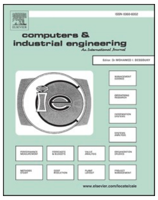
Contents lists available at ScienceDirect

Computers & Industrial Engineering

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



A decomposition approach for solving tri-level defender-attacker-defender problems

Nafiseh Ghorbani-Renani, Andrés D. González, Kash Barker [*]

School of Industrial and Systems Engineering, University of Oklahoma, Norman, OK, USA

ARTICLE INFO

Keywords:
Resilience
Interdependent infrastructure networks
Network interdiction model
Tri-level optimization
Decomposition-based algorithm

ABSTRACT

Network-based systems widely appear in different service, community, industrial, and economic systems such as electric power, water supply, transportation, and telecommunication networks. Due to the significant role of such systems in society, it is essential to have an effective plan to enhance the resilience of infrastructure networks against disruption (e.g., natural disasters, malevolent attacks, or operational failures). In relation to the concept of resilience, two relevant questions arise: (i) how does performance degrade after a disruption, or what is the vulnerability of the system? and (ii) how rapid does the disrupted system return to the desired performance level, or how can we characterize the system's recoverability? To enhance the resilience of a system against disruption, we address simultaneous actions of vulnerability reduction and recoverability enhancement through interdiction model, particularly defender-attacker-defender (DAD) model. However, the proposed model is computationally challenging to solve. To deal with this issue, we design a decomposition-based solution algorithm as a general framework to optimally solve tri-level DAD models in more efficiently. The proposed solution technique is demonstrated with the existing DAD model, namely a tri-level protection-interdiction-restoration model. To define the critical components subject to protection and disruption, an efficient clustering technique is applied which results in generating three sets of candidate components based on three centrality measures. We represent an illustrative case study based on the system of interdependent infrastructure networks in Shelby County, TN, for which we solve the model and assess the computational results for each set of candidate components. The results indicate that the proposed solution algorithm substantially outperforms the traditional covering decomposition method with regard to computational complexity, particularly for the higher budget scenarios. Finally, we compare and analyze the results of the existing interdiction model, the protection-interdiction-restoration formulation represented by M-I, with a new protection-interdiction-counteraction model, denoted by M-II, in which the restoration level is not considered. Results suggest that although M-I is a comprehensive interdiction model relative to M-II, it suffers substantially from computational complexity. Therefore, there exists a tradeoff between employing a more comprehensive model with higher computational complexity and neglecting the recovery process with the interdiction model.

1. Introduction

The occurrence of large-scale disruptions to critical infrastructure networks (e.g., electric power, water supply, transportation) have revealed how these systems are routinely under a host of threats, from natural disasters to malevolent attacks to operational failure (Directive, 2003). In addition, infrastructure networks are not the only networks that exist. Disruptions to infrastructure networks can impact a variety of other networks, including, in particular, the community networks and service networks that interact with and depend on infrastructure networks to function properly. Disruptions can be made worse when multiple networks depend on each other (Chang, McDaniels, Mikawoz, & Peterson, 2007; Mendonça & Wallace, 2006; Nurre, Cavdaroglu, Mitchell, Sharkey, & Wallace, 2012; Rourke, 2006; Wallace, Mendonça, Lee, & Mitchell, 2001). As such, there exists a continued interest in critical infrastructure reliability and sustainability problems. Where previous work in planning for disruptions to critical infrastructure networks emphasized prevention and protection, such planning now more broadly captures the ability of infrastructure networks to withstand a disruption and recovery timely from it. The ability of a system to

[*] Corresponding author at: 202 W. Boyd St., Rm. 124, Norman, OK 73019, USA.
E-mail address: kashbarker@ou.edu (K. Barker).

https://doi.org/10.1016/j.cie.2020.107085
Received 31 July 2020; Received in revised form 17 November 2020; Accepted 21 December 2020

withstand a disruption, adapt to, and recover from it is generally referred to as *resilience* (Aven, 2011; Ayyub, 2014; Haimes, 2009; Hosseini, Barker, & Ramirez-Marquez, 2016). With this definition, resilience is quantified with two primary measures (i) *vulnerability*: the drop in the system performance following a disruptive event, and (ii) *recoverability*: the restoration speed of the disrupted system to the desired performance level. In any networked system, the occurrence of a disruptive event (i. e., disconnection of nodes, links, or both) due to a failure or a malevolent action could affect the performance of the system. Fig. 1 (Barker, Ramirez-Marquez, & Rocco, 2013) depicts system performance, $\varphi(t)$, before and after a disruption, underlining *vulnerability* and *recoverability* as two critical planning dimensions of resilience.

Prior studies have addressed (i) vulnerability optimization models for protecting network components such that the effect of a disruption are mitigated (McCarter, Barker, Johansson, & Ramirez-Marquez, 2018; Ramirez-Marquez, Rocco, & Barker, 2017), and (ii) recovery optimization models for determining both optimal recovery strategies and crew assignment to different recovery tasks (e.g., Almoghathawi, Barker, & Albert, 2019; Gomez, González, Baroud, & Bedoya-Motta, 2019; González, Dueñas-Osorio, Medaglia, & Sánchez-Silva, 2016; González, Dueñas-Osorio, Sánchez-Silva, & Medaglia, 2016; Morshedlou, González, & Barker, 2018; Nurre et al., 2012; Sharkey et al., 2015). However, resilience is thought of as the combination of reducing vulnerability and enhancing recoverability. And there exist a few research studies assessed the system resilience by simultaneously considering pre-disruption and post-disruption resource allocation for the system of interdependent networks. For example, Ghorbani-Renani, González, Barker, and Morshedlou (2020) addressed this by proposing a study of resilience interdiction, developing a tri-level protection-interdiction-restoration model that considers (i) a protection level to make decisions to minimize network vulnerability, (ii) an interdiction level to identify and pursue the most effective disruptions, and (iii) a restoration level to recover the network after the. This resilience interdiction model, which falls into the class of defender-attacker-defender (DAD) models, can be used to simultaneously determine (i) the optimal resource allocation to fortify the network components, (ii) a set of most critical elements through the system, and (iii) the optimal work crew assignment to rapidly recover the disrupted system.

However, the proposed DAD model is computationally challenging to solve. To address this issue, in this study we design a new decomposition-based solution algorithm as a general framework to optimally solve tri-level DAD models more efficiently. The proposed solution technique is demonstrated with an existing resilience interdiction model developed by Ghorbani-Renani et al. (2020), with which we compare the efficiency of the proposed algorithm with the existing exact solution method (covering decomposition method). However, due to the general features of the tri-level DAD models, the computational complexity of the algorithm grows exponentially in large-sized problems. Along with other factors (e.g., the complexity of the formulation itself), the run time of the DAD models are highly sensitive to the number of candidate components that can be interdicted and protected. To deal with this issue, we generate different sets of candidate components based on different centrality measures for disruption and protection. To derive these sets such that they represent a variety of different components, we apply an agglomerative hierarchical clustering technique. In addition, we compare and analyze the results of the existing resilience interdiction model (referring to Ghorbani-Renani et al. (2020)) with the protection-interdiction-counteraction model in which the restoration level is not considered. Note that terms related to the disruptive agent such as attacker and interdictor are used interchangeably through this paper but could otherwise represent a worst-case natural disaster or failure (Smith & Lim, 2008). Likewise, both labels of protector and defender refer to the defending agent.

In summary, the main contribution of this study is to develop a novel solution algorithm as a general framework to optimally solve a wide variety of interdiction models (particularly DAD optimization). The proposed solution approach is based on iteratively solving two bi-level formulations derived from the original tri-level DAD model. The proposed approach substantially outperforms the existing exact solution technique, the covering decomposition method, with regard to computational complexity. We propose an efficient clustering technique for identifying the set of critical components in the network and apply it on the system of interdependent infrastructure networks in Shelby County, TN as the case study. Furthermore, we analyze a new tri-level DAD formulation in which the restoration of interdicted (disrupted) components is not considered in the subsequent defender, and we compare the results with the existing resilience interdiction model proposed by Ghorbani-Renani et al. (2020).

The rest of the paper is structured as follows. In Section 2, a literature review on interdiction models is performed. In Section 3, the general framework of the tri-level formulation developed by Ghorbani-Renani et al. (2020) is discussed in detail. Then, the proposed solution approach for solving the DAD models is represented. An illustrative example is provided in Section 4, based on the system of interdependent infrastructure networks in Shelby County, TN. We applied the proposed solution technique to the existing interdiction model developed by Ghorbani-Renani et al. (2020) and performed a comparative analysis with respect to the previously published solution method (covering decomposition method). Additionally, we introduce an updated tri-level protection-interdiction-counteraction formulation to assess the

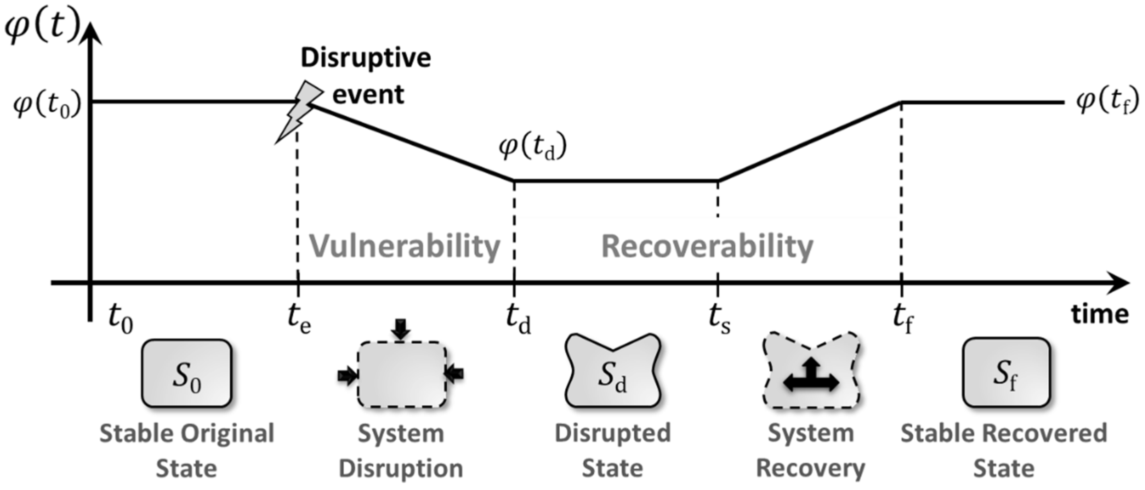


Fig. 1. System performance trajectory, $\varphi(t)$, following a disruptive event, adapted from Barker et al. (2013).

resilience of the system under two DAD models, for which the proposed solution technique is also used. Finally, Section 5 provides concluding remarks and future work.

2. Previous work on interdiction models

Network-based systems widely appear in different service, community, industrial, and economic systems such as electric power, water supply, transportation, and telecommunication networks. Due to the significant role of such systems in society, it is essential to have an effective plan to enhance the resilience of infrastructure networks against disruption (e.g., natural disasters, malevolent attacks, or operational failures) (Nurre et al., 2012; Sadeghi, Seifi, & Azizi, 2017).

The area of network interdiction has received attention for several decades because of its widespread applications in different domains. Table 1 provides a brief (and non-exhaustive) summary of previous research work on different applications of interdiction models. Stackelberg (1952) formulated the basic interdiction problem as a Stackelberg game implying a sequential game between two opposing forces known as (i) the defender and (ii) the attacker, who are in a warlike conflict (Motto, Arroyo, & Galiana, 2005; Salmeron et al., 2004, 2009). Broadly, a Stackelberg game describes situations where the defender attempts to maintain some level of the network performance (e.g., maximizing flow, meeting demand at minimum cost, finding the shortest path) and an intelligent attacker, on the other hand, invests some amount of resources to disrupt or interdict the network (e.g., impeding some links, reducing the network capacity, increasing the traversing time and cost) (Altner et al., 2010; Fulkerson & Harding, 1977; Wollmer, 1964). Generally, such a formulation tends to be bi-level problem, considering attacker and defender actions in the form of max-min or min-max problems, which are referred to as attacker-defender (AD) models in the literature (Israeli & Wood, 2002).

Wollmer (1964) originally applied the interdiction model to a network flow problem by removing links in which the maximum flow between source and sink nodes is minimized. Thereafter, Israeli and Wood (2002) applied the network interdiction problem to maximize the shortest path between source and sink nodes in a directed network with a given interdiction resource. Rad and Kakhki (2013) studied a dynamic version of the network flow interdiction problem where the defender maximizes the flow throughout the network in a certain time period, and an attacker, on the other hand, removes links to minimize the maximum flow within the same period. Salmeron, Wood, and Baldick (2004) developed power grid interdiction model through the bi-level mathematical formulation to identify critical system components with given interdiction budget in which the outage of these components would result in the maximum disruption to the system. Later, the AD model was extended to defender-attacker-defender (DAD) model incorporating one more operator action to determine the best pre-disruption defensive strategy against the attacker's decision (Alderson, Brown, Carlyle, & Wood, 2011; Brown, Carlyle, & Wood, 2008). In this new model, the first defender represents the system planner seeking to determine the best protection plan against the most destructive attacker decision. By introducing an additional level of interaction between the defender and the attacker, the DAD model outperforms the AD formulation since the system planner is able to (i) select the best protection strategy and (ii) assess pre-disruption strategies by altering the defensive budget (Alguacil et al., 2014; Brown, Carlyle, Salmerón, & Wood, 2006; Yao, Edmunds, Papageorgiou, & Alvarez, 2007; Yuan et al., 2016). Recently, interdiction models have begun to address both vulnerability reduction and recoverability enhancement to prepare for and react to an adversarial attack. Few works have incorporated the recovery process of damaged components into a DAD formulation. For example, Ouyang and Fang (2017) considered the repair planning of disrupted components with given recovery resources in a DAD model. Prior works generally considered the recovery duration of disrupted components as parameters in the restoration process (Almoghathawi et al., 2019; Nurre et al., 2012; Ouyang & Fang, 2017). However, in the resilience interdiction model proposed by Ghorbani-Renani et al. (2020), the time required to repair the damaged components is not fixed and depends on (i) the performance rate of the work crew, and (ii) the proportion of the disruption (in the case of partial disruption). In addition, restoration decision variables are time-indexed representing the schedule of work crews through the recovery process.

Table 1
Summary of different applications of interdiction model.

Research work	Application
Ghare, Montgomery, and Turner (1971), McMasters and Mustin (1970), Pan, Charlton, and Morton (2003), and Patterson and Apostolakis (2007)	Defense and military applications
Alguacil, Delgadillo, and Arroyo (2014), Davarikia and Barati (2018), Lai, Illindala, and Subramaniam (2019), Lin and Bie (2018), Salmeron et al. (2004, 2009), Wu and Conejo (2017), Yao et al. (2007), and Yuan et al. (2014)	Power network vulnerability
Alderson et al. (2011), Brown et al. (2006), Ouyang (2017), and Ouyang and Fang (2017)	Critical infrastructure network resilience
Fathollahi-Fard, Hajiaghaei-Keshteli, and Mirjalili (2018) and Fathollahi Fard and Hajiaghaei-Keshteli (2018)	Supply chain resilience
Akbari-Jafarabadia, Tavakkoli-Moghaddam, Mahmoodjanloo, and Rahimi (2016,Akbari-Jafarabadi et al., 2017), Liberatore, Scaparra, and Daskin (2011), Losada, Scaparra, and O'Hanley (2012), and Mohammad, Fard, and Hajiaghaei-keshteli (2018)	Facility location problem
Baycik, Sharkey, and Rainwater (2018) and Nandi, Medal, and Vadlamani (2016)	Cyber security
Brown, Carlyle, Harney, Skroch, and Wood (2009)	Project management
Borndörfer, Sagnol, and Schwartz (2016)	Toll control

Interdiction models or broadly multi-level problems are challenging to solve. Therefore, considering the widespread applications of such models, the development of efficient solution methods has received attention in recent years. In this paper, we study the existing interdiction model developed by Ghorbani-Renani et al. (2020) and solve it to optimality by a new decomposition-based solution approach such that the final solution is found by iteratively solving two bi-level formulations derived from the original tri-level model. In addition, to deal with the complexity of the model and the difficulty of considering all components as possibilities for interdiction and protection, different sets of candidate components are generated based on different topological characteristics. The results are discussed for each set of candidate nodes.

3. Decomposition-based solution approach

For the illustrative purposes, the proposed solution technique is demonstrated with the existing resilience interdiction model proposed by Ghorbani-Renani et al. (2020), namely a tri-level protection-interdiction-restoration model, denoted by M-I. As such, we briefly introduce a generalized depiction of M-I. Then, the proposed decomposition-based solution approach is discussed in detail to solve M-I to optimality.

3.1. *Tri-level formulation: protection-interdiction-restoration model (M-I)*

Ghorbani-Renani et al. (2020) studied the resilience control (enhancement) of interdependent infrastructure networks (e.g., electric power, water supply, transportation) against adversaries using an interdiction model. This problem was formulated as a tri-level DAD formulation with a corresponding hierarchy of decisions, referred to as a protection-interdiction-restoration model. This model includes a series of nested optimization formulations controlled by a set of constraints and decision variables in which the decision made at the top level affect the decisions of other levels. The proposed resilience interdiction model (M-I) aims to optimize the restoration of a system of interdependent networks by minimizing the cumulative unmet demand over time by sequentially performing three levels, as depicted in Fig. 2: (i) the protection level to make the initial investment to minimize system vulnerability (i.e., initial drop in the system performance), (ii) the interdiction level to identify the most effective disruption, and (iii) the restoration level to recover the system after the disruption. The first level, or the protection level, allocates resources (how much and where?) to harden the networks to minimize system vulnerability prior to a disruption. As the defense strategy, protection is accomplished by increasing the capacity of the network component or adding redundancy to it. Through the second level, an intelligent attacker, who has complete information about the network, intentionally interdicts the system. The interdiction level, therefore, allocates resources to maximize the effects of the disruption. This level does not necessarily require a human "attacker" and could represent a worst-case natural disaster. Note that the disruption (interdiction) takes the form of a reduction in the capacity of the network components (either nodes or links). Finally, the network flow problem and repair sequence of interdicted components is provided in the third level, or the restoration level. The third level minimizes the long-term effect after the disruption through network component recovery. The important parameter in the third level is the time to achieve the total system recovery. The definition of the model sets, parameters, and decision variables of the first and second levels of M-I are represented subsequently.

M-I deals with a system of interdependent networks defined by a set of nodes connected with a set of links. In M-I, it is assumed that each network is responsible for providing a specific type of service (a single commodity) across the network and satisfies the demand nodes of the network (e.g., gas network provides gas service, water supply provides water requirements). M-I assumes that infrastructure networks follow the general network flow problem. To briefly describe the general formulation of M-I, assume a set K of infrastructure networks. Network $k \in K$ is represented by $G^k = \left(N^k, A^k\right)$, where N^k is the set of nodes indexed by $i \in N^k$, and A^k is the set of links indexed by $(i,j) \in A^k$ that connect nodes. Nodes can be supply nodes $(N_+^k \subseteq N^k)$, demand nodes $(N_-^k \subseteq N^k)$, and transshipment nodes $(N_0^k \subseteq N^k \backslash \{N_+^k, N_-^k\})$ such that $N_+^k \cap N_-^k = \varnothing$. Let S_i^k and d_i^k denote amount of supply and demand in nodes $i \in N_+^k$ and $i \in N_-^k$, respectively. Sets $N'^k \subseteq N^k$ and $A'^k \subseteq A^k$ are candidate nodes and links, respectively, in network $k \in K$, that can be disrupted or protected in the system of interdependent networks. For every node $i \in N'^k$, binary variables y_i^k and z_i^k represent the first defender and attacker actions, respectively. Likewise, binary variables y_{ij}^k and z_{ij}^k represent the first defender and attacker actions for every link $(i,j) \in A'^k$. There are known cardinality budgets available for protecting and for disrupting the components denoted by parameters B_P and B_I, respectively, suggesting that the protector could protect up to B_P components and the attacker could interdict up to B_I components in the network. Also, binary variables F_i^k and F_{ij}^k show the functionality status for every node $i \in N'^k$ and link $(i,j) \in A'^k$, respectively. There is a known flow capacity for every link $(i,j) \in A^k$ represented by u_{ij}^k and decision variable x_{ij}^k shows flow through the associated link. Parameters $\eta_{it_e}^k$ represent the demand should be met at every node $i \in N_-^k$, where decision variables η_i^k denote actual demand being met at node $i \in N_-^k$. Index $t \in T$ provides the set of available time periods. The time unit (interval) of the model is adjusted by the decision maker. Accordingly, the time horizon of model is set based on the time unit (interval) selected. For example, if the time interval is considered to be one working shift, the time horizon of the model could be set to $T = \{1\}$, $T = \{1, 2, \cdots, 5\}$, and $T = \{1, 2, \cdots, 23\}$ for one work day, one work week, and one work month, respectively. Since time is considered to be discrete in M-I, the required time units for restoring the disrupted components are rounded up to the nearest integer value for the work crew assignment as represented by constraints (A24), (A25), (A27), and (A28) in the appendix. Clearly, the smaller (more granular) the time interval that is selected, the higher the resulting resolution. However, as the time interval becomes smaller, the computational complexity of the algorithm grows. Demand nodes can be ranked with the aim of emphasizing on their importance in a network. Therefore, parameters w_{it}^k show the weight of demand node $i \in N_-^k$ at time $t \in T$, which can be adjusted based on different aspects including locations of the demand nodes (e.g., near hospitals, shelters, and populated or more vulnerable areas). M-I accounts for the physical interdependency of networks where the functionality of a set of nodes in one or more networks enable the functionality of a node in another network due to linkages. Ψ represents interdependency set among networks such that $\left((i,k), \left(\bar{i}, \bar{k}\right)\right) \in \Psi$ denotes node $i \in N^k$ in network $k \in K$ physically depends on node $\bar{i} \in N^{\bar{k}}$ in network $\bar{k} \in K$ to be operational, where $N^k \cap N^{\bar{k}} = \varnothing$, $A^k \cap A^{\bar{k}} = \varnothing$ and $\forall k, \bar{k} \in K : k \neq \bar{k}$.

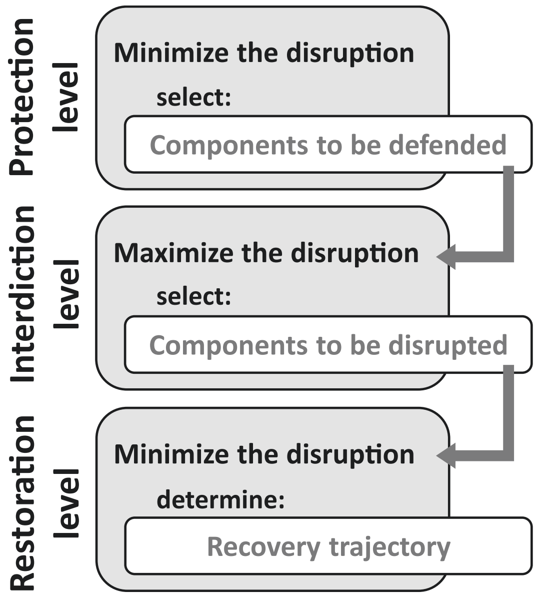


Fig. 2. Tri-level protection-interdiction-restoration process.

To demonstrate various steps of the proposed solution algorithm, we represent an abstract form of M-I as shown by Eqs. (1)–(11). The tri-level DAD model (M-I) aims to deliver the cumulative weighted fraction of unmet demand over the planning horizon, such that this value is minimized by the first defender, maximized by the attacker, and minimized by the subsequent defender, as shown in Eqs. (1) and (2). Constraints (3) and (4) represent the budget restrictions for the first defender and attacker decisions, respectively. Constraints (5)–(8) show the nature of the decision variables for the first and second levels of M-I. Constraints (9) and (10) deliver the functionality status of every node and link, respectively. Set of constraints (11) corresponds to the recovery process in M-I to plan the restoration of disrupted components in which to return the system of networks to a stable operation as rapidly as possible. For more details of this set of constraints, we refer the reader to the appendix, which includes the complete definition of the model parameters and decision variables, as well as the complete form of M-I. Note that although parameter M in constraints (A23), (A26), (A29), (A30), (A34), and (A35) represents a big number, it need be only greater than the maximum required time for restoring the disrupted components.

$$\zeta_{\mathrm{M-I}}(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it}^k}{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it_e}^k} \right) \quad \forall t \in T \tag{1}$$

$$\xi_{\mathrm{M-I}} = \min_{y} \max_{z} \min_{\eta, x, F, \alpha, \beta} \sum_{t \in T} \zeta_{\mathrm{M-I}}(t) \tag{2}$$

$$\sum_{k\in K}\sum_{i\in N'^{k}} y_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} y_{ij}^k \leq B_P \tag{3}$$

$$\sum_{k\in K}\sum_{i\in N'^{k}} z_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} z_{ij}^k \leq B_I \tag{4}$$

$$y_i^k \in \{0,1\} \quad \forall k\in K, \forall i \in N'^{k} \tag{5}$$

$$y_{ij}^k \in \{0,1\} \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{6}$$

$$z_i^k \in \{0,1\} \quad \forall k\in K, \forall i \in N'^{k} \tag{7}$$

$$z_{ij}^k \in \{0,1\} \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{8}$$

$$1 + y_i^k - z_i^k \geq F_i^k \quad \forall k\in K, \forall i \in N'^{k} \tag{9}$$

$$1 + y_{ij}^k - z_{ij}^k \geq F_{ij}^k \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{10}$$

$$\text{Constraints}(\text{A11}) - (\text{A44}) \tag{11}$$

The tri-level formulation is an extension of the bi-level model comprising one more operator/defender action. This type of model, or broadly multi-level problems, are nonconvex. Even in their simplest form, they are challenging to solve (Bard, 1991; Hansen, Jaumard, & Savard, 1992; Wood, 1993). Solution methods developed to solve such complex problems can be categorized into reformulation and duality (Alguacil et al., 2014; Saharidis, Conejo, & Kozanidis, 2013), decomposition (Yao et al., 2007; Yuan, Zhao, & Zeng, 2014), and heuristic-based approaches (Bier, Gratz, Haphuriwat, Magua, & Wierzbicki, 2007; Salmeron et al., 2004). Typically, exact solution methods for solving multi-level models have various limitations from the modeling point of view to computational complexity. In this regard, hybrid algorithms incorporating exact solution algorithm and metaheuristics method have been designed to cope with challenges related to multi-level models (Akbari-Jafarabadi, Tavakkoli-Moghaddam, Mahmoodjanloo, & Rahimi, 2017). For example, Mahmoodjanloo, Parvasi, and Ramezanian (2016) developed a hybrid solution approach consisting of the genetic algorithm and enumeration method to solve the proposed facility interdiction model. Other metaheuristic approaches have been also applied to tackle multi-level models such as simulated annealing (Parvasi et al., 2017) and tabu search (Aksen & Aras, 2012).

In this study, we designed a new exact solution algorithm, based on decomposing the original tri-level model into two bi-level formulations, namely (i) the master problem, and (ii) the subproblem, which provide the lower and upper bounds for the model, respectively. Fig. 3 shows the general framework of decomposing the tri-level protection-interdiction-restoration formulation, denoted by M-I, into the master problem and subproblem. By iteratively solving the two constructed problems, the gap between two bounds is reduced until the final solution is found. The details of constructing two bi-level problems are described subsequently.

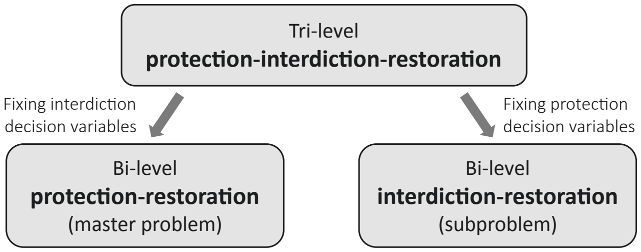

Tri-level
protection-interdiction-restoration
Fixing interdiction decision variables
Fixing protection decision variables
Bi-level
protection-restoration
(master problem)
Bi-level
interdiction-restoration
(subproblem)

Fig. 3. Decomposition framework of the tri-level resilience interdiction model.

3.2. Master problem

As depicted in Fig. 3, the master-problem is constructed by fixing the attacker decision variables in the original model, $z \leftarrow \widehat{z}$, where z is the attacker decision. As such, the tri-level DAD model is transformed to the bi-level min-min formulation as represented in constraints (12)–(18). By solving the mater problem, the protection plan is determined, $y \leftarrow \widehat{y}$, which will be the input of the subproblem (likewise, y is the protector decision). Since the master problem is a relaxed problem in comparison with the original formulation, it provides a lower bound value for the model.

$$\min_{y} \min_{\eta,x,F,\alpha,\beta} \sum_{t\in T} \zeta_{\mathrm{M-I}}(t) \tag{12}$$

$$\sum_{k\in K}\sum_{i\in N'^{k}} y_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} y_{ij}^k \leq B_P \tag{13}$$

$$y_i^k \in \{0,1\} \quad \forall k\in K, \forall i \in N'^{k} \tag{14}$$

$$y_{ij}^k \in \{0,1\} \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{15}$$

$$1 + y_i^k - \widehat{z}_i^k \geq F_i^k \quad \forall k\in K, \forall i \in N'^{k} \tag{16}$$

$$1 + y_{ij}^k - \widehat{z}_{ij}^k \geq F_{ij}^k \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{17}$$

$$\text{Constraints}(\text{A11}) - (\text{A44}) \tag{18}$$

Theorem 1. *The master problem provides a valid lower bound for the tri-level model (M-I).*

Proof. By fixing the attacker decision variables ($\widehat{z}$) through the original model, the master problem, which is a relaxed problem in comparison with the original tri-level DAD formulation, is constructed. Since (i) the attacker aims to maximize the model and (ii) only a subset of all possible attacker plans are considered, the master problem provides a valid lower bound value for the entire tri-level DAD model.

3.3. Subproblem

On the other hand, by fixing the protector decision variables found through the master problem, $y \leftarrow \widehat{y}$, the subproblem is constructed as the bi-level max-min formulation including attacker and second defender (restoration) levels as represent in constraints (19)–(25). Note that the subproblem is also a relaxed problem, and it provides an upper bound value for the model. By solving the subproblem, the interdiction plan is determined, $z \leftarrow \widehat{z}$, which will be the input of the master problem.

$$\max_{z} \min_{\eta,x,F,\alpha,\beta} \sum_{t\in T} \zeta_{M-I}(t) \tag{19}$$

$$\sum_{k\in K}\sum_{i\in N'^{k}} z_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} z_{ij}^k \leq B_I \tag{20}$$

$$z_i^k \in \{0,1\} \quad \forall k\in K, \forall i \in N'^{k} \tag{21}$$

$$z_{ij}^k \in \{0,1\} \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{22}$$

$$1 + \widehat{y}_i^k - z_i^k \geq F_i^k \quad \forall k\in K, \forall i \in N'^{k} \tag{23}$$

$$1 + \widehat{y}_{ij}^k - z_{ij}^k \geq F_{ij}^k \quad \forall k\in K, \forall (i,j) \in A'^{k} \tag{24}$$

$$\text{Constraints}(\text{A11}) - (\text{A44}) \tag{25}$$

Theorem 2. *The subproblem provides a valid upper bound for the tri-level*

DAD model (*M-I*).

Proof. By fixing the protector decision variables ($\hat{y}$) through the original model, the subproblem, which is a relaxed problem in comparison with the original tri-level DAD formulation, is constructed. Since (i) the protector aims to minimize the model and (ii) only a subset of all possible protector plans are considered, the subproblem provides a valid upper bound value for the entire tri-level DAD model.

3.4. Decomposition approach

Note that both master problem and subproblem are bi-level formulations that often cannot be solved directly with available optimization solvers. Therefore, further manipulations are required to make them generic optimization models (e.g., single level optimization formulations). As such, we integrate Benders decomposition with set-covering decomposition to tackle the master problem and subproblem, respectively, such that the bi-level min-min model generated through the master problem can be transformed to a single minimization formulation by implementing Benders decomposition method, which can be solvable directly using available optimization solvers. To implement Benders decomposition method, we define a set of attack plans that are indexed by the algorithm iteration. Subsequently, the new set of decision variables for the given attacker decision indexed by iteration and their corresponding constraints are added to master problem at every iteration. For more information about implementing Benders decomposition, we refer the reader to Yuan et al. (2014) and Zeng and Zhao (2013).

By solving the master problem, the best solution for the defender decision variables (y) are found which will be the input for the subproblem. Since the attacker decision variables are binary in this formulation, the subproblem (the bi-level max-min formulation) can be solved using the set-covering decomposition approach (Israeli & Wood, 2002), delivering the best attacker decision (z). Note that converting the two levels of the subproblem into a single level by taking the dual of the inner level is not applicable to this formulation since the restoration level is a mixed integer problem and Karush-Kuhn-Tucker optimality conditions are not satisfied in this situation (Israeli & Wood, 2002; Wood, 1993). In addition, the covering decomposition algorithm, which tackles both the master problem and subproblem using the set-covering decomposition approach, is not efficient enough since it is significantly time-consuming (Yuan et al., 2014). To implement the set-covering approach for solving the subproblem, an inequality is added to the second level of the interdiction model, which is a feasibility seeking problem. This inequality forces the attacker to find at least one component to be interdicted while subject to the available budget. Note that the generated inequality at each iteration is distinct from the previous inequalities. Therefore, due to the budget restriction for the attacker, at one iteration, the interdiction model cannot satisfy all inequalities added to the model, and it becomes infeasible. The set covering algorithm is then terminated with the optimal attack plan which serves as the input to Benders decomposition algorithm. Since the interdictor tends to maximize the objective value, the amount of disruption imposed to the system, at each iteration of set covering algorithm, the best solution is recorded by comparing the objective value of the restoration level. Note that at this level, both protection and interdiction decision variables are known, so the restoration level can be solved directly since it is a single level optimization model. For more information about implementing the set-covering algorithm, we refer the reader to Israeli and Wood (2002).

The proposed solution algorithm finds the optimal solution in a finite number of iterations, as at each iteration the subproblem introduces an effective (optimal) attacker plan associated with a given protection scenario, while the master problem keeps expanding with the corresponding new attack scenarios and finds the best (optimal) associated protection plan. Since the number of components that can be attacked is limited, attack scenarios satisfying the attacker budget are finite. Similarly, the protection budget and the number of components that can be protected are limited. By iteratively generating a new set of variables and constraints and solving the updated master problem, eventually the upper and lower bound values converge, and the optimal solution is obtained. Additional details on the proof of convergence for iterative algorithms of this nature can be found in Zeng and Zhao (2013). Fig. 4 represents the general framework of the proposed solution algorithm.

Based on the above discussion for solving the master problem and subproblem, the pseudocode representing the implementation steps of the solution algorithm is provided in Table 2. Note that ε is the solution gap set by the decision maker as the stopping criterion of the algorithm. LB, UB, obj_{MP}, and obj_{SP} refer to the lower bound, upper bound, master problem (MP), and subproblem (SP) objective values, respectively. RL refers to the restoration level, where its corresponding objective value is represented by obj_{RL}, and IL represents the interdiction level, which is a feasibility seeking problem in this algorithm. At each iteration of algorithm, the attacker plan is distinguished from previous plans as it is indexed by the iteration index represented by c (e.g., $\widehat{z}^{c}$) and fed into master problem. Note that the master problem is updated at each iteration by receiving the new set of attacker decisions generated by the subproblem. Mentioned previously, the interdictor tends to find the most destructive plan by considering the current protection decision. Therefore $P\_^{c}$ is responsible for keeping the best interdictor solution in its record by comparing obj_{RL} with the previous best objective value (referring to steps 13 and 14). Finally, y^{*} and z^{*} denote the best protection and interdiction decisions, respectively. Note that the algorithm is initialized by the preliminary feasible solution $z \leftarrow 0$, meaning that no components are interdicted at this step.

To deal with the computational complexity of the proposed tri-level protection-interdiction-restoration model (M-I), we proposed a decomposition-based solution algorithm to optimally solve it more efficiently. However, due to the features of the model, the computational complexity of the algorithm grows exponentially for large-sized problems. Along with other factors (e.g., the complexity of the formulation itself), the run time of the proposed model is highly sensitive to the number of candidate components that can be interdicted and protected. By increasing the number of candidate components, possible combinations for interdiction and protection grow exponentially, which results in increasing computational complexity. To deal with this issue, we generate different sets of candidate components based on different centrality measures for disruption and protection However, generated sets most likely include numerous similar components. To derive sets such that they represent a variety of different components, we apply an agglomerative hierarchical clustering technique (Murtagh, 1983; Murtagh & Contreras, 2011). To implement this clustering method, a proximity matrix, which represents the distances between each point, is

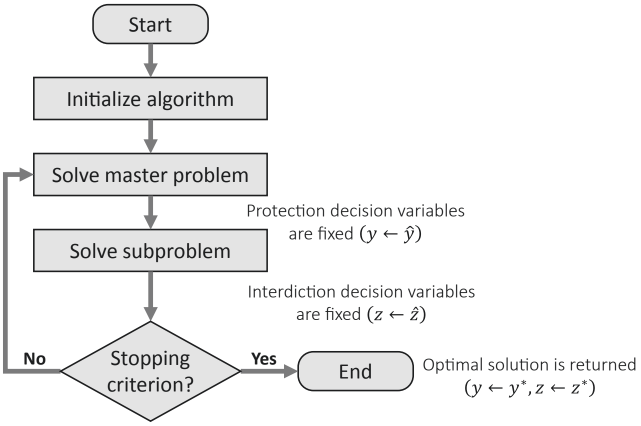

Start
Initialize algorithm
Solve master problem
Protection decision variables are fixed ($y \leftarrow \hat{y}$)
Solve subproblem
Interdiction decision variables are fixed ($z \leftarrow \hat{z}$)
Stopping criterion?
No
Yes
End
Optimal solution is returned ($y \leftarrow y^{*}, z \leftarrow z^{*}$)

Fig. 4. The general framework of the proposed solution algorithm.

Table 2
The pseudocode of implementation steps of the solution algorithm.

```
Step 1   Initialization: $LB \leftarrow -\infty$, $UB \leftarrow +\infty$, and $\hat{z}^c \leftarrow 0$, $\underline{P}^c \leftarrow -\infty$ in $c \leftarrow 0$
Step 2   While $\frac{UB-LB}{LB} > \varepsilon$ do:
Step 3       Solve MP and obtain its value $obj_{MP}$ and protection decision $\hat{y}$
Step 4       $\hat{y}^* \leftarrow \hat{y}$, $LB \leftarrow obj_{MP}$, $c \leftarrow c+1$
Step 5       If attacker budget is enough to interdict all components $(N'^k \cup A'^k)$ then:
Step 6           $\hat{z}^c \leftarrow 1$
Step 7           Solve RL for objective value $obj_{RL}$
Step 8           $\underline{P}^c \leftarrow obj_{RL}$ and go to Step 15
Step 9       While IL is feasible do:
Step 10          Add the following inequality to IL:
                 $\sum_{k\in K}\sum_{i\in N'^k|z_i^k=0} z_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^k|z_{ij}^k=0} z_{ij}^k \geq 1$
Step 11          Solve IL, obtain interdiction decision $\hat{z}$
Step 12          Solve RL and obtain its value $obj_{RL}$
Step 13          If $obj_{RL} > \underline{P}^c$ then:
Step 14              $\hat{z}^c \leftarrow \hat{z}$ , $\underline{P}^c \leftarrow obj_{RL}$
Step 15      $obj_{SP} \leftarrow \underline{P}^c$
Step 16      $UB \leftarrow \min\{UB, obj_{SP}\}$
Step 17      Return $\hat{z}^c$
Step 18      Update MP by creating a new set of decision variables and constraints
Step 19  $z^* \leftarrow \hat{z}^c$
Step 20  Return $y^*$, $z^*$ (optimal solutions with objective value $obj_{SP}$)
```

required. At the beginning, each set is assigned to an individual cluster. Then, the closest pair of clusters are merged, and this step is repeated until only one cluster remains. Since the clusters are merged at each step, this type of clustering is also known as additive hierarchical clustering.

4. Experimental results

To study the efficient solvability of the proposed solution algorithm, we apply this formulation to the interdependent system of water, gas, and power networks in Shelby County, TN, USA, where a set of nodes in the water network depends on the power network to be functional and the power network is dependent on the water network for cooling and emission control. This system of interdependent networks includes 125 nodes and 164 links as depicted in Fig. 5 for each network separately (González, Dueñas-Osorio, & Sánchez-Silva, et al., 2016). Note that descriptions of the test network are adapted from Hernandez-Fajardo and Dueñas-Osorio (2011) and Song and Ok (2010), which offer a more in-depth discussion of their interconnectedness.

We implemented the solution algorithm in Python 3.6.5 with the Gurobi optimizer 8.0.1 for the optimization problem. Computational results were conducted on a 64-bit operating system, Intel® Core™ i7-6700 CPU @ 3.40 GHz 3.41 GHz desktop computer. Note that the convergence ratio of upper bound and lower bound (e.g., the stopping criterion of the algorithm) is set to 0.01, e.g., $\varepsilon = 0.01$.

4.1. Model parameters

The importance weight w_{it}^k can be adjusted by decision makers to prioritize the demand satisfaction in some nodes relative to others at time t. This prioritization affects the restoration process of the disrupted network by forcing the model to satisfy the demand in high-ranked nodes prior to others (e.g., hospitals, populated areas, or vulnerable communities might have priority to other nodes in a network). In this study, since we aim to analyze the results derived from different sets of candidate nodes, equal weights are assigned to the demand nodes. We consider equal value for the restoration rate of the components. Note that these parameters can vary by the network as they are indexed by k. In this study, the restoration rate for each component is assumed similar regardless of the type of work crews available at each network. However, the restoration rates, λ_i^k and λ_{ij}^k, can be also indexed by the type of work crews available at each network. In this case study, we assume that the time interval is one working shift which includes 8 h, and the time horizon of the model is chosen to be one working month defined as 23 working shifts, $T = \{1, 2, \cdots, 23\}$. Different scenarios account for the resource available for protector and interdictor (B_P and B_I) as discussed in the computational results section.

4.2. Set of components subject to protection or interdiction

For the experimental purposes, we assume that nodes are the only components that can be either protected or disrupted. To define the

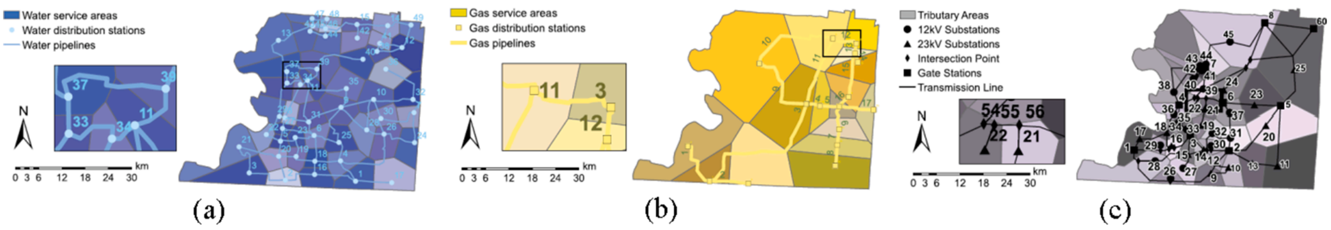


Fig. 5. Graphical illustration of the (a) water, (b) gas, and (c) power networks (adapted from González et al., 2016b)).

critical nodes subject to protection and disruption, an efficient clustering technique is applied in this case study which results in generating three sets of candidate nodes based on three centrality measures. The details of deriving the set of critical nodes (i.e., candidate nodes subject to protection or disruption) are described subsequently.

To generate different sets of candidate nodes subject to protection or disruption, $N^{\prime k}$, we explore five main centrality measures to rank nodes based on these measures separately: Degree, Betweenness, Closeness, Katz, PageRank, and Load centralities (Newman, 2018). Note that the interdependency relationships among networks (e.g., water, gas, power networks) are considered as links, so the three networks are merged and viewed as a single system for calculating above mentioned centrality measures. To choose sets of candidate nodes including the most different nodes in compared to other sets, we assess the proportion of similar nodes delivered by each centrality measure, as shown in Table 3. Note that for each set, we select the top high-ranked 15 nodes based on their ranking provided by every centrality measure, accounting for 25% of the total number of nodes.

To select sets of candidate nodes that generate sufficient differences in the makeup of those candidate sets, we apply an agglomerative hierarchical clustering technique (Murtagh, 1983; Murtagh & Contreras, 2011). To apply this clustering method, a proximity matrix, which represents the distances between each point, is found, as shown in Table 4.

At the beginning, we assign each set to an individual cluster. Then, we merge the closest pair of clusters and repeat this step until only one cluster remains. Since we merge the clusters at each step, this type of clustering is also known as additive hierarchical clustering. Fig. 6 shows the dendrogram representing different clusters of candidate nodes based on the proximity matrix. The dashed horizontal line in Fig. 6 represents the threshold distance of 0.5 chosen for this problem. Three clusters result: one that represents the sets from Katz, Degree, and PageRank, a second that contains the set found from Closeness centrality, and a third representing sets from Load and Betweenness. From the first and third clusters, PageRank and Load centrality measures are selected since they are at the center of their corresponding clusters.

Therefore, Closeness, PageRank, and Load centrality measures are selected as they generate sufficiently differences in the makeup of those candidate sets. With regard to these selected sets built upon three centrality measures, (i) Closeness centrality indicates how close a node is to all other nodes in the network (Golbeck, 2013), (ii) PageRank centrality measures the transitive influence or connectivity of a node in a network (Needham & Hodler, 2019), and (iii) the Load centrality of a node is the fraction of all shortest paths that pass through that node (Goh, Kahng, & Kim, 2001).

Fig. 7 shows the map and topology of the interdependent system of water, gas, and power networks in Shelby County, TN, where the notation w, g, and p refer to water, gas, and power networks, respectively. Note that the dashed lines in Fig. 7b represent the interdependency relationship between water and power networks in this case study.

4.3. Computational results of M-I

In this subsection, we demonstrate the efficiency of the proposed solution algorithm denoted by S-I. In addition, we discuss the computational results of M-I for (i) different sets of candidate nodes and (ii) multiple work crews.

4.3.1. Performance of the solution algorithm

To demonstrate the efficient solvability of the proposed solution approach, denoted by S-I, we compare its performance with an existing exact solution algorithm, the covering decomposition method, denoted by S-II (Israeli & Wood, 2002; Yao et al., 2007). Fig. 8 depicts the computation speed of S-I with respect to S-II for different protector budgets (B_P) and attacker budgets (B_I). To be consistent in recording the time, we track the solution time of S-I and S-II for similar set of candidate nodes (Closeness centrality set). The trends generally indicate that S-I surpasses S-II in terms of computation time. Particularly for the higher budget scenarios, the performance of S-I considerably exceeds S-II. For example, for $B_I = 4$, S-I finds the optimal solution around 3.5 times faster than S-II for $B_P = 3$, and this rate increases substantially to about 7 for $B_P = 4$.

Fig. 9 depicts the convergence behavior of the upper bound and lower bound values in the S-I algorithm for the candidate nodes built upon the closeness centrality set for$B_P = 4$ under different attacker budgets. The trend shows that, as the algorithm iteration continues to grow, the gap between the upper and lower bound values either decreases or remains the same until the tolerance gap is zero or sufficiently small. As such, the whole algorithm is terminated, and the final solution is returned. In addition, the number of algorithm iterations grows as the complexity of the problem increases (in terms of the available budget), which results in a longer computational time. In the initial iterations, the drop in the upper bound values is substantial since the most effective attack plans are sent to the master problem, and the master problem finds an optimal protection decision in such a way that the least disruption is imposed to the system. Therefore, as the algorithm iteration grows, critical components are fortified, and the importance of the components decreases (from the perspective of the attacker). Consequently, in early iterations, we witness a noticeable improvement in the solution as the gap between the upper bound and lower bound values reduces rapidly. Then this improvement slows down until the convergence ratio of upper bound and lower bound (i.e., the stopping criterion of the algorithm, ε) is reached and the final solution is found. Clearly, the larger the convergence ratio that is selected by the decision maker, the quicker the algorithm is terminated. As a result, the computational complexity of the algorithm lessens considerably as it is also a function of convergence ratio.

4.3.2. Computational results of M-I for different sets of candidate nodes

To compare the objective function value of each set of candidate nodes, the algorithm is executed for every set separately under different budget scenarios, the results of which are provided in Table 5. As the base scenario, we solve the model assuming that a single work crew is available for each network. Thereafter, different scenarios account for

Table 3
The proportion of similar nodes.

	Degree	Betweenness	Closeness	Katz	PageRank	Load
Degree	1	0.37	0.33	0.83	0.57	0.37
Betweenness		1	0.37	0.37	0.27	0.90
Closeness			1	0.43	0.27	0.30
Katz				1	0.60	0.40
PageRank					1	0.30
Load						1

Table 4
The proximity matrix of different sets of candidate nodes.

	Degree	Betweenness	Closeness	Katz	PageRank	Load
Degree	0	0.63	0.67	0.17	0.43	0.63
Betweenness		0	0.63	0.63	0.73	0.10
Closeness			0	0.57	0.73	0.70
Katz				0	0.40	0.60
PageRank					0	0.70
Load						0

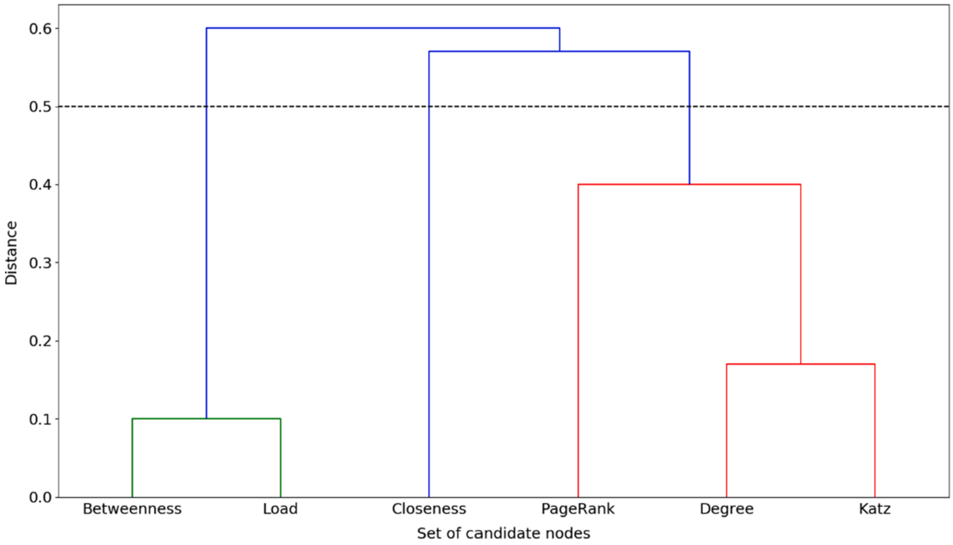


Fig. 6. The dendrogram of clustering different sets of candidate nodes.

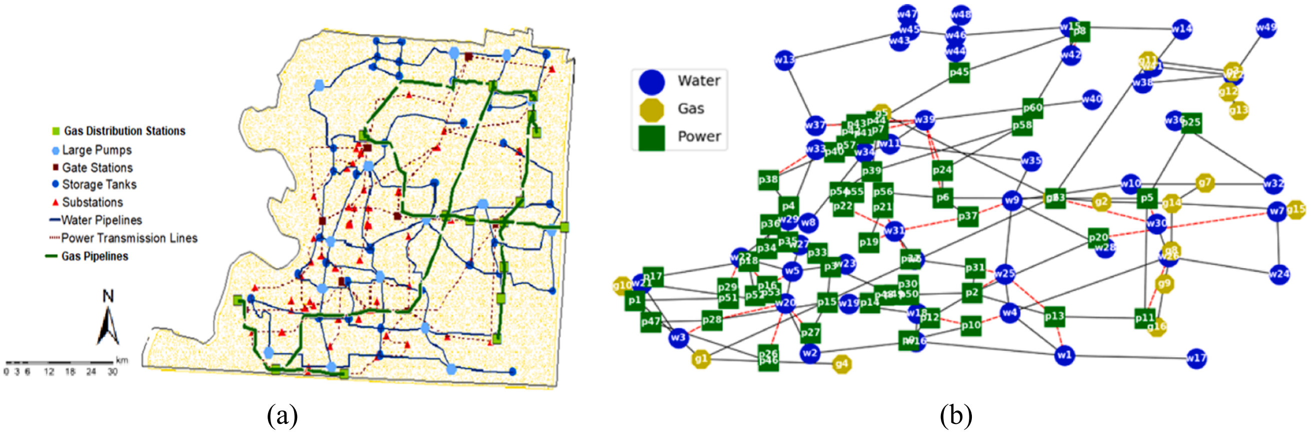


Fig. 7. The (a) map and (b) topology of the interdependent system of water, gas, and power networks in Shelby County, TN, USA.

multiple crews for a selected number of budget scenarios, and the results are discussed subsequently. In addition to the objective value of the model ($\xi_{\text{M-I}}$), we record the immediate drop in the system performance following the attack, $t = 1$, when the restoration process has not yet commenced, denoted by $\nu_{\text{M-I}}$ in Table 5.

From Table 5, the immediate drop in the system performance does not reduce substantially as the protection budget increases. For example, for $B_I = 4$, although the protector budget increases from 3 to 4, the reduction in system vulnerability is negligible. This is because in the objective function of M-I in Eq. (A2), the recovery process over time is also considered. Therefore, the optimal decision made by the attacker is not necessarily the one the decreases the performance of the system the most at $t = 1$. Instead, the interdiction strategy is based upon maximizing the summation of loss over the time span of the model. Likewise, the protector considers the total time required for the system to be fully recovered to minimize the amount of loss over time. Therefore, the protector does not only focus on vulnerability reduction immediately after disruption, but also simultaneously considers the restoration process of the system. As such, the solution returned by M-I allocates resources to harden the system to simultaneously (i) mitigate its vulnerability against disruptions, and (ii) minimize the long-term effect after the disruption.

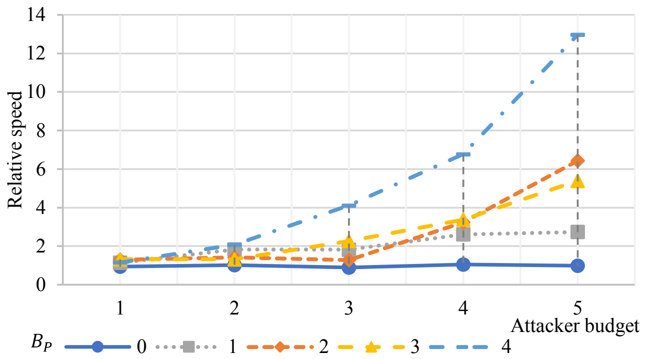


Fig. 8. Computation speed of S-I with respect to S-II under different budget scenarios.

Fig. 10 illustrates the trend of the objective value for M-I under different sets of candidate nodes for protection budgets of 0–4. Clearly, for a given protection budget, the objective value ($\xi_{\text{M}-\text{I}}$), standing for the system resilience measure over time, deteriorates for all three sets of candidate nodes as the attacker budget continues to increase. By comparing five figures, it is revealed that by adding protection resources, the system resilience measure over time regularly improves from Fig. 10a to Fig. 10e. Note that the objective value for the set constructed based on the Load centrality measure is higher than other two sets for protection budget 0–2. However, the objective value derived from PageRank centrality set surpasses Load centrality set for protection budget of 4. In addition, the objective value resulting from the set constructed based on Closeness centrality measure is generally lower than other two sets for all protection budget scenarios except for zero. Therefore, it can be concluded that the set built upon Load centrality measure is more critical since it imposes more loss to the system if they are interdicted, followed by the PageRank centrality set and Closeness centrality set which are ranked as the least critical sets, respectively, for this case study.

4.3.3. *Computational results of M-I for multiple work crews*

One of the advantages of M M-I I is that multiple work crews can operate simultaneously for each network for the recovery process. To illustrate the broad capabilities of both model (M-I) and proposed solution algorithm (S-I), we double and triple the available work crews at each infrastructure network and compare the results of the model with the base scenario in which a single work crew operates for every network. The aim of this analysis is to study the impact of resource (work crew) changes on the long-term effect of disruption. To be consistent in obtaining the results, we track the objective function value of similar set of candidate nodes (Closeness centrality set) for each scenario of available work crew. With respect to the budget availability, we solve the model for $B_I = 5$ under two protection budgets (i.e., $B_I = 5$ and $B_P = 0$ and 1).

As mentioned in Section 1 and in reference to Fig. 1, network performance at time t is represented with $\varphi(t) = 1 - \zeta(t)$. Note that $\zeta(t)$ is the weighted fraction of unmet demand at time t, as shown in Eq. (1). Fig. 11 illustrates network performance trajectories for different scenarios of work crew (WC) availability. Discussed previously, in the initial step, there is a drop in the performance of network followed by the disruption represented by $\nu_{\text{M}-\text{I}}$ in Table 5. Then, the restoration procedure begins until the whole system is fully recovered. Clearly, considering multiple work crews expedites the restoration process as multiple jobs can be operated in parallel, which results in earlier system recovery. From Fig. 11 for both budget scenarios, the whole system returns to its normal operation at time 7 and 5 for doubled resources and tripled resources, respectively. However, the recovery process lasts until time 11 for the single work crew scenario (base scenario). The trend of recovery (the required time for restoring each disrupted component) is similar for all cases as the restoration rate for each component, λ_i^k, is assumed equal regardless of the type of work crews available at each network. Note that the immediate drops in network performance for Fig. 11a and b are $\nu_{\text{M}-\text{I}} = 0.36$ and $\nu_{\text{M}-\text{I}} = 0.29$, respectively. This difference is the result of changing the protection budget from 0 to 1, and the attacker decision is changed accordingly. With respect to computational complexity, the proposed algorithm (S-I) performs efficiently for all three scenarios of resource availability, and the differences among computational times are not significant for three scenarios.

4.4. *Tri-level Formulation: Protection-Interdiction-Counteraction model (M-II)*

As discussed in Section 3.1, the proposed tri-level model (M-I) accounts for restoration level in the third level. To analyze the value of simultaneous consideration of both pre-disruption investments (to reinforce critical network components) and post-disruption resource assignment and crew scheduling, we modify M-I to M-II such that the system operator reacts to the disruption by solving an optimal network flow problem to minimize the unmet demand ($\zeta_{\text{M}-\text{II}}(t=1)$) without taking into account the recovery process. We represent specific changes to the model indices, parameters, decision variables, and constraints in M-I to build up the new model (M-II).

Like M-I, we define $\zeta_{\text{M}-\text{II}}(t)$ as the weighted proportion of unmet demand (relative to the met demand before the disruption), as shown in Eq. (26). Then, the objective function of M-II is defined as Eq. (27), including three successive actions: (i) the system planner minimizes the unmet demand by reinforcing the network components before disruption, (ii) the interdictor maximizes the unmet demand by interdicting the network components, and (iii) the system operator minimizes the unmet demand by optimally sending the flow through the network after the attack is observed. Since M-II does not include the recovery process of the disrupted components, the time horizon of the model is considered one period ($T = 1$), representing the immediate drop in the system performance following the attack. So, the objective function is denoted by $\nu_{\text{M}-\text{II}}$ as shown in Eq. (27). Note that the entire parameters and decision variables indexed by time ($t \in T$) are also considered only for one-time unit such that $t = 1$.

$$\zeta_{\text{M}-\text{II}}(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it}^k}{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it_e}^k} \right) \qquad \forall t \in T \tag{26}$$

$$\nu_{\text{M}-\text{II}} = \min_{y} \max_{\text{z}} \min_{\eta, x, F} \zeta_{\text{M}-\text{II}}(t = 1) \tag{27}$$

Constraints (A11)-(A14), (A23)-(A35), and (A41)-(A44) in M-I are removed as they correspond to the restoration level. Constraints (A20)–(A22) are substituted with constraints (28)-(30), representing the amount of positive flow through any given link is a function of the functionality status of the corresponding link, along with its head and tail nodes.

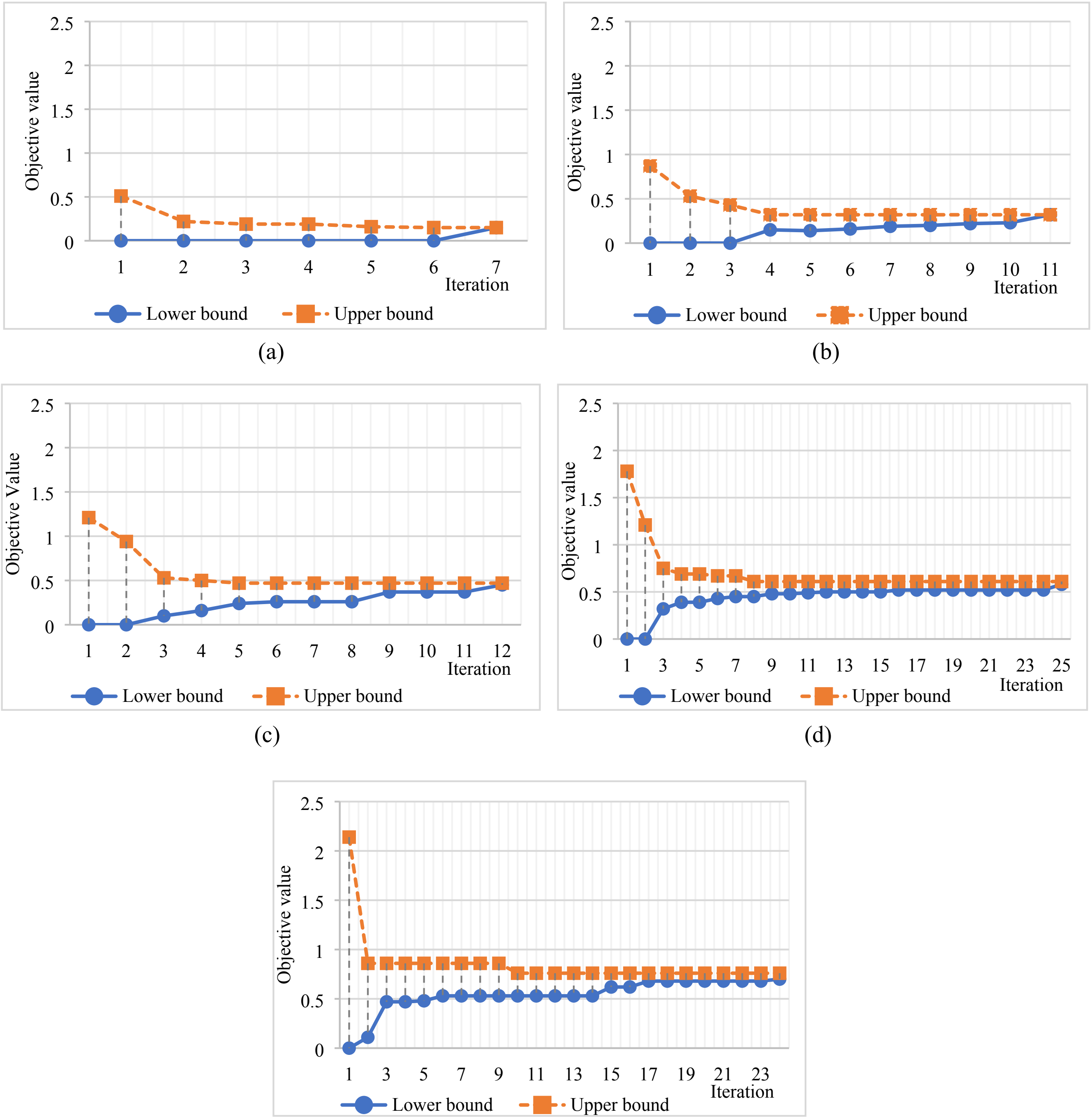
$$x_{ij1}^k \le u_{ij}^k F_{ij}^k \qquad \forall (i,j) \in A'^k, \forall k \in K \tag{28}$$

$$x_{ij1}^k \le u_{ij}^k F_i^k \qquad \forall (i,j) \in A^k, \forall i \in N'^k, \forall k \in K \tag{29}$$

$$x_{ij1}^k \le u_{ij}^k F_j^k \qquad \forall (i,j) \in A^k, \forall j \in N'^k, \forall k \in K \tag{30}$$

Finally, constraint (A36) in M-I is replaced by constraints (31), representing the physical interdependency among the networks of a system. In particular, constraints (31) state that positive flow through a link is a function of the functionality status of its corresponding related parent nodes (in other networks).

$$\begin{aligned} x_{ij1}^k \le u_{ij}^k F_{\bar{i}}^{\bar{k}} \qquad & \forall (i,j) \in A^k, \forall \bar{i} \in N'^{\bar{k}}, \forall k, \bar{k} \in K \big| \left((i,k), \left(\bar{i}, \bar{k} \right) \right) \\ & \in \Psi \text{ or } \left((j,k), \left(\bar{i}, \bar{k} \right) \right) \in \Psi \end{aligned} \tag{31}$$



(a)

(b)

(c)

(d)

(e)

Fig. 9. Convergence trend of upper bound and lower bound values in S-I algorithm as for$B_P = 4$ under (a)$B_I = 1$, (b) $B_I = 2$, (c) $B_I = 3$, (d) $B_I = 4$, and (e) $B_I = 5$.

Table 5
Computational results of M-I for each set of candidate nodes (generated based on different centrality measures) under different budget scenarios.

Protector budget (B_P)	Attacker budget (B_I)	Candidate node sets					
		Closeness		PageRank		Load	
		ξ_{M-I}	ν_{M-I}	ξ_{M-I}	ν_{M-I}	ξ_{M-I}	ν_{M-I}
0	1	0.31	0.16	0.28	0.14	0.31	0.16
	2	0.86	0.29	0.65	0.22	0.86	0.29
	3	1.10	0.31	1.05	0.26	1.33	0.36
	4	1.44	0.34	1.47	0.31	1.77	0.42
	5	1.73	0.36	2.05	0.33	2.28	0.44
1	1	0.28	0.14	0.25	0.12	0.28	0.14
	2	0.48	0.16	0.60	0.22	0.60	0.22
	3	0.79	0.21	0.96	0.24	0.95	0.24
	4	1.21	0.26	1.24	0.33	1.40	0.30
	5	1.57	0.29	1.68	0.29	1.93	0.35
2	1	0.19	0.09	0.21	0.10	0.19	0.09
	2	0.45	0.16	0.53	0.18	0.47	0.16
	3	0.76	0.21	0.83	0.31	0.81	0.21
	4	1.02	0.24	1.11	0.38	1.23	0.27
	5	1.33	0.26	1.46	0.43	1.51	0.29
3	1	0.15	0.08	0.20	0.10	0.17	0.08
	2	0.36	0.12	0.47	0.16	0.45	0.16
	3	0.68	0.17	0.81	0.21	0.80	0.22
	4	0.99	0.20	1.03	0.23	0.95	0.29
	5	1.13	0.20	1.24	0.33	1.25	0.24
4	1	0.14	0.07	0.19	0.10	0.15	0.08
	2	0.34	0.12	0.45	0.16	0.39	0.14
	3	0.61	0.16	0.79	0.21	0.70	0.18
	4	0.80	0.19	0.99	0.31	0.93	0.21
	5	0.93	0.25	1.20	0.31	1.09	0.23

Note that η^k_{i1}, x^k_{ij1}, F^k_i, and F^k_{ij} are the decision variables of the third level in M-II. The computational results of M-II, and the computational time comparison of M-I and M-II are discussed subsequently.

4.4.1. Computational results of M-II for different sets of candidate nodes

Table 6 shows computational results of M-II for each set of candidate nodes under different budget scenarios. Although the immediate drop in the system performance in M-I does not noticeably improve by increasing the protection budget (referring to $\nu_{\text{M-I}}$ in Table 5), the system vulnerability in M-II (referring to $\nu_{\text{M-II}}$ in Table 6) remarkably continues to reduce as the protection budget increases. This is because in the objective function of M-II, Eq. (27), the immediate drop in the system performance is the only resilience component taken into account. Therefore, the optimal decision made by the attacker is the one that decreases the performance of the system the most at $t = 1$. Likewise, the protector only focuses on the vulnerability reduction immediately after disruption in M-II. In addition, by comparing the objective values of two models, $\xi_{\text{M-I}}$ and $\nu_{\text{M-II}}$, under different budget scenarios, it is concluded that the system that is fortified based on M-I is considerably more resilient relative to M-II. These outcomes show the value of such a decision support tool (M-I) aiming to make a system more resilient by simultaneous consideration of (i) mitigating vulnerability and (ii) minimizing the long-term effect after disruption.

Fig. 12 illustrates the trend of objective value changes for M-II ($\nu_{\text{M-II}}$) under different sets of candidate nodes for protection budgets of 0–4. As it can be seen from Fig. 12a to e, the highest objective value belongs to the set created based on the PageRank centrality measure followed by the Load and Closeness centrality measures, respectively. This suggests that nodes in the PageRank set are more critical than other two sets in this system in terms of imposing more loss to the system immediately after a disruption if they are interdicted.

4.4.2. Computation time comparison of M-I and M-II

Table 7 provides the computational time of the algorithm for solving M-I and M-II under different budget scenarios. To be consistent in recording the time, we track the solution time of M-I and M-II for similar set of candidate nodes (Closeness centrality set). Fig. 13 illustrates the computation time (min) of M-I (a) and M-II (b) along with the relative speed of M-I in comparison with M-II (c) under different budget scenarios. The results suggest that there is an upward trend in computational burden of both M-I and M-II as the available budget continues to increase. Note that the vertical axis units in Fig. 13a and b are different since the computational time of two models are considerably variant (e.g., the maximum computation time in M-I is 456.28 however this time is 55.43 for M-II). According to Fig. 13c, M-II is significantly faster than M-I for all budget scenarios since the complexity of M-I is noticeably more than M-II (e.g., the number of decision variables and constraints). However, for a given interdiction budget, there are some fluctuations in the relative speed of M-I with respect to M-II as the protector budget changes since the convergence speed of the algorithm reduces for some specific budget scenarios.

5. Concluding remarks

Due to the growing dependency on critical infrastructure systems, ensuring their resilience is a main concern as even a small failure in one can cause considerable adverse impacts on community welfare and economic productivity for extended periods (Kettl, 2013). Infrastructure systems have complex structures that can be modeled as the network where the commodity (service) running through each infrastructure system represented by the flow. Interdiction models are widely applied to address the vulnerability reduction of such systems under hazard of an intelligent attack. In particular, the DAD model is considered as a useful tool to guide the improvement of the system performance from the beginning of a disruptive event to the total system recovery.

In this paper, we designed a new decomposition-based solution approach as a general framework to optimally solve DAD models such that the final solution is found by iteratively solving two bi-level formulations derived from the original tri-level model. To illustrate the efficient solvability of the proposed solution technique, we study the existing interdiction model proposed by Ghorbani-Renani et al. (2020) referred to as a protection-interdiction-restoration model (M-I). We illustrated M-I for the system of interdependent networks in Shelby County, TN, USA. The results indicate that the proposed solution algorithm substantially outperforms the covering decomposition method regarding the computational complexity. In addition, we generated different sets of candidate components as possibilities for disruption and protection based on different topological characteristics and using an agglomerative hierarchical clustering technique to derive the most vulnerable components. The results revealed that the set built upon the Load centrality measure is more critical since it imposes more loss to the system if interdicted, followed by the PageRank centrality set and Closeness centrality set.

Furthermore, we studied a protection-interdiction-counteraction model, denoted by M-II, to compare results and computational complexity with respect to the original protection-interdiction-restoration model (M-I). We solved M-II for three different sets of candidate nodes built upon Closeness, PageRank, and Load centrality measures. The results suggested that nodes in the PageRank set are more critical than other two sets in terms of imposing more loss to the system immediately after a disruption if they are interdicted. We can conclude that since PageRank set includes nodes which link from other important and link parsimonious nodes, or they are highly linked in this network, their failures result in the higher immediate loss to this system. Regarding the computation time, the results showed that although M-I is a comprehensive interdiction model relative to M-II since it accounts for both vulnerability reduction and recoverability enhancement, M-I is significantly computationally challenging and an efficient solution algorithm is required to solve such a complex model in a reasonable time. However, M-I is an effective tool for providing pre-disruption

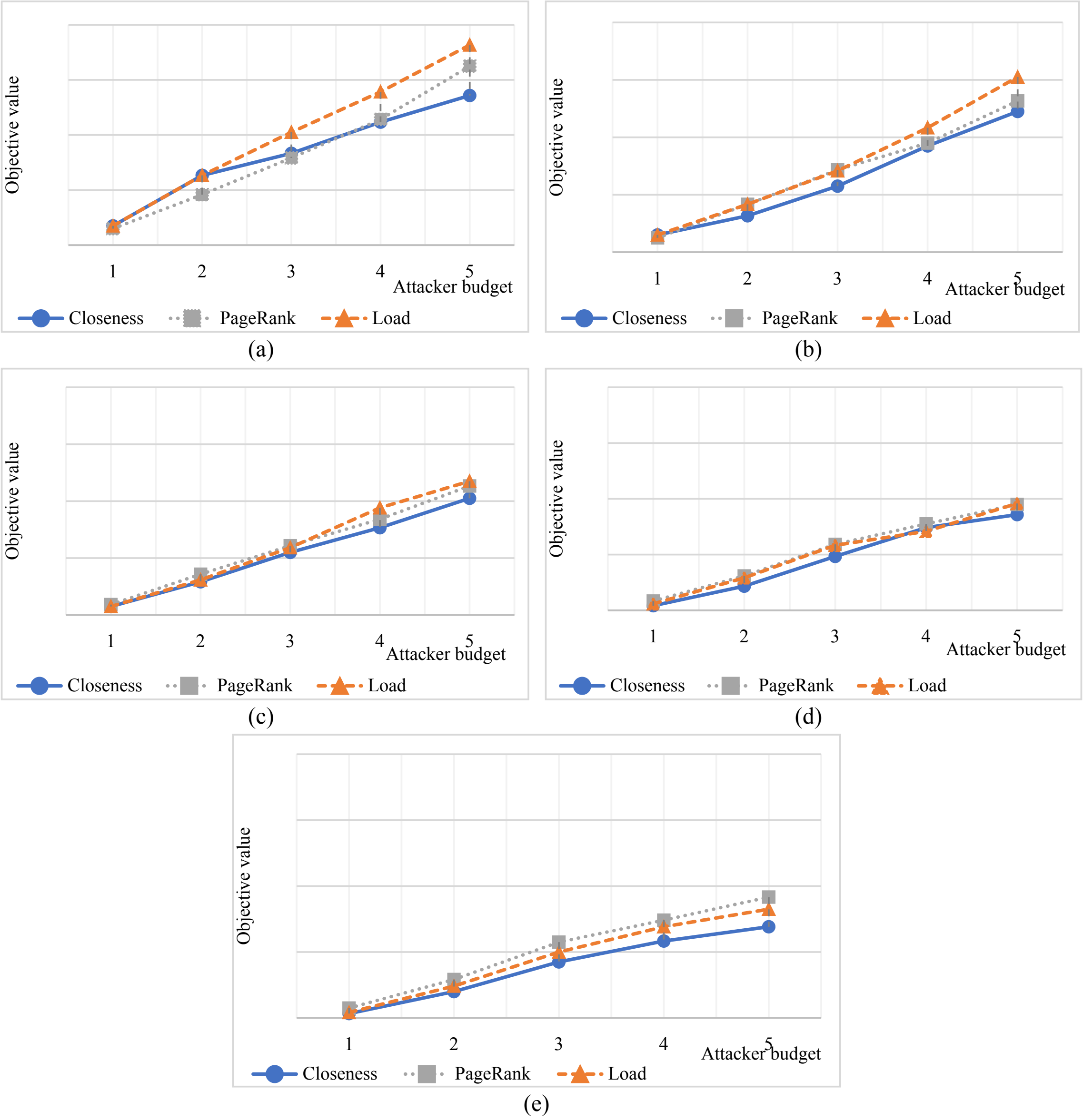
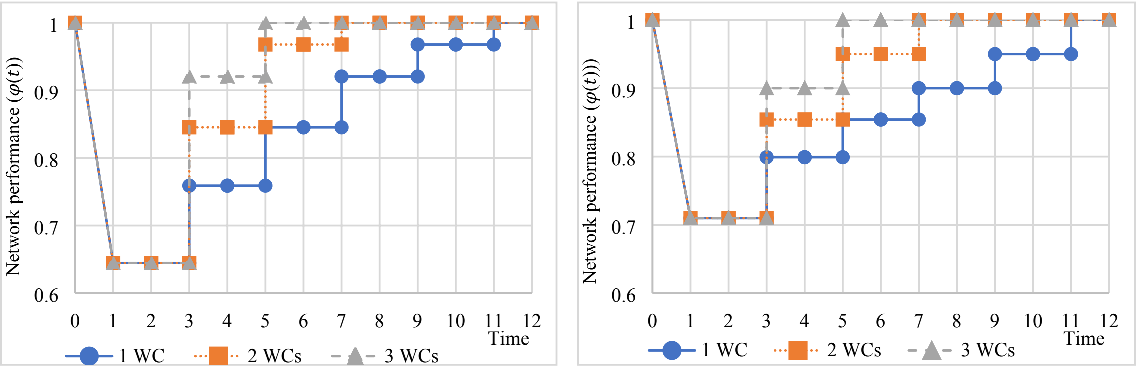


Fig. 10. Objective value of M-I ($\xi_{\mathrm{M-I}}$) for different sets of candidate nodes (generated based on different centrality measures) for protection budgets of (a) 0, (b) 1, (c) 2, (d) 3, and (e) 4.



(a) (b)

Fig. 11. Network performance $\varphi(t)$ of M-I as for$B_I = 5$ under (a)$B_P = 0$ and (b)$B_P = 1$.

Table 6
Objective value of M-II ($\nu_{\text{M-II}}$) for each set of candidate nodes (generated based on different centrality measures) under different budget scenarios.

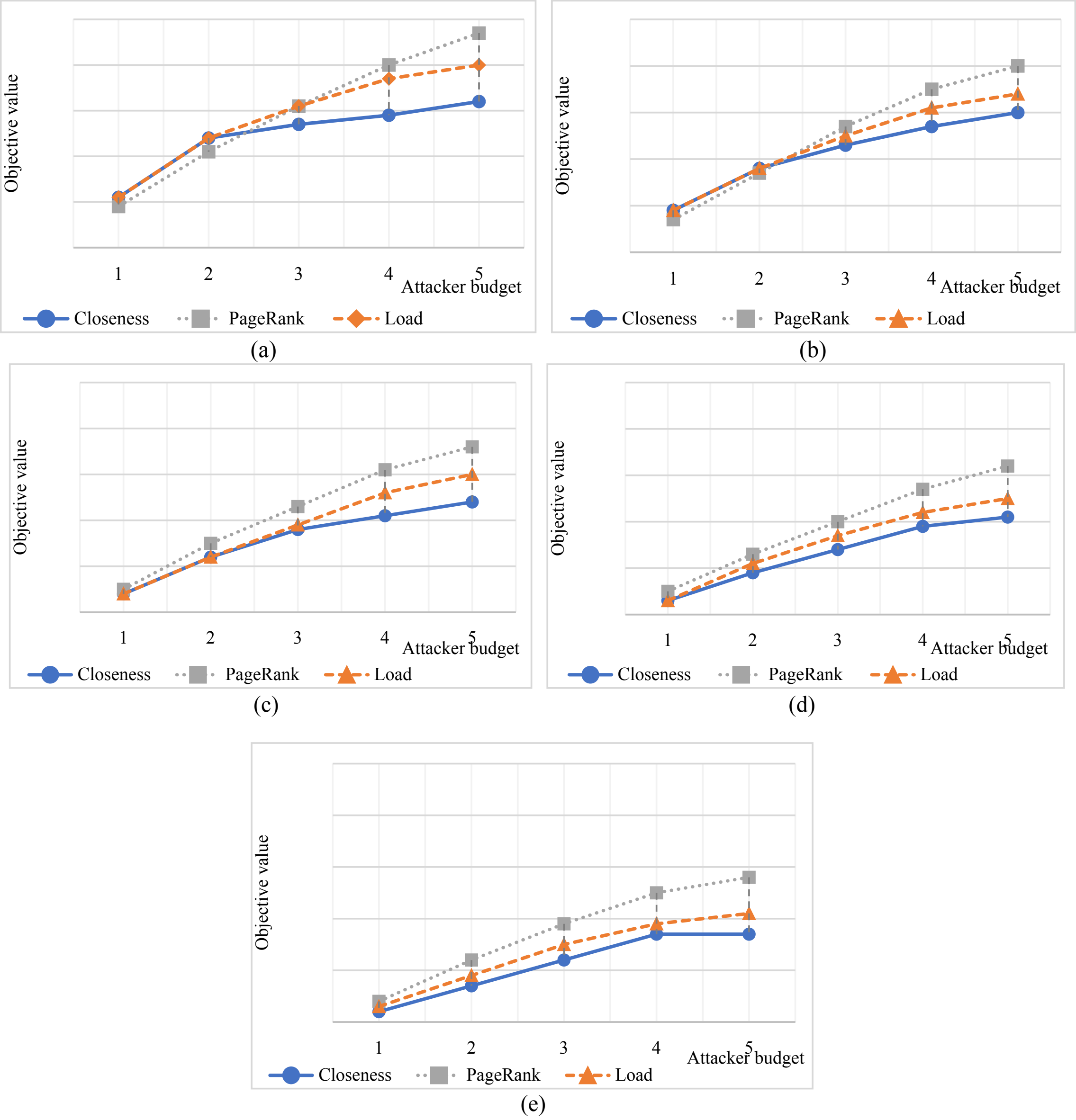
Protector budget (B_P)	Attacker budget (B_I)	Candidate node sets		
		Closeness	PageRank	Load
0	1	0.16	0.14	0.16
	2	0.29	0.26	0.29
	3	0.32	0.36	0.36
	4	0.34	0.45	0.42
	5	0.37	0.52	0.45
1	1	0.14	0.12	0.14
	2	0.23	0.22	0.23
	3	0.28	0.32	0.30
	4	0.32	0.40	0.36
	5	0.35	0.45	0.39
2	1	0.09	0.10	0.09
	2	0.17	0.20	0.17
	3	0.23	0.28	0.24
	4	0.26	0.36	0.31
	5	0.29	0.41	0.35
3	1	0.08	0.10	0.08
	2	0.14	0.18	0.16
	3	0.19	0.25	0.22
	4	0.24	0.32	0.27
	5	0.26	0.37	0.30
4	1	0.07	0.09	0.08
	2	0.12	0.17	0.14
	3	0.17	0.24	0.20
	4	0.22	0.30	0.24
	5	0.22	0.33	0.26

preparation decisions and post-disruption restoration planning. Therefore, there exists a tradeoff between employing a more comprehensive model with higher computational complexity or neglecting the recovery process of disrupted system through the interdiction model.

Though interdiction models have widespread applications from military to infrastructure networks along with other domains, they are generally nonconvex problems and computationally challenging to solve. Therefore, efficient solution methods are necessary to deal with such complex problems. For future work, we plan to explore heuristic solution techniques to overcome the computational complexity of interdiction models. In addition, machine learning techniques could be used to estimate the restoration schedule of disrupted components, which could significantly improve the efficiency of the algorithm. Furthermore, in the proposed model, an intelligent attacker with complete information about the network intentionally interdicts the system. The protector, on the other hand, defends (fortifies) the system in response to such a prospective interdiction. Another future consideration will explore the value of defender secrecy and deception for defensive investments in the interdiction models.

CRediT authorship contribution statement

Nafiseh Ghorbani-Renani: Methodology, Investigation, Writing - original draft. **Andrés D. González:** Conceptualization, Writing - review & editing. **Kash Barker:** Supervision, Writing - review & editing.



(a)

(b)

(c)

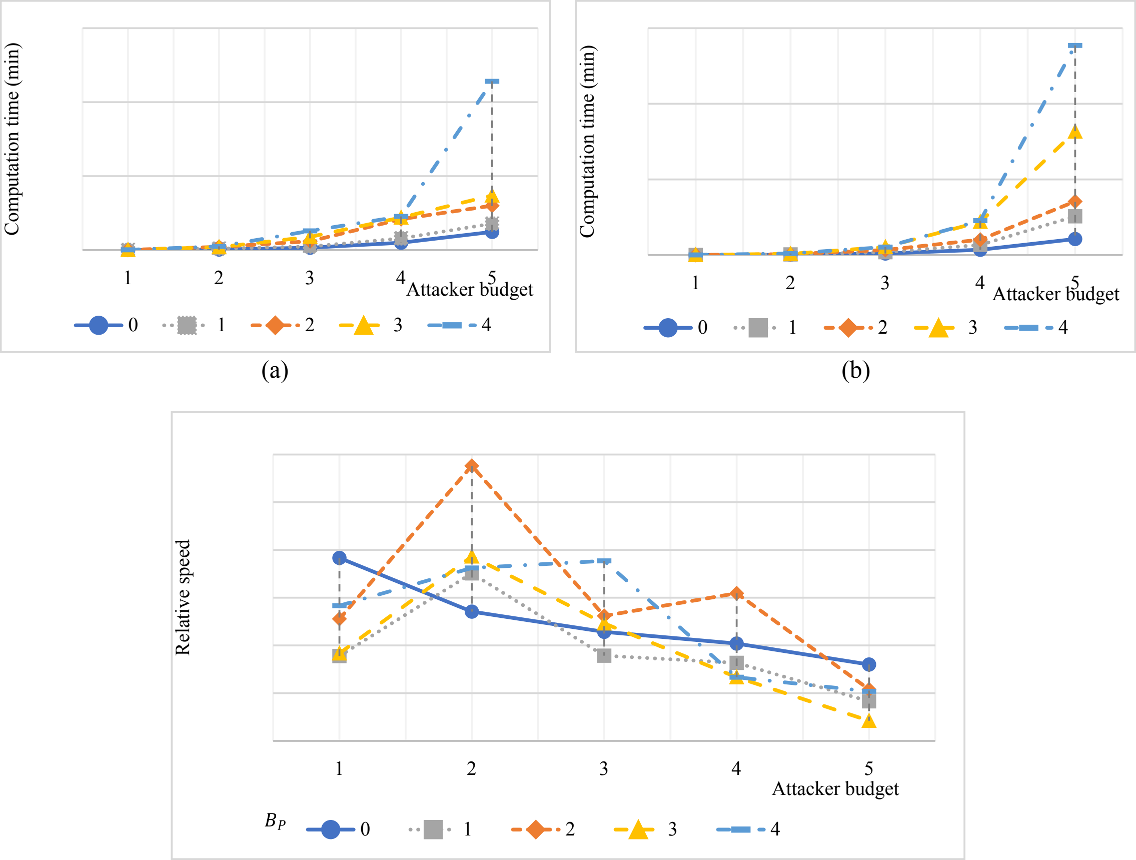
(d)

(e)

Fig. 12. The objective value of M-II ($\nu_{\text{M-II}}$) in different sets of candidate nodes (generated based on different centrality measures) for protection budgets of (a) 0, (b) 1, (c) 2, (d) 3, and (e) 4.

Table 7
Computational time of M-I and M-II under different budget scenarios.

Protector budget (B_P)	Attacker budget (B_I)	$\Gamma_{\text{M-I}}$(min)	$\Gamma_{\text{M-II}}$(min)	$\left(\frac{\Gamma_{\text{M-I}}}{\Gamma_{\text{M-II}}}\right)$
0	1	0.25	0.01	25.00
	2	1.46	0.08	18.25
	3	6.44	0.41	15.71
	4	19.93	1.4	14.24
	5	49.19	4.24	11.60
1	1	0.38	0.03	12.67
	2	3.92	0.17	23.06
	3	9.66	0.76	12.71
	4	31.64	2.68	11.81
	5	71.51	10.25	6.98
2	1	0.52	0.03	17.33
	2	8.78	0.24	36.58
	3	23.74	1.34	17.72
	4	83.67	4.07	20.56
	5	120.11	14.18	8.47
3	1	0.65	0.05	13.00
	2	8.06	0.32	25.19
	3	35.72	2.13	16.77
	4	87.94	8.79	10.00
	5	147.73	32.65	4.52
4	1	0.76	0.04	19.00
	2	9.97	0.42	23.74
	3	51.97	2.11	24.63
	4	91.04	9.1	10.00
	5	456.28	55.43	8.23



(a)

(b)

(c)

Fig. 13. Computation time of M-I (a) and M-II (b) along with the relative speed of M-I with respect to M-II (c) under different budget scenarios.

Appendix A. Tri-level Formulation: Protection-Interdiction-Restoration model (M-I)

Assume a set K of infrastructure networks. Network $k \in K$ is defined by $G^k = (N^k, A^k)$, where N^k is the set of nodes and A^k is the set of links that connect nodes. Let R be the set of work crews available for the system of interdependent networks, where the subset $R^k \subseteq R$ indicates the work crews that operate in network $k \in K$. Tables A1–A3 outline the model indices, parameters, and decision variables, respectively. Note that all parameters of the model are known and certain.

Objective function

$$\zeta_{\mathrm{M-I}}(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it}^k}{\sum_{k \in K} \sum_{i \in N_-^k} w_{it}^k \eta_{it_e}^k} \right) \qquad \forall t \in T \tag{A1}$$

$$\xi_{\mathrm{M-I}} = \min_{y} \max_{z} \min_{\eta, x, F, \alpha, \beta} \sum_{t \in T} \zeta_{\mathrm{M-I}}(t) \tag{A2}$$

Table A1
Model sets and indices.

K	Set of all infrastructure networks, indexed by k
N^k	Set of all nodes in network $k \in K$, indexed by i
A^k	Set of all links in network $k \in K$, indexed by (i,j)
N_+^k	Set of supply nodes in network $k \in K$ such that $N_+^k \subseteq N^k$
N_-^k	Set of demand nodes in network $k \in K$ such that $N_-^k \subseteq N^k$
N_0^k	Set of transshipment nodes in network $k \in K$ such that $N_0^k \subseteq N^k$
N'^k	Set of nodes that can be either protected or interdicted in network $k \in K$ such that$N'^k \subseteq N^k$
A'^k	Set of links that can be either protected or interdicted in network $k \in K$ such that$A'^k \subseteq A^k$
R^k	Set of work crews in network $k \in K$, indexed by$r$
T	Set of time periods, indexed by$t$

Table A2
Model parameters.

$\eta_{it_e}^k$	Flow reaching node $i \in N_-^k$ in network $k \in K$ before the attack
w_{it}^k	Importance weight assigned to node $i \in N_-^k$ in network $k \in K$ at time$t \in T$
B_P	Cardinality budget for the protector,$B_P \in \mathbb{Z}^*$
B_I	Cardinality budget for the interdictor,$B_I \in \mathbb{Z}^*$
S_i^k	Amount of supply in node $i \in N_+^k$ in network $k \in K$
d_i^k	Amount of demand in node $i \in N_-^k$ in network $k \in K$
u_{ij}^k	Capacity of link $(i,j) \in A^k$ in network $k \in K$
λ_i^k	Restoration rate of node $i \in N'^k$ in network $k \in K, 0 < \lambda_i^k \leq 1$
λ_{ij}^k	Restoration rate of link $(i,j) \in A'^k$in network $k \in K, 0 < \lambda_{ij}^k \leq 1$
M	An arbitrarily large positive number

Table A3
Model decision variables.

η_{it}^k	Amount of demand met at node $i \in N_-^k$ in network $k \in K$ in time $t \in T$, continuous
x_{ijt}^k	Flow on link$(i,j) \in A^k$ in network $k \in K$ in time $t \in T$, continous
y_i^k	Equal to 1 if node $i \in N'^k$in network $k \in K$ is protected, binary
y_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is protected, binary
z_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$is interdicted, binary
z_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is interdicted, binary
F_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is functional, binary
F_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is functional, binary
α_{it}^{kr}	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is restored by work crew $r \in R^k$in time $t \in T$, binary
α_{ijt}^{kr}	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is restored by work crew $r \in R^k$in time $t \in T$, binary
β_{it}^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is reactivated at time $t \in T$, binary
β_{ijt}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is reactivated at time $t \in T$, binary

First Level: Protection

$$\sum_{k\in K}\sum_{i\in N'^{k}} y_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} y_{ij}^k \leq B_P \tag{A3}$$

$$y_i^k \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K \tag{A4}$$

$$y_{ij}^k \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{A5}$$

Second Level: Interdiction

$$\sum_{k\in K}\sum_{i\in N'^{k}} z_i^k + \sum_{k\in K}\sum_{(i,j)\in A'^{k}} z_{ij}^k \leq B_I \tag{A6}$$

$$z_i^k \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K \tag{A7}$$

$$z_{ij}^k \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{A8}$$

Third Level: Restoration

$$1 + y_i^k - z_i^k \geq F_i^k \qquad \forall i \in N'^{k}, \forall k \in K \tag{A9}$$

$$1 + y_{ij}^k - z_{ij}^k \geq F_{ij}^k \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{A10}$$

$$F_{it}^k \leq 1 - \beta_{it}^k \qquad \forall i \in N'^{k}, \forall k \in K, \forall t \in T \tag{A11}$$

$$F_{ijt}^k \leq 1 - \beta_{ijt}^k \qquad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T \tag{A12}$$

$$\beta_{i1}^k = 0 \qquad \forall i \in N'^{k}, \forall k \in K \tag{A13}$$

$$\beta_{ij1}^k = 0 \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{A14}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k \leq S_i^k \qquad \forall i \in N_+^k, \forall k \in K, \forall t \in T \tag{A15}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k = 0 \qquad \forall i \in N_0^k, \forall k \in K, \forall t \in T \tag{A16}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k = -\eta_{it}^k \qquad \forall i \in N_-^k, \forall k \in K, \forall t \in T \tag{A17}$$

$$\eta_{it}^k \leq d_i^k \qquad \forall i \in N_-^k, \forall k \in K, \forall t \in T \tag{A18}$$

$$x_{ijt}^k \leq u_{ij}^k \qquad \forall (i,j) \in A^k, \forall k \in K, \forall t \in T \tag{A19}$$

$$x_{ijt}^k \leq u_{ij}^k\left(F_{ij}^k + \beta_{ijt}^k\right) \qquad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T \tag{A20}$$

$$x_{ijt}^k \leq u_{ij}^k\left(F_i^k + \beta_{it}^k\right) \qquad \forall (i,j) \in A^k, \forall i \in N'^{k}, \forall k \in K, \forall t \in T \tag{A21}$$

$$x_{ijt}^k \leq u_{ij}^k\left(F_j^k + \beta_{jt}^k\right) \qquad \forall (i,j) \in A^k, \forall j \in N'^{k}, \forall k \in K, \forall t \in T \tag{A22}$$

$$\sum\nolimits_{s=1}^{t} \alpha_{is}^{kr} \leq M\left(1 - \left(\alpha_{i(t+1)}^{kr} - \alpha_{it}^{kr}\right)\right) \qquad \forall i \in N'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A23}$$

$$\sum_{r\in R^k}\sum_{t\in T} \alpha_{it}^{kr} \geq \frac{\left(1 - F_i^k\right)}{\lambda_i^k} \qquad \forall i \in N'^{k}, \forall k \in K \tag{A24}$$

$$\sum_{r\in R^k}\sum_{t\in T} \alpha_{it}^{kr} < \left(\frac{\left(1 - F_i^k\right)}{\lambda_i^k} + 1\right) \qquad \forall k \in K, \forall i \in N'^{k} \tag{A25}$$

$$\sum\nolimits_{s=1}^{t} \alpha_{ijs}^{kr} \leq M\left(1 - \left(\alpha_{ij(t+1)}^{kr} - \alpha_{ijt}^{kr}\right)\right) \qquad \forall (i,j) \in A'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A26}$$

$$\sum_{r\in R^k}\sum_{t\in T} \alpha_{ijt}^{kr} \geq \frac{\left(1 - F_{ij}^k\right)}{\lambda_{ij}^k} \qquad \forall k \in K, \forall (i,j) \in A'^{k} \tag{A27}$$

$$\sum_{r\in R^k}\sum_{t\in T} \alpha_{ijt}^{kr} < \left(\frac{\left(1 - F_{ij}^k\right)}{\lambda_{ij}^k} + 1\right) \qquad \forall k \in K, \forall (i,j) \in A'^{k} \tag{A28}$$

$$\sum_{\substack{s \in R^k \\ s \neq r}} \sum_{t \in T} \alpha_{it}^{ks} \leq M\left(1 - \alpha_{it}^{kr}\right) \quad \forall i \in N'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A29}$$

$$\sum_{\substack{s \in R^k \\ s \neq r}} \sum_{t \in T} \alpha_{ijt}^{ks} \leq M\left(1 - \alpha_{ijt}^{kr}\right) \quad \forall (i,j) \in A'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A30}$$

$$\sum_{r \in R^k} \alpha_{it}^{kr} \leq 1 \quad \forall i \in N'^{k}, \forall k \in K, \forall t \in T \tag{A31}$$

$$\sum_{r \in R^k} \alpha_{ijt}^{kr} \leq 1 \quad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T \tag{A32}$$

$$\sum_{(i,j) \in A'^{k}} \alpha_{ijt}^{kr} + \sum_{i \in N'^{k}} \alpha_{it}^{kr} \leq 1 \quad \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A33}$$

$$1 - \left(\frac{\frac{\left(1 - F_i^k\right)}{\lambda_i^k} - \sum_{r \in R^k} \sum_{s=1}^{t-1} \alpha_{is}^{kr}}{M} \right) \geq \beta_{it}^k \quad \forall i \in N'^{k}, \forall k \in K, \forall t \in T | t \neq 1 \tag{A34}$$

$$1 - \left(\frac{\frac{\left(1 - F_{ij}^k\right)}{\lambda_{ij}^k} - \sum_{r \in R^k} \sum_{s=1}^{t-1} \alpha_{ijs}^{kr}}{M} \right) \geq \beta_{ijt}^k \quad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T | t \neq 1 \tag{A35}$$

$$x_{ijt}^k \leq u_{ij}^k \left(F_{\bar{i}}^{\bar{k}} + \beta_{\bar{i}t}^{\bar{k}} \right) \quad \forall (i,j) \in A^k, \forall \bar{i} \in N'^{\bar{k}}, \forall k, \bar{k} \in K | \left((i,k), \left(\bar{i}, \bar{k}\right) \right) \in \Psi \;\; or \;\; \left((j,k), \left(\bar{i}, \bar{k}\right) \right) \in \Psi, \forall t \in T \tag{A36}$$

$$\eta_{it}^k \geq 0 \quad \forall i \in N_{-}^k, \forall k \in K, \forall t \in T \tag{A37}$$

$$x_{ijt}^k \geq 0 \quad \forall (i,j) \in A^k, \forall k \in K, \forall t \in T \tag{A38}$$

$$F_i^k \in \{0,1\} \quad \forall i \in N'^{k}, \forall k \in K \tag{A39}$$

$$F_{ij}^k \in \{0,1\} \quad \forall (i,j) \in A'^{k}, \forall k \in K \tag{A40}$$

$$\alpha_{it}^{kr} \in \{0,1\} \quad \forall i \in N'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A41}$$

$$\alpha_{ijt}^{kr} \in \{0,1\} \quad \forall (i,j) \in A'^{k}, \forall r \in R^k, \forall k \in K, \forall t \in T \tag{A42}$$

$$\beta_{it}^k \in \{0,1\} \quad \forall i \in N'^{k}, \forall k \in K, \forall t \in T \tag{A43}$$

$$\beta_{ijt}^k \in \{0,1\} \quad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T \tag{A44}$$

References

Akbari-Jafarabadi, M., Tavakkoli-Moghaddam, R., Mahmoodjanloo, M., & Rahimi, Y. (2017). A tri-level r –interdiction median model for a facility location problem under imminent attack. *Computers & Industrial Engineering, 114*(October), 151–165.

Akbari-Jafarabadia, M., Tavakkoli-Moghaddam, R., Mahmoodjanloo, M., & Rahimi, Y. (2016). A three-level mathematical model for an r-interdiction hierarchical facilities location problem.

Aksen, D., & Aras, N. (2012). A bilevel fixed charge location model for facilities under imminent attack. *Computers & Operations Research, 39*(7), 1364–1381.

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Wood, R. K. (2011). Solving Defender-Attacker-Defender Models for Infrastructure Defense. *12th INFORMS Computing Society Conference, 28–49, 7*.

Alguacil, N., Delgadillo, A., & Arroyo, J. M. (2014). A trilevel programming approach for electric grid defense planning. *Computers and Operations Research, 41*(1), 282–290.

Almoghathawi, Y., Barker, K., & Albert, L. A. (2019). Resilience-driven restoration model for interdependent infrastructure networks. Reliability Engineering and System Safety, 185(December 2017), 12–23.

Altner, D. S., Ergun, Ö., & Uhan, N. A. (2010). The Maximum Flow Network Interdiction Problem: Valid inequalities, integrality gaps, and approximability. *Operations Research Letters, 38*(1), 33–38.

Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis, 31*(4), 515–522.

Ayyub, B. M. (2014). Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. *Risk Analysis, 34*(2), 340–355.

Bard, J. F. (1991). Some properties of the bilevel programming problem. *Journal of Optimization Theory and Applications, 68*(2), 371–378.

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability Engineering & System Safety, 117*, 89–97.

Baycik, N. O., Sharkey, T. C., & Rainwater, C. E. (2018). Interdicting layered physical and information flow networks. *IISE Transactions, 50*(4), 316–331.

Bier, V. M., Gratz, E. R., Haphuriwat, N. J., Magua, W., & Wierzbicki, K. R. (2007). Methodology for identifying near-optimal interdiction strategies for a power transmission system, 92, 1155–1161.

Borndörfer, R., Sagnol, G., & Schwartz, S. (2016). An Extended network interdiction problem for optimal toll control. *Electronic Notes in Discrete Mathematics, 52*, 301–308.

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530–544.

Brown, G. G., Carlyle, W. M., Harney, R. C., Skroch, E. M., & Wood, R. K. (2009). Interdicting a Nuclear-Weapons Project. *Operations Research, 57*(4), 866–877.

Brown, G. G., Carlyle, W. M., & Wood, R. K. (2008). Optimizing Department of Homeland Security Defense Investments : Applying Defender-Attacker (-Defender)

Optimization To Terror Risk Assessment and Mitigation. Appendix E, National Academies Press, Washington, DC, pp. 1–30.

Chang, S. E., McDaniels, T. L., Mikawoz, J., & Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: Power outage consequences in the 1998 Ice Storm. *Natural Hazards, 41*(2), 337–358.

Davarikia, H., & Barati, M. (2018). A tri-level programming model for attack-resilient control of power grids. *Journal of Modern Power Systems and Clean Energy, 6*(5), 918–929.

Fathollahi-Fard, A. M., Hajiaghaei-Keshteli, M., & Mirjalili, S. (2018). Hybrid optimizers to solve a tri-level programming model for a tire closed-loop supply chain network design problem. *Applied Soft Computing Journal, 70*, 701–722.

Fathollahi Fard, A. M., & Hajiaghaei-Keshteli, M. (2018). A tri-level location-allocation model for forward/reverse supply chain. *Applied Soft Computing Journal, 62*, 328–346.

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

Ghare, P. M., Montgomery, D. C., & Turner, W. C. (1971). Optimal interdiction policy for a flow network. *Naval Research Logistics Quarterly, 18*(1), 37–45.

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

Goh, K.-I., Kahng, B., & Kim, D. (2001). Universal Behavior of Load Distribution in Scale-Free Networks. *Phys. Rev. Lett., 87*(27), 278701.

Golbeck, J. (2013). Chapter 3 – Network Structure and Measures. In J. Golbeck (Ed.), *Analyzing the Social Web* (pp. 25–44). Boston: Morgan Kaufmann.

Gomez, C., González, A. D., Baroud, H., & Bedoya-Motta, C. D. (2019). Integrating operational and organizational aspects in interdependent infrastructure network recovery. *Risk Analysis, 39*(9), 1913–1929.

González, A. D., Dueñas-Osorio, L., Medaglia, A. L., & Sánchez-Silva, M. (2016a). The time-dependent interdependent network design problem (td-INDP) and the evaluation of multi-system recovery strategies in polynomial time. In H. W. Huang, J. Li, J. Zhang, & J. B. Chen (Eds.), The 6th Asian-Pacific Symposium on Structural Reliability and its Applications (pp. 544–550). Shanghai, China.

González, A. D., Dueñas-Osorio, L., Sánchez-Silva, M., & Medaglia, A. L. (2016). The interdependent network design problem for optimal infrastructure system restoration. *Computer-Aided Civil and Infrastructure Engineering, 31*(5), 334–350.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29*(4), 498–501.

Hansen, P., Jaumard, B., & Savard, G. (1992). New branch-and-bound rules for linear bilevel programming. *SIAM Journal on Scientific and Statistical Computing, 13*(5), 1194–1217.

Hernandez-Fajardo, I., & Dueñas-Osorio, L. (2011). Sequential propagation of seismic fragility across interdependent lifeline systems. *Earthquake Spectra, 27*(1), 23–43.

Homeland Security Presidential Directive (2003). Critical Infrastructure Identification, Prioritization, and Protection.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety, 145*, 47–61.

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

Kettl, D. F. (2013). *System Under Stress: Homeland Security and American Politics*. CQ Press.

Lai, K., Illindala, M., & Subramaniam, K. (2019). A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Applied Energy, 235*, 204–218.

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

Lin, Y., & Bie, Z. (2018). Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding. *Applied Energy, 210*, 1266–1279.

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

Mahmoodjanloo, M., Parvasi, S. P., & Ramezanian, R. (2016). A tri-level covering fortification model for facility protection against disturbance in r-interdiction median problem. *Computers & Industrial Engineering, 102*, 219–232.

McCarter, M., Barker, K., Johansson, J., & Ramirez-Marquez, J. E. (2018). A bi-objective formulation for robust defense strategies in multi-commodity networks. *Reliability Engineering & System Safety, 176*, 154–161.

McMasters, A. W., & Mustin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly, 17*(3), 261–268.

Mendonça, D., & Wallace, W. A. (2006). Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures, 12(December), 260–270.

Mohammad, A., Fard, F., & Hajiaghaei-keshteli, M. (2018). A bi-objective partial interdiction problem considering different defensive systems with capacity expansion of facilities under imminent attacks. *Applied Soft Computing Journal, 68*, 343–359.

Morshedlou, N., González, A. D., & Barker, K. (2018). Work crew routing problem for infrastructure network restoration. *Transportation Research Part B: Methodological, 118*, 66–89.

Motto, A. L., Arroyo, J. M., & Galiana, F. D. (2005). A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat. *IEEE Transactions on Power Systems, 20*(3), 1357–1365.

Murtagh, F. (1983). A survey of recent advances in hierarchical clustering algorithms. *The Computer Journal, 26*(4), 354–359.

Murtagh, F., & Contreras, P. (2011). Methods of Hierarchical Clustering. *Computing Research Repository – CORR*.

Nandi, A. K., Medal, H. R., & Vadlamani, S. (2016). Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender–attacker model. *Computers & Operations Research, 75*, 118–131.

Needham, M., & Hodler, A. E. (2019). *Graph Algorithms: Practical Examples in Apache Spark and Neo4j*. O'Reilly Media.

Newman, M. (2018). Networks. OUP Oxford.

Nurre, S. G., Cavdaroglu, B., Mitchell, J. E., Sharkey, T. C., & Wallace, W. A. (2012). Restoring infrastructure systems: An integrated network design and scheduling (INDS) problem. *European Journal of Operational Research, 223*(3), 794–806.

Ouyang, M. (2017). A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks. *European Journal of Operational Research, 262*(3), 1072–1084.

Ouyang, M., & Fang, Y. (2017). A mathematical framework to optimize critical infrastructure resilience against intentional attacks. *Computer-Aided Civil and Infrastructure Engineering, 32*(11), 909–929.

Pan, F., Charlton, W. S., & Morton, D. P. (2003). A Stochastic Program for Interdicting Smuggled Nuclear Material. In D. L. Woodruff (Ed.), *Network Interdiction and Stochastic Integer Programming* (pp. 1–19). Boston, MA: Springer, US.

Parvasi, S. P., Mahmoodjanloo, M., & Setak, M. (2017). A bi-level school bus routing problem with bus stops selection and possibility of demand outsourcing. *Applied Soft Computing, 61*, 222–238.

Patterson, S. A., & Apostolakis, G. E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering & System Safety, 92*(9), 1183–1203.

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

Ramirez-Marquez, J. E., Rocco, C. M., & Barker, K. (2017). Bi-objective vulnerability-reduction formulation for a network under diverse attacks. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 3*(4), 04017025.

Rourke, T. D. O. (2006). Critical Infrastructure , Interdependencies , and Resilience.

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

Saharidis, G. K. D., Conejo, A. J., & Kozanidis, G. (2013). Exact Solution Methodologies for Linear and (Mixed) Integer Bilevel Programming. In E.-G. Talbi (Ed.), *Metaheuristics for Bi-level Optimization* (pp. 221–245). Berlin, Heidelberg: Springer, Berlin Heidelberg.

Salmeron, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems, 19*(2), 905–912.

Salmeron, J., Wood, K., & Baldick, R. (2009). Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids. *IEEE Transactions on Power Systems, 24*(1), 96–104.

Sharkey, T. C., Cavdaroglu, B., Nguyen, H., Holman, J., Mitchell, J. E., & Wallace, W. A. (2015). Interdependent network restoration: On the value of information-sharing. *European Journal of Operational Research, 244*(1), 309–321.

Smith, J. C., & Lim, C. (2008). Algorithms for Network Interdiction and Fortification Games. In A. Chinchuluun, P. M. Pardalos, A. Migdalas, & L. Pitsoulis (Eds.), *Pareto Optimality, Game Theory And Equilibria* (pp. 609–644). New York, NY: Springer, New York.

Song, J., & Ok, S.-Y. (2010). Multi-scale system reliability analysis of lifeline networks under earthquake hazards. *Earthquake Engineering & Structural Dynamics, 39*(3), 259–279.

Stackelberg, H. V. (1952). *The Theory of Market Economy*. Oxford: Oxford University Press.

Wallace, W. A., Mendonça, D., Lee, E. E., & Mitchell, J. E. (2001). *Managing Disruptions to Critical Interdependent Infrastructures in the Context of the 2001*. World Trade Center Attack.

Wollmer, R. (1964). Removing arcs from a network. *Operations Research, 12*(6), 934–940.

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

Wu, X., & Conejo, A. J. (2017). An efficient tri-level optimization model for electric grid defense planning. *IEEE Transactions on Power Systems, 32*(4), 2984–2994.

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

Yuan, W., Wang, J., Qiu, F., Chen, C., Kang, C., & Zeng, B. (2016). Robust optimization-based resilient distribution network planning against natural disasters. *IEEE Transactions on Smart Grid, 7*(6), 2817–2826.

Yuan, W., Zhao, L., & Zeng, B. (2014). Optimal power grid protection through a defender-attacker-defender model. *Reliability Engineering and System Safety, 121*, 83–89.

Zeng, B., & Zhao, L. (2013). Solving two-stage robust optimization problems using a column-and- constraint generation method. *Operations Research Letters, 41*(5), 457–461.