSSNIP. Because the information obtained relates to interdicted arcs, called risky or most vital arcs, on the shortest paths in the transportation network, the authorizes can improve the security of the aid processes at the operational level thanks to this information. Overall, the paper presents the mathematical model that will be able to be used directly in the defense systems by assuming the terrorists aim to interdict arcs located on the shortest paths in the transportation network. From an application area novelty point of view, because this study presents a comprehensive framework that provides resilient security strategies by determining the most important arcs against interdictions in the city transportation network, it has a wide range of implementation areas.

The remaining parts of the study are organized as follows. In Section 2, the academic literature related to the shortest path of NIP is reviewed. In Section 3, the CMSSP is defined, and its exact mathematical formulation is presented. Also, after the CMSSNIP is defined, the problems of the network user and the attacker are formulated, respectively. In Section 4, a real-case application is carried out. In Section 5, a computational study is performed to evaluate the performance of the model in terms of the run time of the different-sized problems that are generated hypothetically. In addition, a sensitivity analysis is performed to reveal the changes in the objective function value based on changes in both source and sink node numbers. This study ends with the conclusions and future suggestions in Section 6.

2. LITERATURE REVIEW

The relevant academic literature is reviewed, and earlier studies are presented in a comparatively way. First studies related to the NIP usually determine the most important components: node(s) and arc(s). Lubore et al. [9] and Wollmer [10] determined the most significant arc(s) on the network. Ball et al. [11], Ratliff et al. [12], Wollmer [13], Jiang and Hu [14], Lin and Chern [15], and Malik et al. [16] aimed to determine the most important arcs on the network again. Most studies before Wood's formulations [17] formulations are case-based and cannot be generalized. Wood developed a 'min-max' formulation to reformulate the maximum flow NIP and reduced it to a one-level integer programming model (IP) [17]. With the study of Wood, the number of NIP studies has increased and NIP becomes a well-studied research topic from many different scopes, such as minimizing the maximum flow or maximizing the shortest path on a given network, national defense [18, 19], humanitarian logistics [20], facility or sensor locations [21, 22], nuclear smuggling interdiction [23, 24].

To demonstrate the position of this issue in the word literature, the "shortest path network interdiction problem" is searched using the "title, abstract, keywords" section in the SCOPUS database. 140 studies are identified when the keywords "shortest path" and "interdiction problem" or "network interdiction problem" are searched in the SCOPUS database. Due to the fact that both searches turned up some of them, they are repeated. Therefore, repeated studies were removed from the list, bringing the total up to 115. The exclusion criteria are established following the SCOPUS search, and papers that are very pertinent to this subject are found. The following is a list of exclusion criteria.

- Unavailability of full texts for studies
- Studies that don't clearly explain their methodology or findings,
- Not using shortest path algorithms in studies
- Non-English studies that were published prior to 2002.
- Studies not written in English,
- Studies published before 2002.

41 studies published in 2002 or later are found to be related to this study after the studies are evaluated using the aforementioned criteria. All studies in English between 2002 and 2021 are selected and shown in Figure 1. This reveals that there are a few studies in the academic literature on SPNIP.

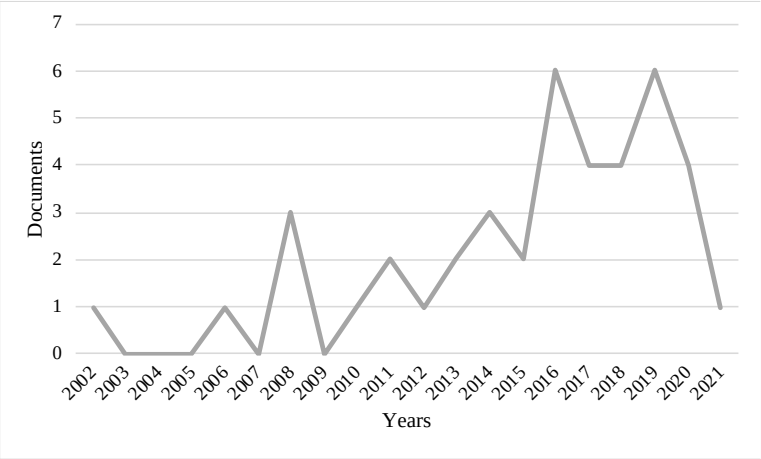


Figure 1. *The number of SPNIP studies by year*

Fulkerson and Harding maximized the shortest path for the traditional network (one node for the source and on the node for the sink) considering the predetermined budget with a linear cost function [25]. Golden developed a new mathematical model, increasing the shortest path of the competitor using the minimum investment cost, based on the study by Fulkerson and Harding [26]. Corley & David reformulated the traditional shortest path problem that includes two sides (an attacker and a system operator) with contradictory objectives [27]. Ball et al. aimed to find the most vital arcs on the traditional shortest path and proved that the problem is NP-hard [11] . Malik et al. also studied on the traditional shortest path and presented a heuristic algorithm to identify the most vital arc that works for nondirectional and positive arcs [16]. Israeli and Wood proposed a new two-level mathematical model for SPNIP and then formulated this model as a single-level mixed-integer programming model to solve the problem in a reasonable time [6]. Khachiyan et al. extended the Dijkstra [28] algorithm to a special version that is usable for SPNIP [29]. Khachiyan et al. studied the SPNIP considering two different types of the interdiction budget and presented an algorithm which can also work with nonnegative arcs [30]. Bayrak and Bailey considered the SPNIP where the sides have different levels of information. They linearized the problem that was formulated as a nonlinear mixed integer program (MIP) and then solved the MIP formulations using the standard branch-and-bound algorithm [31]. Ramirez-Marquez and Rocco formulated the SPNIP for the first time as a two-purpose one considering maximizing the distance of the shortest path and minimizing the interdiction budget. Unlike the traditional shortest path problem [32]. Yates and Sanjeevi studied the problem in which terrorists try to reach from multiple source nodes to the destination in the shortest way. They tried to reduce the effectiveness of terrorists by placing sensors on the pathways [33]. Yates et al. focused on *k*- SPNIP [34]. Yates and Chen introduced an algorithm to determine the location points based on network properties for discrete SPNIP [35]. Song and Shen considered stochastic SPNIP and studied the problem where the attacker wants to minimize the interdiction cost while the network user tries to use the shortest path with uncertain arc lengths between certain two nodes [36]. Casas et al. studied SPNIP for different geographic characteristics [37]. Borndörfer et al. introduced the problem of determining the optimal locations for toll control stations considering parallel secondary paths that drivers can avoid from control stations [38]. Sefair and Smith, Cappenera and Scaparra, Sadeghi et al., Lozano and Smith studied trilevel mathematical models for various SPNIPs [8, 39–41]. Pay et al. studied a stochastic SPNIP where the attacker has ambiguous preferences. They assumed that the attacker acts according to the expected utility theory [42]. Bidgoli and Kheirkah focused on the interdiction of the problem of network for the vehicle routing with asymmetric information [43]. Quadros et al. proposed a linear programming model that can be solved with the branch-and-cut algorithm for fortification of a hub and spoke network [44]. Ayyildiz et al. studied multiple sink SPNIP and proposed a mixed-integer mathematical model [45]. Wei et al. considered a novel stochastic extension of SPNIP with a target threshold and proposed a decomposition algorithm. They studied the algorithm on multiple-sink and multiple-source networks by introducing an artificial source and destination.

By doing so, they converted the networks to single sink and single source networks [46]. Baycik and Sullivan examined a robust SPNIP considering the possibility that the follower might know some information about the placement of the interdictions [47]. Ketkov and Prokopyev studied SPNIP with different levels of information for two sides and presented a heuristic algorithm to solve this problem with respect to some assumptions. As a result, greedy interdiction policies that block *k*-most vital arcs and provided computational complexity of the evader problem [48]. A summary of all reviewed SNIP studies is given in Table 1.

Table 1. *A summary of some notable SPNIP studies*

Reference	The structure of network	The concept of the study	Solution Method	Robust (R) / Stochastic (S) / Deterministic (D)
[25]	single-source, single-sink	maximizing the SP	a mathematical model	D
[26]	single-source, single-sink	maximizing the SP	a mathematical model	D
[27]	single-source, single-sink	finding most vital arc and node	an algorithm	D
[11]	single-source, single-sink	finding most vital arcs	an algorithm	D
[16]	single-source, single-sink, directed	finding most vital arc(s)	a heuristic algorithm	D
[6]	single-source, single-sink, directed	maximizing the SP	a bi-level mathematical model, decomposition algorithms	D
[29]	single-source, single-sink, directed	extending Dijkstra's algorithm for SPNIP	extending Dijkstra's algorithm and breadth-first search	D
[30]	single-source, single-sink	maximizing the SP for the different types of interdiction budgets	modified extending Dijkstra's algorithm and breadth-first search	D
[31]	single-source, single-sink	SPNIP where the sides have different levels of information about the network	a branch and bound algorithm	D
[32]	single-source, single-sink	multi-objective SPNIP	an evolutionary algorithm	D
[39]	single-source, single-sink	multi-level optimization	an implicit enumeration algorithm	D
[49]	single-source, single-sink	maximizing the SP	knapsack approximation	D
[34]	multiple shortest paths for single source-sink	maximizing the multiple SPs	benders decomposition	D
[50]	single-source, single-sink	regret minimization problem with time horizon	three different algorithms	S
[36]	single-source, single-sink	minimizing interdiction cost	a branch-and-cut algorithm and apply lifting techniques to exploit the combinatorial structure	S
[41]	single-source, single-sink	trilevel optimization (fortification-attack-recourse)	a mathematical model+decomposition+algorithm	D
[40]	single-source, single-sink	trilevel optimization (fortification-attack-determine SP)	trilevel to bilevel (duality) + decomposition	D
[45]	single-source, multiple-sink	maximizing the SP	a mathematical model	D
[51]	single-source, single-sink	maximizing the SP	benders decomposition	D
[46]	multiple-source, multiple-sink (converted to single-source, single-sink)	maximizing the SP	decomposition algorithm	S
[47]	single-source, single-sink	maximizing the SP	benders decomposition	R
[42]	single-source, single-sink	maximizing the expected utility	a mathematical model	S
[52]	single-source, single-sink	maximizing the SP	a heuristic algorithm	S
[48]	single-source, single-sink	minimizing cumulative loss	a heuristic algorithm	S
This study	capacitated multiple-source nodes, multiple-sink nodes that have demand	maximizing the total SP	a bi-level mathematical model	D

SP: Shortest Path; SPNIP: Shortest-Path Network Interdiction Problem

Overall, the conducted literature review reveals that the majority of the relevant SPNIP studies are handled in a deterministic environment and there is no study regarding the SPNIP considering capacitated multiple source nodes and multiple sink nodes, that have demands. In this manner, this study intends to fill this gap by presenting an exact mixed-integer mathematical model to solve directly the presented the CMSSNIP.

3. PROBLEM DESCRIPTIONS AND MODEL FORMULATIONS

In this section, after a capacitated multiple-source multiple-sink shortest path problem (CMSSP) is defined, its extension, called the capacitated multiple-source multiple-sink shortest path network interdiction problem (CMSSNIP), is presented. In addition, the exact mathematical models are given separately.

Based on the SPNIP literature review given in the previous section, to propose a deterministic mixed integer programming model to solve CMSSNIP under symmetric information condition, the models are formulated under the following key assumptions:

- Problems are defined in an undirected network. (**CMSSP and CMSSNIP**)
- The total capacity is enough for all demands. (**CMSSP and CMSSNIP**)
- All demands can be satisfied. (**CMSSP and CMSSNIP**)
- Transfers are impossible if there is no connection between nodes. (**CMSSP and CMSSNIP**)
- There is no rule between source-sink node pairs. (**CMSSP and CMSSNIP**)
- The network user and the interdictor have sufficient information about each other, which means that the interdictor's main objective is to try to explicitly maximize the shortest path (achieved by the network user) by interdicting the arc(s) (making the link(s) unusable). **(CMSSNIP)**
- There is a predetermined cost to interdict each arc, and interdiction costs are adjusted in accordance with the number of the required equipment to interdict corresponding arcs. **(CMSSNIP)**
- The interdictor has a predetermined interdiction budget. **(CMSSNIP)**

The sets and indices, parameters, and decision variables regarding the CMSSP and CMSSNIP are given below.

Sets and indices
S: set of source nodes
F: set of sink nodes
D: set of remaining nodes ($D = N \setminus (S \cup F)$)
N: set of all nodes ($N = S \cup F \cup D$) (The cardinality of N is n)
A: set of arcs
i or j: index for any nodes ($i \epsilon N$) and ($j \epsilon N$) (i or $j := 1,2, \dots, n$)
s: index for the source nodes ($s \epsilon S$)
f: index for the sink nodes ($f \epsilon F$)
k: index for the remaining nodes ($k \epsilon D$)

Parameters
d_{ij}: the distance between i^{th} node and j^{th} node
P_s: the capacity of s^{th} node
I_f: the demand of f^{th} node
C: the penalty for interdiction process (a large enough number)
T: the interdiction budget level
b_{ij}: the interdiction cost for arc*(i,j)*

Decision variables
x_{ij}: the number of travels from node i to node j (amount of flow through the arc)
y: the dual variables related to the constraint sets.

w_{ij}: $\begin{cases} \text{if arc}(i,j) \text{ is interdicted, } 1 \\ \text{otherwise, } 0 \end{cases}$.

3.1. The Capacitated Multiple-Source Multiple-Sink Shortest Path Problem (CMSSP)

The CMSSP deals with finding the total length of the shortest path traveled on a network considering the relation between the capacities of multiple-source nodes and the demands of multiple-sink nodes to satisfy all demands.

The exact mathematical model proposed for the CMSSP, is formulated as follows:

$$Z^* = min \sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij} d_{ij} \quad (1)$$

Subject to:

$$\sum_{j=1}^{n} x_{sj} - \sum_{i=1}^{n} x_{is} \leq P_s; \quad \forall s \in S \quad (2)$$

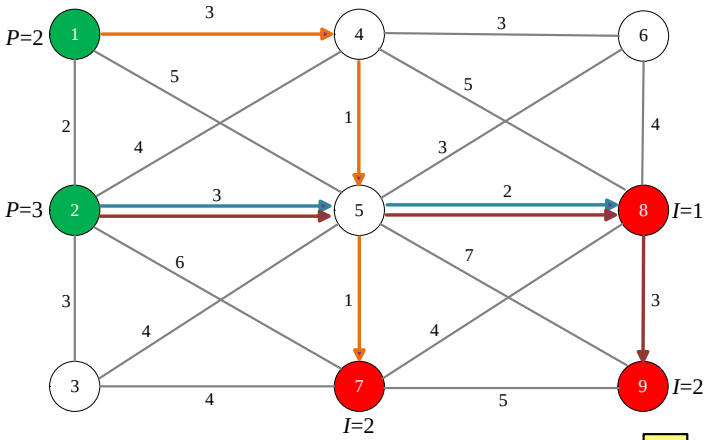
$$\sum_{i=1}^{n} x_{if} - \sum_{j=1}^{n} x_{fj} \geq I_f; \quad \forall f \in F \quad (3)$$

$$\sum_{i=1}^{n} x_{ik} - \sum_{i=1}^{n} x_{kj} = 0; \quad \forall k \in D \quad (4)$$

$$x_{ij} \geq 0; \quad \forall i,j \in N\ . \quad (5)$$

The objective function (1) minimizes the total distance traveled. Constraints (2) and (3) ensure control of the capacities of the source nodes and the demands of the sink nodes, respectively. The constraint set (4) states balance constraints for the remaining nodes. Constraint set (5) implies nonnegativity for the decision variables.

Consider the network shown in Figure 2 to make the structure of the CMSSP. The network consists of 9 nodes and 20 arcs. In this network, nodes 7, 8, and 9 are sink nodes and their demands are 2, 1, and 2-unit, respectively. Nodes 1 and 2 are source nodes and their capacities are 2 and 3 units, respectively. The arc lengths are shown on each corresponding arc. According to the results, the total minimum traveled route is 31 units to satisfy all demands. In this case, the network user prefers route 1→4→5→7 two times to satisfy the demand of node 7, and route 2→5→8 one time to satisfy the demand of node 8, and route 2→5→8→9 two times to satisfy the demand of node 9. The optimal routes for the network user are presented in Figure 2. Different colors are used to show different routes.



Route 1	Route 2	Route 3	Route 4	Route 5
1-4-5-7	1-4-5-7	2-5-8	2-5-8-9	2-5-8-9
5*	5	5	8	8

(*) the traveled distance for each route
The total traveled distance is 31-unit.

Figure 2. *G*(9,20) *network*

3.2. The Capacitated Multiple-Source Multiple-Sink Shortest-Path Network Interdiction Problem (CMSSNIP)

The CMSSNIP deals with the circumstances in which terrorists interdict the aid processes to be provided to these locations on a network after they take destructive actions at several locations at the same time to harm society. In traditional SPNIP, the network user wants to travel from the single source node to the single sink node through the shortest path using the remaining arcs after the intercepts. Additionally, the source nodes have no capacities, and the sink nodes have no demands as well.

The CMSSNIP differs from the known SPNIP in three aspects: (i) All possible sink nodes defined in S, which is the subset of N are starting nodes on the network and its number can be more than one. (ii) Similarly, all possible sink nodes defined in F, which is the subset of N are ending nodes on the network and its number can be more than one. (iii) The source nodes have capacities and the sink nodes have demands.

The network user must start with the nodes in S without exceeding the capacity of each node and must meet the demands of the nodes in F. The network user tries to determine the shortest path, while the attacker maximizes the total distance of the shortest path for the network user by interdicting the arc(s) on the network. In the CMSSNIP, the sides conflict in a two-step and consecutive game process. Initially, the attacker interdicts arcs to maximize the distance of network user's shortest path depending on budget. Then, the network user tries to determine the shortest path using 'interdiction-free' arcs.

In this study four different mathematical models are presented. Two of these models are developed to solve the problems of the network user: (i) the mathematical model for the shortest path (*NU-Model*) and (ii) the corresponding dual model for NU-Model (*NU-Model(D)*). The remaining models deal with the attacker's models: (i) bilevel mathematical model (*I-Model*) and (ii) exact mixed integer mathematical model (*I-Model(F)*) regarding the CMSSNIP.

3.2.1. Problem of the network user: *NU-Model*

The exact formulation of the CMSSP introduced in Section 3.1 corresponds to the network user's model (*NU-Model*).

3.2.2. The dual form of the *NU-Model*: *NU-Model(D)*

The *NU-Model(D)* ensure reducing to a single level of the attacker's bi-level interdiction model in the stage of the modeling of the attacker's problem. In the dual model, y is dual variable related to the constraint sets (2), (3) and (4). There are $i = 1,2,\dots,n$ dual variables, defined in the dual model because there are n constraints in the *NU-Model*.

$$\textit{NU-Model(D)}: Z^* = max \sum_{s=1}^{n} P_s y_s + \sum_{f=1}^{n} I_f y_f \quad (6)$$

Subject to:

$$y_i - y_j \le d_{ij}; \qquad \forall i,j \in (S \cup D) \quad (7)$$

$$y_i + y_f \le d_{if}; \qquad \forall i \in (S \cup D)\ and\ \forall f \in F \quad (8)$$

$$-y_f - y_j \le d_{fj}; \qquad \forall f \in F\ and\ \forall j \in (S \cup D) \quad (9)$$

$$-y_i + y_j \le d_{ij}; \qquad \forall i,j \in F\ and\ i \ne j \quad (10)$$

$$y_s \le 0; \qquad \forall s \in S \quad (11)$$

$$y_f \ge 0; \qquad \forall f \in F \quad . \quad (12)$$

3.2.3. The attacker's problem: I-Model

Firstly, *I-Model* is formulated as a bi-level mathematical model as follows:

I-Model: $Z^* = maxmin \sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij}(d_{ij} + Cw_{ij})$ (13)

Subject to:

$\sum_{j=1}^{n} x_{sj} - \sum_{i=1}^{n} x_{is} \leq P_s; \quad \forall s \in S$ (14)

$\sum_{i=1}^{n} x_{if} - \sum_{j=1}^{n} x_{fj} \geq I_f; \quad \forall f \in F$ (15)

$\sum_{i=1}^{n} x_{ik} - \sum_{i=1}^{n} x_{kj} = 0; \quad \forall k \in D$ (16)

$\sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} b_{ij} \leq T$ (17)

$x_{ij} \geq 0; \quad \forall i, j \in N$ (18)

$w_{ij} \in \{0, 1\} \quad \forall i, j \in N$. (19)

The objective function (13) maximizes the total travelled distance under the interdictions of the arcs. Here, the interdicted arcs' lengths are penalized by *C* units. This causes the network user avoids using the arcs interdicted by the attacker. In other words, if the $\boldsymbol{w_{ij}}$ takes the value 1, the corresponding arc $(\boldsymbol{i}, \boldsymbol{j})$ is interdicted and thus the penalized length of the arc$(\boldsymbol{i}, \boldsymbol{j})$ becomes "$\boldsymbol{d_{ij} + C}$". A constraint set (17) is added, which indicates that the total cost of interdicted arcs is smaller than or equal to the interdiction budget. Constraint sets (18)-(19) are non-negativity and binary constraints for decision variables, respectively.

3.2.4. The final version of the attacker model: *I-Model(F)*

The attacker's bilevel "*max-min*" model is reduced to a single-level "*max-max*" model which is a maximization model. In this transformation, the inner minimization problem is converted to its dual problem by fixing k_{ij} temporarily, and then releasing k_{ij}

I-Model(F): $Z^* = max \sum_{s=1}^{n} P_s y_s + \sum_{f=1}^{n} I_f y_f$ (20)

Subject to:

$y_i - y_j \leq d_{ij} + Cw_{ij}; \quad \forall i, j \in (S \cup D)$ (21)

$y_i + y_f \leq d_{if} + Cw_{if}; \quad \forall i \in (S \cup D) \; and \; \forall f \in F$ (22)

$-y_f - y_j \leq d_{fj} + Cw_{fj}; \quad \forall f \in F \; and \; \forall j \in (S \cup D)$ (23)

$-y_i + y_j \leq d_{ij} + Cw_{ij}; \quad \forall i, j \in F \; and \; i \neq j$ (24)

$\sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} b_{ij} \leq T$ (25)

$y_s \leq 0; \quad \forall s \in S$ (26)

$y_f \geq 0; \quad \forall f \in F$ (27)

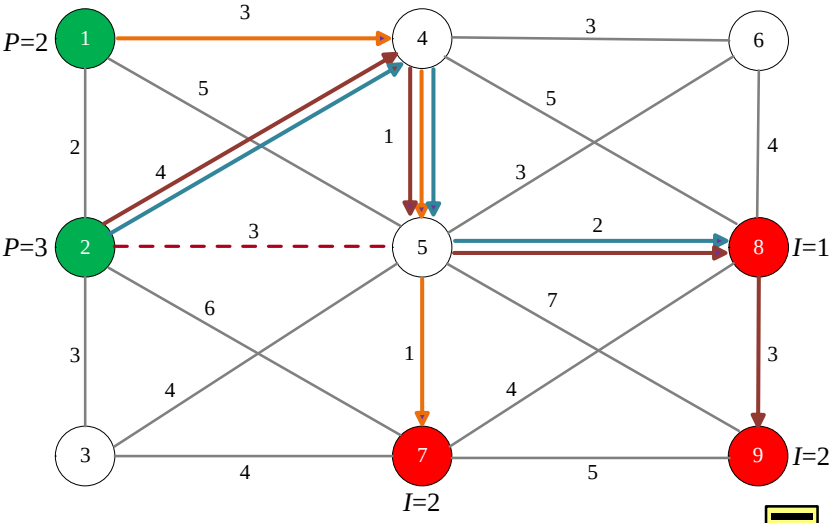
$w_{ij} \in \{0, 1\} \quad \forall i, j \in N$. (28)

The objective function (20) determines the total distance of the shortest path used by the network user after the interdictions of the attacker. Constraint sets (21-24) are dual constraints. The constraint set (25) ensures that the total cost of interdictions is smaller or equal to the budge. If $T = 0$, this model is equivalent to the exact formulation of the CMSSP in terms of generating the same results. The dual variables (26) related to the source nodes must be smaller than 0, and the dual variables (27) related to the sink nodes must be larger than 0. Constraint set (28) is binary constraints.

An illustrative example regarding the CMSSNIP is conducted to better explain the addressed problem. If we recall Figure 2, the thick lines on the network indicate the CMSSP solution. This solution corresponds to the solution to the network user's problem when there is no interdiction, that is, the interdiction budget equals zero.

For different interdiction budgets ($T > 0$), sensitivity analysis is performed for the network represented in Figure 2. The arcs interdicted by the attacker and the total shortest path traveled by the network user are determined for each interdiction budget level and are shown in Figure 3. The optimal routes for the network user are presented in Figure 3 in different colors, while the interdicted arcs are shown by dashed lines. For example, if the attacker has a 1-unit interdiction budget, he increases the total distance by up to 6-units by

interdicting the arc$(2-5)$ (See: Figure 3(a)). Similarly, analyzes are also performed for $T=2$ and $T=3$ on the same network and are shown in Figure 3(b and c). It is observed that the attacker can interdict a certain part of the network in (a and b) while he can interdict all possible paths that reach the demand nodes in (c).

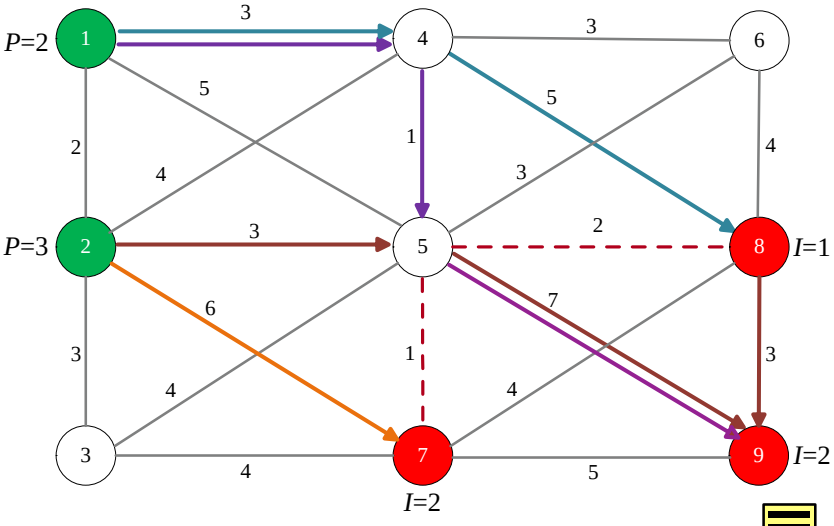


(a) $T=1$

Route 1	Route 2	Route 3	Route 4	Route 5
1-4-5-7	1-4-5-7	2-4-5-8	2-4-5-8-9	2-4-5-8-9
5	5	7	10	10

interdicted arcs

The total traveled distance is 37-unit.



(b) $T=2$

Route 1	Route 2	Route 3	Route 4	Route 5
2-7	2-7	1-4-8	1-4-5-9	2-5-9
6	6	8	11	10

interdicted arcs

The total traveled distance is 41-unit.

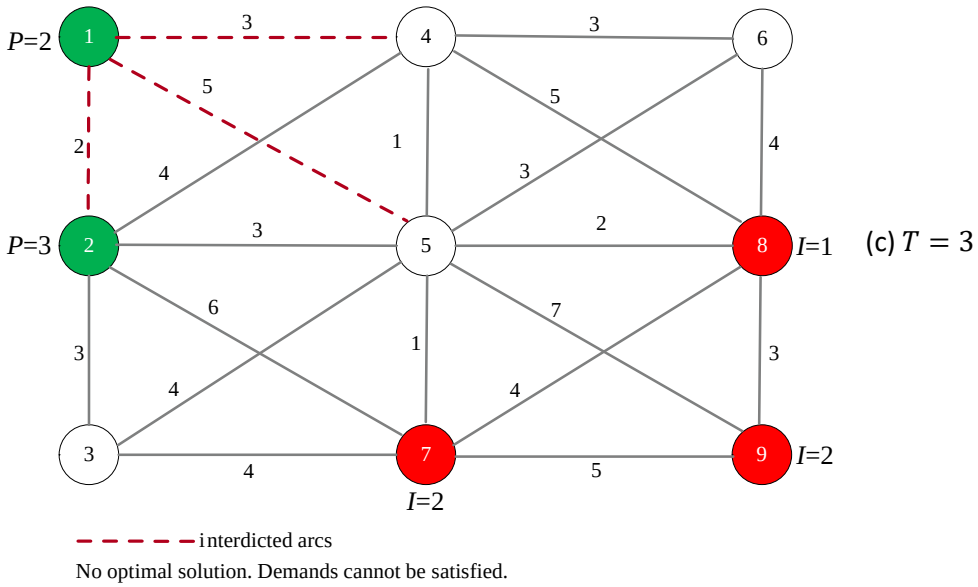


Figure 3. *The travels and interdiction(s) on the* $G(9,20)$ *network*

4. A REAL CASE STUDY IN TURKEY

For usage in national security, well-known optimization issues including network interdiction and vehicle routing issues have been modified [53]. The network interdiction problem was initially stated and addressed in this context, along with many other contemporary homeland security applications. Typically, network interdiction is modeled as a two-player game in which the attacker attempts to destroy or disable a group of network arcs in order to reduce the maximum amount of traffic that can pass through the network, and the defender incurs costs in order to defend or fortify the network arcs (a budget restricts the defender's ability to protect a certain number of network arcs) [33]. A different model for the network interdiction problem shows an attacker attempting to maximize the shortest path between two points. The assumptions made by both the attacker and the defender in this situation regarding arc capacities, current flows, and the cost per unit or effect of arc destruction or disablement are the same. The assumption of perfect information is the name given to this informational presumption. This kind of study is crucial in situations such as the aforementioned example of a covert terrorist attack where there are widespread issues with homeland security [54].

To investigate conflict scenarios regarding city safety, Şişli, one of the districts of İstanbul province in Turkey, is considered. Şişli is one of the important central districts of Istanbul, the largest city in Turkey. The district, which has a daytime population of more than 3 million, has recently become the most important commercial and cultural center in Istanbul. It is known that the density of industry, workplaces, trade centers, and the daytime population is very high as a result of the flow of people who come from all over Istanbul to work, visit, and shopping. The district, which is a frequent destination for people, is very crowded at night with touristic service hotels and entertainment venues. In short, Şişli is one of the important residential areas of Istanbul and Turkey. At this point, it is essential to increase security measures in the district and to be prepared for terrorist attacks. For these reasons, Şişli district has been determined as the application area. A map showing provincial distribution of Istanbul can be seen in Figure 4.

Figure 4. *The map of Istanbul*

In this context, a real-case application is performed based on the approximate locations and distances extracted from Google Maps. The map considered is given in Figure 5. This figure shows approximate locations of the police stations and possible crime regions and represents a situation where terror groups harm the environment or society in two regions denoted in red at the same time. The number in police vehicles of the police stations is represented in Figure 5 for all scenarios as capacity. Similarly, the demands for the crime locations are represented by the number of police cars required and are given in Table 3 for each scenario.

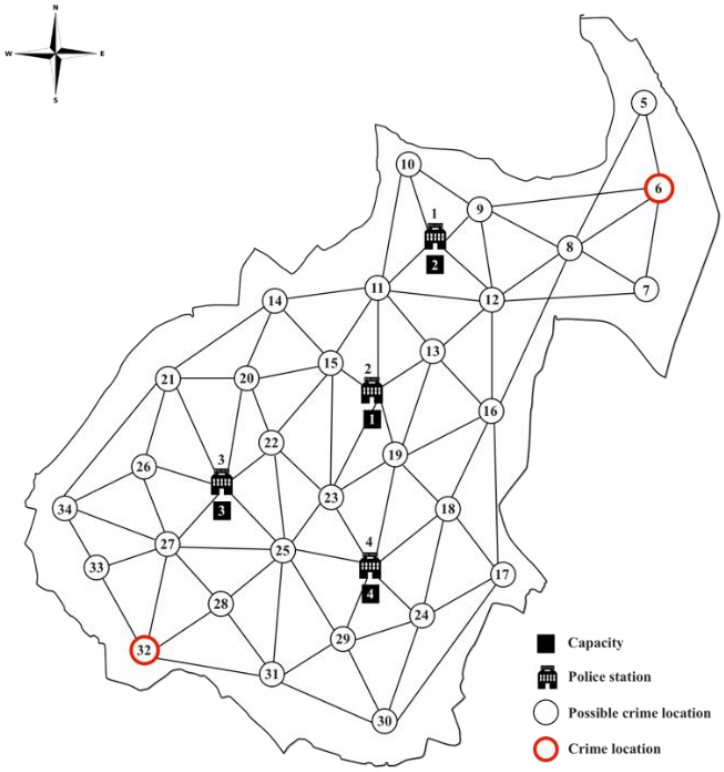


Figure 5. *The approximate locations of the police stations and possible crime regions in Şişli*

Table 2 shows the lengths between the nodes and the interdiction costs of the roads. Geographic features or security aspects can affect the costs of interdiction to interdict the roads. As mentioned above, the interdiction costs are adjusted in accordance with equipment number of the required to interdict corresponding arcs. In this context, scenarios are constructed considering conflict situations against crimes occurring in different numbers and analyzed under different levels of interdiction budget levels in the

addressed regions. Table 3 reports all computational results in terms of the objective function values, interdicted arcs, and runtimes (in seconds) under varying interdiction budgets for different scenarios.

Table 2. *The lengths and interdiction costs of the roads in the addressed network*

A	D	I.C.	A	D	I.C.	A	D	I.C.	A	D	I.C.	A	D	I.C.	A	D	I.C.
(1-9)	0.36	2	(3-27)	0.55	3	(8-9)	0.49	2	(14-15)	0.50	2	(19-23)	0.48	2	(26-27)	0.44	2
(1-10)	0.52	3	(4-18)	0.65	3	(8-12)	0.53	3	(14-20)	0.54	3	(20-21)	0.45	2	(26-34)	0.45	2
(1-11)	0.48	2	(4-19)	0.68	3	(8-16)	0.85	4	(14-21)	0.67	3	(20-22)	0.38	2	(27-28)	0.40	2
(1-12)	0.55	3	(4-23)	0.50	2	(9-10)	0.47	2	(15-20)	0.62	3	(21-26)	0.44	2	(27-32)	0.56	3
(2-11)	0.62	3	(4-24)	0.43	2	(9-12)	0.51	3	(15-22)	0.68	3	(21-34)	0.70	3	(27-33)	0.36	2
(2-13)	0.46	2	(4-25)	0.58	3	(10-11)	0.74	3	(15-23)	0.74	3	(22-23)	0.35	2	(27-34)	0.49	2
(2-15)	0.27	2	(4-29)	0.52	3	(11-12)	0.58	3	(16-17)	0.85	4	(22-25)	0.42	2	(28-31)	0.48	2
(2-19)	0.45	2	(5-6)	0.54	3	(11-13)	0.60	3	(16-18)	0.69	3	(23-25)	0.30	2	(28-32)	0.51	3
(2-23)	0.70	3	(5-8)	0.80	4	(11-14)	0.56	3	(16-19)	0.65	3	(24-29)	0.39	2	(29-30)	0.60	3
(3-20)	0.72	3	(6-7)	0.66	3	(11-15)	0.55	3	(17-18)	0.51	3	(24-30)	0.47	2	(29-31)	0.48	2
(3-21)	0.74	3	(6-8)	0.62	3	(12-13)	0.48	2	(17-24)	0.55	3	(25-27)	0.56	3	(30-31)	0.65	3
(3-22)	0.48	2	(6-9)	0.92	4	(12-16)	0.55	3	(17-30)	0.92	4	(25-28)	0.49	2	(31-32)	0.72	3
(3-25)	0.55	3	(7-8)	0.49	2	(13-16)	0.61	3	(18-19)	0.45	2	(25-29)	0.63	3	(32-33)	0.56	3
(3-26)	0.60	3	(7-12)	0.77	4	(13-19)	0.72	3	(18-24)	0.53	3	(25-31)	0.55	3	(33-34)	0.38	2

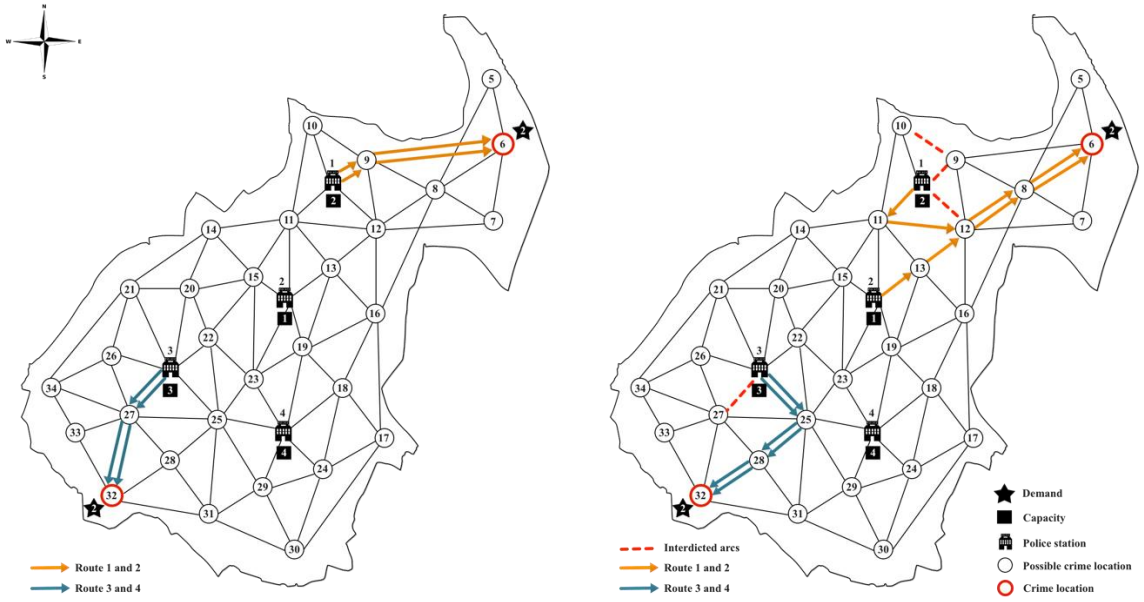
A, D, and I.C. represent arcs, distances (km), and interdiction cost (number of required equipments), respectively.

According to Table 3, it is worth stating that all optimal results are achieved in seconds. This fact reveals the tractability of the proposed model for real implementation. Additionally, the total length of the shortest path is seen to increase as the level of the interdiction budget increases. It is observed that the interdictors can achieve interdicting all possible roads to at least one crime location at a certain level of interdiction budget. In other words, if the demand for even at least one crime location cannot be satisfied, a feasible solution cannot be attained. This situation is indicated in Table 3, as "no optimal solution". To visualize the results, the results related to scenarios 2 and 3 are drawn on the addressed network for different interdiction budgets and shown in Figures 6 and 7, respectively. While Figures 6(a) and 7(a) show the shortest paths to the crime locations when there is no interdiction, Figures 6(b) and 7(b) show the shortest paths to the crime locations under interdiction for $T = 10$ and $T = 7$, respectively.

Table 3. *The computational results for all scenarios*

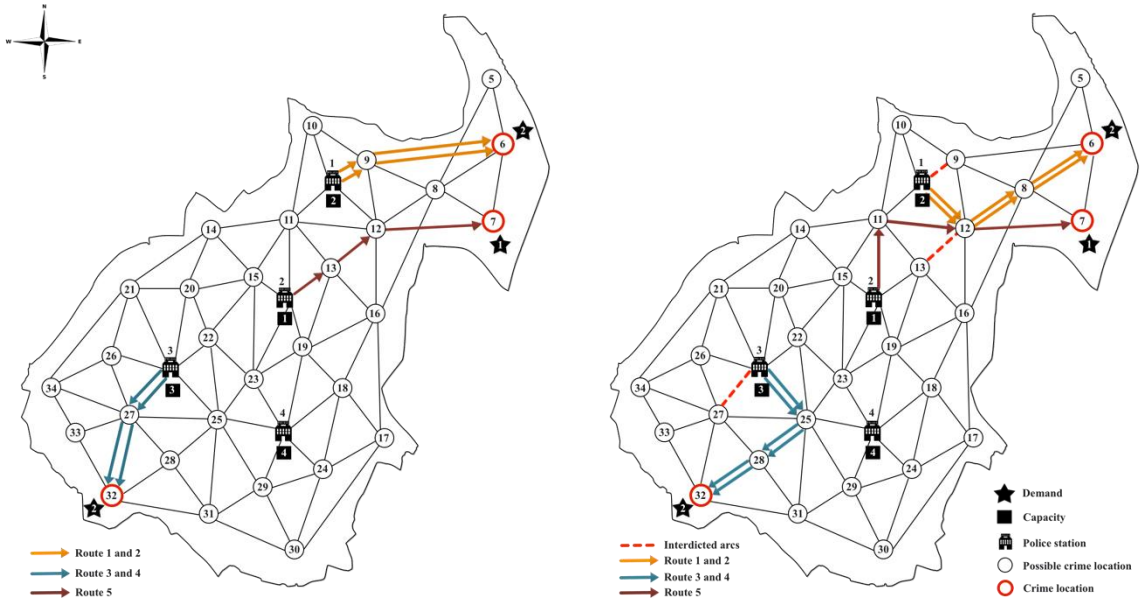
Scenario 1: Crime location: 6; Demand: 4 vechicles			
T	**Runtime (in sec)**	***Shortest path length (in km) (Z*)***	**Interdicted arcs**
0	***	7.45	***
1	0.78	7.45	***
2	0.85	8.29	(1-9)
3	0.85	8.29	(1-9)
4	0.97	8.55	(1-9), (2-13)
5	0.91	9.50	(1-9), (8-6)
6	1.01	9.50	(1-9), (8-6)
7	1.00	9.76	(1-9), (8-6), (2-13)
8	1.25	9.76	(1-9), (8-6), (2-13)
9	1.20	10.68	(1-9), (10-9),(1-11), (1-12)
10	1.16	11.12	(1-9), (1-10),(1-11), (1-12)
11	1.26	11.12	(1-9), (1-10),(1-11), (1-12)
12	1.71	12.22	(1-9), (8-6), (10-9),(1-11), (1-12)
13	0.78	No optimal solution	(8-6), (9-6), (7-6), (5-6)
Scenario 2: Crime locations: 6 and 32; Demands: 2 vechicles for each crime location			
T	**Runtime (in sec)**	***Shortest path length (in km) (Z*)***	**Interdicted arcs**
0	***	4.78	***
1	0.84	4.78	***
2	0.79	5.62	(1-9)
3	0.82	5.66	(3-27)
4	0.89	5.66	(3-27)
5	0.90	6.50	(1-9), (3-27)
6	1.13	6.50	(1-9), (3-27)
7	0.90	6.60	(1-9), (3.27), (25-28)
8	1.24	6.92	(1-9), (3-27), (8-6)
9	1.04	7.11	(1-9), (10-9), (1-11), (1-

			12)
10	1.44	7.40	(1-9), (10-9), (1-12), (3-27)
11	1.41	7.40	(1-9), (10-9), (1-12), (3-27)
12	0.94	No optimal solution	(27-32), (28-32), (31-32), (33-32)
Scenario 3: Crime location: 6, 7, and 32; Demands: 2 vechicles for 6th and 32nd locations, and 1 vechicle for 7th location			
T	**Runtime (in sec)**	***Shortest path length (in km) (Z*)***	**Interdicted arcs**
0	***	6.49	***
1	0.80	6.49	***
2	0.83	7.33	(1-9)
3	0.83	7.37	(3-27)
4	0.80	7.59	(1-9), (2-13)
5	0.90	8.21	(1-9), (3-27)
6	0.83	8.21	(1-9), (3-27)
7	0.84	8.47	(1-9), (3-27), (13-12)
8	0.94	8.63	(1-9), (1-12), (3-27)
9	0.87	No optimal solution	(6-7), (8-7), (12-7)
Scenario 4: Crime locations: 6, 7, 22, and 32; Demands: 1 vehicle for each crime location			
T	**Runtime (in sec)**	***Shortest path length (in km) (Z*)***	**Interdicted arcs**
0	***	4.19	***
1	0.83	4.19	***
2	0.78	4.61	(1-9)
3	0.95	4.63	(3-27)
4	0.86	4.98	(1-9), (3-22)
5	0.84	5.21	(1-9), (1-12)
6	0.87	5.21	(1-9), (1-12)
7	0.94	5.58	(1-9), (1-12), (3-22)
8	1.20	5.65	(1-9), (8-7), (12-7)
9	0.87	No optimal solution	(6-7), (8-7), (12-7)



(a) (b)

Figure 6. *Visualization of the results for scenario 2: (a)* $T = 0$ *and* $T = 10$



(a) (b)

Figure 7. *Visualization of the results for scenario 3: (a)* $T = 0$ *and (b)* $T = 7$

5. COMPUTATIONAL EXPERIMENTS

In this section, computational experiments are performed in two ways. (i) Performance of the *I-Model(F)* is tested on varying-sized networks generated randomly. This analysis is carried out for each network $G(9, 20), G(21, 79), G(43,234), G(86, 476)$ and $G(190, 1542)$. (ii) Changes in the objective function value are observed according to different numbers of source and sink nodes on the network $G(21, 79)$. The interdiction cost of each arc is assumed as 1-unit in all applications.

In all experiments, the interdiction budget level is increased until the solution becomes infeasible. The infeasible solution is obtained when the attacker can interdict all possible paths to at least one demand node. In this case, the network user cannot satisfy the demands and the optimal objective function takes an extremely large value depending on the determined C parameter in Equation (13).

(i) Analysis of model performance:

Besides the network $G(9, 20)$ discussed in Section 3, the performance of *I-Model(F)* is tested on the networks $G(21, 79), G(43, 234), G(86, 476)$, and $G(190, 1542)$ in terms of runtime (in seconds). The experimental results are summarized in terms of attained runtimes achieved and objective function values for each level of the interdiction budget and given in Table 4 for all generated instances. The results emphasize that the *I-Model(F)* can solve all the problems addressed optimally. Although runtime slightly increases depending on network size for low interdiction budget levels (i.e., $T = 1,\ T = 2$), the runtime obviously increases exponentially depending on the increase in the interdiction budget in all instances. Especially in the network $G(190, 1542)$, the runtimes change from 9.33 sec to 243562 sec although *I-Model(F)* can solve the problems. For this network, the runtime exceeded 24 hours for some T levels in this network. In Table 4, two optimal solutions are the same on $T = 12$ and $T = 13$ budget for the network $G(190, 1542)$ since there are alternative paths that give the same optimal solution value. Redundancy occurs due to the discrete interdiction (discrete decision variable). In such a case, it is reasonable that the attacker prefers a lower budget interdiction plan ($T = 12$) to achieve the value of the aimed objective function. For the interested readers, detailed information on the efficient usage of limited interdiction budget can be found at [55]. Generally, as the number (interdiction budget level (T)) increases, the total distance traveled by the network user also increases. (See Figure 5).

Table 4. *The experimental results of the model performance analysis based on different networks*

G	Number of source nodes	Number of sink nodes	*N*	*A*	*T*	Shortest path length (Z^*)	Runtime (in sec)
G (9,20)	2	3	9	20	0	31	0.52
					1	37	0.68
					2	41	0.65
					3	No optimal solution[a]	0.77
G (21,79)	3	2	21	79	0	62	0.64
					1	67	0.84
					2	72	1.19
					3	77	1.41
					4	80	4.31
					5	86	7.42
					6	98	8.64
					7	100	18.73
					8	101	101.25
					9	108	197.25
					10	No optimal solution	0.78
G (43,234)	4	2	43	234	0	73	0.66
					1	80	1.40
					2	89	1.53
					3	99	3.41
					4	105	13.12
					5	112	164.68
					6	115	1402.9
					7	No optimal solution	0.79
G (86,476)	4	2	86	476	0	226	0.78
					1	229	5.42
					2	238	11.84
					3	240	179.32
					4	243	1133.2
					5	250	16150
					6	255	27988
					7	268	34323
					8	273	41028
					9	No optimal solution	10.53
G (190, 1542)	2	5	190	1542	0	423	1.65
					1	443	9.33
					2	461	146.09
					3	473	194.97
					4	480	328.02
					5	485	1598.69
					6	491	16996.25
					7	495	29321
					8	499	34652
					9	502	57821
					10	508	96624
					11	509	143523
					12	516	210462
					13	516	243562
					14	No optimal solution	1.12

(a) The attacker can interdict all possible paths to at least one demand node. There is no optimal solution since the objective function value takes an abnormally value.

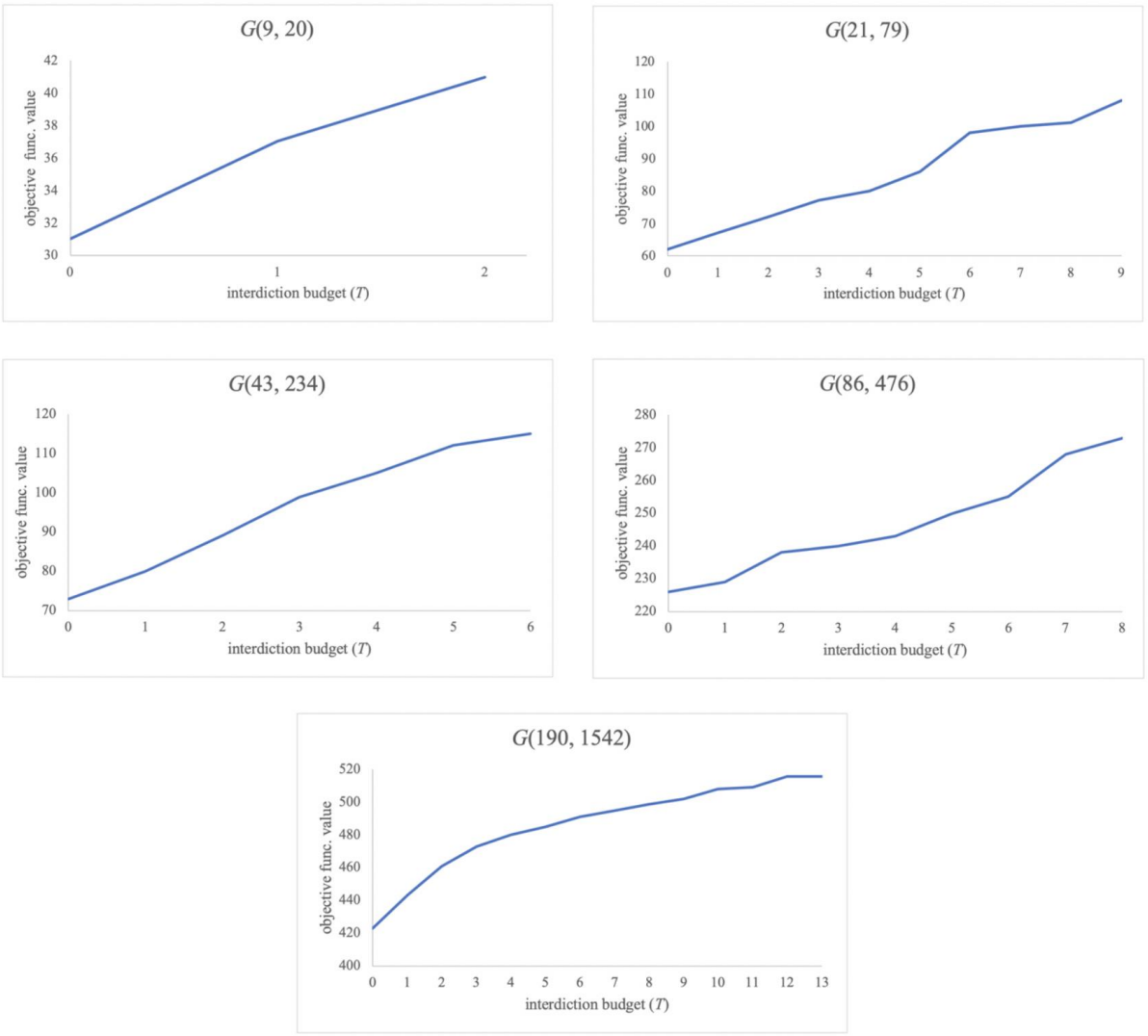


Figure 7. *The objective function value & Interdiction budget level graphs for the networks*

(ii) Impact of the number of source and sink nodes:

In this analysis, changes in the objective function are observed under varying numbers of source and sink nodes for the network $G(21,79)$ given in Figure 8. In this regard, nodes 1, 2, 3, 4, and 5 are selected for the source nodes, while nodes 17, 18, 19, 20, and 21 are selected for the sink nodes on the addressed network. Possible some problems are constructed by considering the combinations among these nodes. For example, in Table 5, the first row represents the problem in which nodes 1 and 2 are selected for source nodes, and nodes 20 and 21 are selected for sink nodes. Similarly, the seventh row represents the problem in which nodes 1, 2, 3, and 4 are selected for the source nodes, and nodes 19, 20, and 21 are selected for the sink nodes.

The experimental results are obtained for $T = 2$ by considering the addressed network and are given in Table 5.

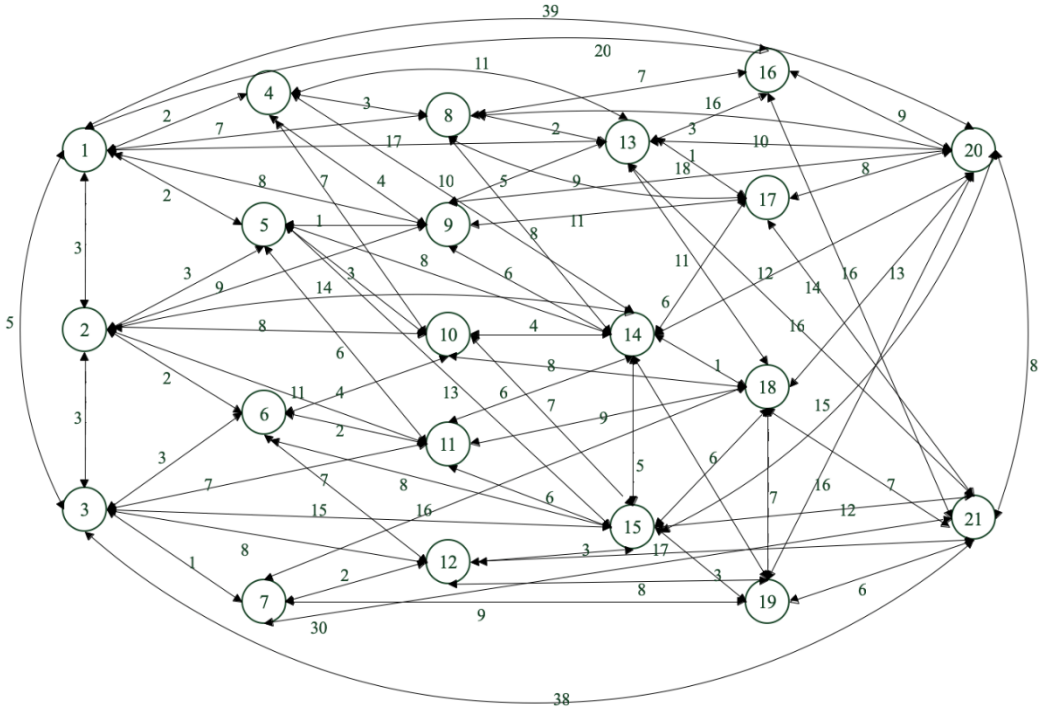


Figure 8. *$G(21,79)$ network*

Table 5. *Experimental results according to numbers of source and sink nodes in the network G(21, 79)*

Number of source nodes	Number of sink nodes	Interdicted arcs	Nominal shortest path lenght	After interdictions, shortest parth lenght	Runtime (in sec)
2	2	(8-13), (9-13)	33	38	0.52
3	2	(8-13), (9-13)	31	36	0.02
4	2	(3-7), (4-8)	29	34	0.06
5	2	(3-7), (4-8)	29	34	0.33
2	3	(3-7),(15-19)	45	50	0.31
3	3	(3-7),(15-19)	42	49	0.16
4	3	(3-7),(15-19)	40	47	0.34
5	3	(3-7),(18-21)	38	46	0.34
2	4	(18-21),(19-21)	58	60	0.03
3	4	(18-21),(19-21)	55	57	0.05
4	4	(18-21),(19-21)	53	55	0.23
5	4	(18-21),(19-21)	49	53	0.05
2	5	(1-5),(13-17)	71	75	0.33
3	5	(1-5),(13-17)	67	72	0.58
4	5	(3-7),(13-17)	64	69	0.36
5	5	(8-13),(9-13)	58	63	0.38

The proposed *I-Model(F)* is run 111 times with different-sized network instances, including the real case implementation analyzes. According to the experimental results, the solutions are computationally tractable. On the other hand, the proposed model provides resilient strategies against interdictions in terms of safe shortest paths at the operational level within seconds in the real case application. Even the *I-Model(F)* can optimally solve all generated network instances and prove interdiction plans.

According to the computational experiments, some insights are provided as follows.

- The experimental results show that *I-Model(F)* can provide all possible optimal interdiction plans considering the attacker's all interdiction capabilities related to the addressed network.
- It is observed that all generated networks can be solved with the *I-Model(F)*.
- In Table 4, results show that the runtime slightly increases depending on the size of the network for low interdiction budget levels (i.e., $T = 1$, $T = 2$), and the runtime obviously increases exponentially depending on the increase in the interdiction budget in all instances.
- As expected, the *I-Model(F)* could not solve the problem within 24 hours, although it can give optimal solutions on some T levels for the network $G(190, 1542)$. Therefore, it will become more difficult to obtain the optimal solution after this size to make decisions, especially at the operational level. On the other hand, the *I-Model(F)* is also effective in relatively large-scale networks in terms of runtime performance to make decisions at the operational level. This situation is proven by a real case study conducted in Section 4. In this context, the proposed attack optimization model for the CMSSNIP can be employed in defense systems.
- From Table 5, it is deduced that the length of the shortest path decreases as the number of source nodes increases. For example, when the number of sink nodes is 2, the shortest path length is 33-unit with 2 source nodes, whilst the shortest path length is 29-unit with 5 source nodes. On the length of the other hand, the shortest path increases as the number of sink nodes increases. It can be said that alternative routes, which occurred with an increase in the number of source nodes, cause a decrease in the shortest path length.
- It can be inferred that the proposed optimization model is sensitive to different numbers of source nodes and sink nodes since reasonable results are obtained in different combinations of the number of source nodes and sink nodes.

6. CONCLUSION AND DISCUSSION

It is a critical issue that humanitarian processes are provided quickly in city transportation networks when a terror act occurs. This study aims to help decision makers to develop resilience strategies by determining the most vital arcs and nodes under terrorist interdictions in the city transport network for the provision of these humanitarian processes in a safe environment. For this purpose, first, the capacitated shortest path problem (CMSSP) is defined and formulated. Later, CMSSNIP, handling the situations in which terrorists interdict the aid processes to be provided to these locations on a network after they take devastating actions at several locations at the same time to harm society, is presented and formulated. By doing so, the *I-Model(F)*, corresponding to the attacker's model and can be used effectively in defense systems at the operational level since the model provides interdiction plans (i.e., likely roads to be interdicted) of the attacker, is presented.

Real-life case implementation is performed through a set of scenarios based on the interdiction budget levels and the number of crime locations to show the applicability of the model. In addition, computational experiments are performed to see the performance of the *I-Model(F)* in terms of the runtime at the generated different-sized network instances and to reveal the changes in the objective function value according to varying numbers of source and sink nodes.

The contributions of the paper can be summarized as follows: (i) The CMSSP is defined, and its mathematical model is presented. (ii) CMSSNIP, which is the extension of CMSSP in the NIP framework, is studied for the first time. (iii) An exact formulation that will be able to use directly in defense systems is proposed to enhance security regarding the aid processes against especially terror acts. (iv) Guided discussions are made related to the objective function values and runtimes for the instances by considering different interdiction budget levels.

The following identifies some current limits of modeling and solution techniques for tackling issues brought on by variations of the shortest path network interdiction problem. First, optimizing adaptive security measures against terrorist attacks computationally efficiently is a barrier to their successful implementation in large-scale systems with a large number of nodes. In order for these algorithms to calculate nearly optimal strategies, it is imperative to create the next generation of computationally efficient algorithms and reliable

computational infrastructure. Second, some data may not be available in real city systems, and assumptions about terrorists' knowledge levels may not always be correct. In such cases, the problem can be addressed through stochastic or fuzzy approaches. Third, the majority of current defensive tactics are reactive in nature. Existing reactive defense techniques may soon approach their limits in reducing these dangers, since threats from terrorist attacks are increasing quickly in both quantity and variety. It is necessary to develop new defense tactics, such as deliberately sabotaging the information networks that link terrorist organizations and operatives.

For the future research, the study may be extended in some interesting directions: (i) Metaheuristic algorithms can be developed in case optimal solutions cannot be obtained at larger network sizes. (ii) In this paper, the attacker tries solely to maximize the total shortest path achieved by the network user. The CMSSNIP can be studied as a multi-objective optimization problem that maximizes the total traveled shortest path by the network user and minimizes the interdiction budget simultaneously. (iii) We handle a CMSSNIP for the crisp environment. In CMSSNIP, the arc lengths, node demands, or capacities can be considered as fuzzy numbers to cope with uncertainties. (iv) In the CMSSNIP, the attacker considers the single interdiction resource. Multiple interdiction resources, which vary depending on interdiction success rates or costs, may be added to the model. In the study, the interdiction success rate of the corresponding interdiction resource is considered 100%. That is, if the attacker interdicts the arc, the arc is destroyed completely. The effect of partial interdictions of arcs may also be examined by adding different interdiction resources to the model. (v) Besides, it might be handled that terrorists attack a target audience or a building, a crowded place in general, or a place in a city where the main assets are already well known. For example, the proposed models can be used as a decision support system to increase security measures in possible attacks on points such as intersections, public buildings, public transport stops, etc. Thus, strategies can be developed in the city's security plans.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Zheng, K., Albert, L.A., "Interdiction models for delaying adversarial attacks against critical information technology infrastructure", Naval Research Logistics, 66(5): 411–429, (2019).

[2] Fang, Y., Sansavini, G., Zio, E., "An Optimization-Based Framework for the Identification of Vulnerabilities in Electric Power Grids Exposed to Natural Hazards", Risk Analysis, 39(9): 1949–1969, (2019).

[3] Baycik, N.O., Sharkey, T.C., "Interdiction-Based Approaches to Identify Damage in Disrupted Critical Infrastructures with Dependencies", Journal of Infrastructure Systems, 25(2): 04019013, (2019).

[4] Ghorbani-Renani, N., González, A.D., Barker, K., Morshedlou, N., "Protection-interdiction-restoration: Tri-level optimization for enhancing interdependent network resilience", Reliability Engineering & System Safety, 199: 106907, (2020).

[5] Bhuiyan, T.H., Medal, H.R., Nandi, A.K., Halappanavar, M., "Risk-averse bi-level stochastic network interdiction model for cyber-security risk management", International Journal of Critical Infrastructure Protection, 32: 100408, (2021).

[6] Israeli E., Wood R.K., "Shortest-path network interdiction", Networks, 40(2): 97–111, (2002).

[7] Xiang, Y., Wei, H., "Joint optimizing network interdiction and emergency facility location in terrorist attacks", Computers & Industrial Engineering, 144: 106480, (2020).

[8] Sefair, J.A., Smith, J.C., "Dynamic shortest-path interdiction", Networks, 68(4): 315–330, (2016).

[9] Lubore, S.H., Ratliff, H.D., Sicilia, G.T., "Determining the most vital link in a flow network", Naval Research Logistics, 18(4): 497–502, (1971).

[10] Wollmer, R.D., "Some methods for determining the most vital link in a railway network", Rand Corporation, (1963).

[11] Ball, M.O., Golden, B.L., Vohra, R.V., "Finding the most vital arcs in a network", Operations Research Letters, 8(2): 73–76, (1989).

[12] Ratliff, H.D., Sicilia, G.T., Lubore, S.H., "Finding the n Most Vital Links in Flow Networks", Management Science, 21(5): 531–539, (1975).

[13] Wollmer, R., "Removing Arcs from a Network", Operations Research, 12(6): 934–940, (1964).

[14] Jiang, Y., Hu, A., "Finding the Most Vital Link with Respect to the Characteristic of Network Communication", Journal of Networks, 6(3): 462–469, (2011).

[15] Lin, K.C., Chern, M.S., "The fuzzy shortest path problem and its most vital arcs", Fuzzy Sets and Systems, 58(3): 343–353, (1993).

[16] Malik, K., Mittal, A.K., Gupta, S.K., "The k most vital arcs in the shortest path problem", Operations Research Letters, 8(4): 223–227, (1989).

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

[18] Brown, G., Carlyle, M., Salmerón, J., Wood, K., "Defending critical infrastructure", Interfaces (Providence), 36(6): 530–544, (2006).

[19] Yao, Y., Edmunds, T., Papageorgiou, D., Alvarez, R., "Trilevel optimization in power network defense", IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(4): 712–718, (2007).

[20] Delkhosh, F., "A dynamic leader-follower model based on lack of central authority in emergency situations", International Journal of Data and Network Science, 4(1): 73–90, (2020).

[21] Johnson, M.P., Gutfraind, A., "Evader interdiction and collateral damage", In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer, Berlin, Heidelberg, 86–100, (2012).

[22] Karabulut, E., Aras, N., Altınel, K., "Optimal sensor deployment to increase the security of the maximal breach path in border surveillance", European Journal of Operational Research, 259(1): 19–36, (2017).

[23] Pan, F., Charlton, W.S., Morton, D.P., "A stochastic program for interdicting smuggled nuclear material", Operations Research/Computer Science Interfaces Series, 22: 1–19, (2003).

[24] Morton, D.P., Pan, F., "Using Sensors to Interdict Nuclear Material Smuggling", In IIE Annual Conference. Proceedings, Institute of Industrial and Systems Engineers (IISE), (2005).

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

[26] Golden, B., "A problem in network interdiction", Naval Research Logistics, 25(4): 711–713, (1978).

[27] Corley, H.W., David, Y.S., "Most vital links and nodes in weighted networks", Operations Research Letters, 1(4): 157–160, (1982).

[28] Dijkstra, E.W., "A note on two problems in connexion with graphs", Numerische Mathematik, 1(1): 269–271, (1959).

[29] Khachiyan, L., Gurvich, V., Zhao, J., "Extending Dijkstra's algorithm to maximize the shortest path by node-wise limited arc interdiction", In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 221–234, (2006).

[30] Khachiyan, L., Boros, E., Borys, K., Elbassioni, K., Gurvich, V, Rudolf, G., Zhao, J., "On short paths interdiction problems: Total and node-wise limited interdiction", Theory of Computing Systems, 43(2): 204–233, (2008).

[31] Bayrak, H., Bailey, M.D., "Shortest path network interdiction with asymmetric information", Networks, 52(3): 133–140, (2008).

[32] Ramirez-Marquez, J.E., Rocco, C.M., "A bi-objective approach for shortest-path network interdiction", Computers & Industrial Engineering, 59(2): 232–240, (2010).

[33] Yates, J., Sanjeevi, S., "A length-based, multiple-resource formulation for shortest path network interdiction problems in the transportation sector", International Journal of Critical Infrastructure Protection, 6(2): 107–119, (2013).

[34] Yates, J., Wang, X., Chen, N., "Assessing the effectiveness of k-shortest path sets in problems of network interdiction", Optimization and Engineering, 15(3): 721–749, (2014).

[35] Yates, J., Chen, N., "A Spatial Segmentation Algorithm for Resource Allocation in an Integrated Spatial and Networked Environment", Applied Spatial Analysis and Policy, 7(4): 317–336, (2014).

[36] Song, Y., Shen, S., "Risk-Averse Shortest Path Interdiction", INFORMS Journal on Computing, 28(3): 527–539, (2016).

[37] Casas, I., Delmelle, E., Yates, J., "Geographic characteristics of a network interdiction problem", Geo Journal, 81(1): 37–53, (2016).

[38] Borndörfer, R., Sagnol, G., Schwartz, S., "An Extended Network Interdiction Problem for Optimal Toll Control", Electronic Notes in Discrete Mathematics, 52: 301–308, (2016).

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

[40] Sadeghi, S., Seifi, A., Azizi, E., "Trilevel shortest path network interdiction with partial fortification", Computers & Industrial Engineering, 106: 400–411, (2017).

[41] Lozano, L., Smith, J.C., "A backward sampling framework for interdiction problems with fortification", INFORMS Journal on Computing, 29(1): 123–139, (2017).

[42] Pay, B.S., Merrick, J.R.W., Song, Y., "Stochastic network interdiction with incomplete preference", Networks, 73(1): 3–22, (2019).

[43] Bidgoli, M.M., Kheirkhah, A.S., "An arc interdiction vehicle routing problem with information asymmetry", Computers & Industrial Engineering, 115: 520–531, (2018).

[44] Quadros, H., Costa Roboredo, M., Alves Pessoa, A., "A branch-and-cut algorithm for the multiple allocation r-hub interdiction median problem with fortification", Expert Systems with Applications, 110: 311–322, (2018).

[45] Ayyildiz, E., Özçelik, G., Demirci, E., "Multiple-Sink Shortest Path Network Interdiction Problem", Sigma Journal of Engineering and Natural Sciences, 9(4): 395–403, (2018).

[46] Wei, X., Xu, K., Jiao, P., Yin, Q., Zha, Y., "A Decomposition Approach for Stochastic Shortest-Path Network Interdiction with Goal Threshold", Symmetry (Basel), 11(2): 237, (2019).

[47] Baycik, N.O., Sullivan, K.M., "Robust location of hidden interdictions on a shortest path network", IISE Transactions, 51(12): 1332–1347, (2019).

[48] Ketkov, S.S., Prokopyev, O.A., "On greedy and strategic evaders in sequential interdiction settings with incomplete information", Omega (United Kingdom), 92: 102161, (2020).

[49] Yates, J., Lakshmanan, K., "A constrained binary knapsack approximation for shortest path network interdiction", Computers & Industrial Engineering, 61(4): 981–992, (2011).

[50] Borrero J.S., Prokopyev O.A., Sauré D., "Sequential Shortest Path Interdiction with Incomplete Information", Decision Analysis, 13(1): 68–98, (2016).

[51] Ayyildiz, E., Ozcelik, G., Temel Gencer, C., "Determining the most vital arcs on the shortest path for fire trucks in terrorist actions that will cause fire", Communications Faculty of Sciences University of Ankara Series A1: Mathematics and Statistics, 68(1): 441–450, (2019).

[52] Xu, K., Zeng, Y., Zhang, Q., Yin, Q., Sun, L., Xiao, K., "Online probabilistic goal recognition and its application in dynamic shortest-path local network interdiction", Engineering Applications of Artificial Intelligence, 85: 57–71, (2019).

[53] Zhang, J., Zhuang, J., Behlendorf, B., "Stochastic shortest path network interdiction with a case study of Arizona–Mexico border", Reliability Engineering & System Safety, 179: 62–73, (2018).

[54] Yates, J., Casas, I., "Role of Spatial Data in the Protection of Critical Infrastructure and Homeland Defense", Applied Spatial Analysis and Policy, 5(1): 1–23, (2012).

[55] Özçelik, G., Gencer, C., "A goal programming model that ensures efficient usage of limited interdiction budget in the procurement game", Croatian Operational Research Review, 9(1): 75–85, (2018).