UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

TRI-LEVEL INTERDICTION MODEL FOR ENHANCING INTERDEPENDENT NETWORK RESILIENCE

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

NAFISEH GHORBANI RENANI
Norman, Oklahoma
2021

TRI-LEVEL INTERDICTION MODEL FOR ENHANCING INTERDEPENDENT NETWORK RESILIENCE

A DISSERTATION APPROVED FOR THE
SCHOOL OF INDUSTRIAL AND SYSTEMS ENGINEERING

BY THE COMMITTEE CONSISTING OF

Dr. Kash Barker, Chair

Dr. Andrés González, Co-chair

Dr. Yang Hong

Dr. Theodore Trafalis

Dr. Talayeh Razzaghi

To

A real Jedi, Alireza

My supportive parents

And

Amir and Iman, my beloved brothers

Acknowledgements

First, I would like to express my sincere gratitude to Dr. Kash Barker, my advisor, for his continuous support, invaluable advice, patience, encouragement, and immense knowledge. I cannot express how much I truly appreciate his great mentorship.

Special thanks to Dr. Andrés González, my co-advisor, for his enormous guidance, assistance, and immense knowledge in the path of my research.

I would like to acknowledge my committee members, Dr. Yang Hong, Dr. Theodore Trafalis, and Dr. Talayeh Razzaghi. I am grateful for their time and insightful feedback towards the completion of this work.

I extend my gratitude to Dr. Raman, the faculty, and staff of the School of Industrial and Systems Engineering at the University of Oklahoma for their continuous support and encouragement.

My deepest gratitude and appreciation to my mother and father, for their love, support, and encouragement. They are truly my very first mentors who taught me kindness, perseverance, patience, and independence.

Most importantly, I would like to thank my supportive husband, Alireza, who is absolutely a real Jedi, the guardian of peace in the galaxy of our life. This accomplishment would not have been possible without him.

Finally, I am very appreciative of my colleagues and friends for their feedback, support, encouragement, and good wishes.

Table of Contents

List of Tables

List of Figures

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.

As such, the first contribution of this research is to propose a tri-level protection-interdiction-restoration problem for a system of interdependent networks, to balance vulnerability and recoverability before and after a disruption. In particular, the proposed tri-level model represents decisions made (i) by a defender before a disruption to reduce network vulnerability, (ii) by an attacker to effectively disrupt the network, and (iii) by a defender after the disruption to enhance recoverability. To solve the proposed protection-interdiction-restoration model to optimality, we use a tailored extension of the covering decomposition algorithm. To illustrate the proposed tri-level model and the modified covering decomposition algorithm, we present a case-study of the system of

interdependent water, gas, and power utilities in Shelby County, TN. The computational results show the value of simultaneous analysis of both pre-disruption investments (to reinforce critical network components) and post-disruption resource assignment and crew scheduling.

Interdiction models have a wide variety of real-world applications from military to facility location problem to project management. DAD formulation is a type of interdiction model that can be applied to study the resilience of a system against intelligent attacks. However, DAD models are computationally challenging to solve, requiring efficient solution methods to deal with such complex problems. As the second contribution of this research, we address this issue by designing 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. In addition, 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.

The third contribution of this research is to develop a general framework for novel hybrid solution techniques that are applicable in a wide range of interdiction (particularly DAD) models. Hence, we propose two hybrid algorithms that solve smaller nested bi-level problems (master problem and subproblem) to cope with the computational burden of tri-level DAD models. The first solution approach integrates Benders decomposition method with a metaheuristic algorithm, while the second combines a set covering approach and metaheuristic algorithm. The two hybrid algorithms are applied to solve the existing DAD model, namely a tri-level protection-interdiction-restoration model. Two systems of interdependent networks with different sizes are studied to demonstrate the efficient solvability of the developed solution approaches for real-sized problems. The results highlight the capabilities of the two solution approaches for solving such a complex model under different budget scenarios in terms of the quality of solution and computational time.

Finally, we address optimization of protection strategies of a critical infrastructure network for cascading failures. This work aims to enhance network resilience against cascading failures initiated by intentional attack with a model that accounts for both pre-

and post-disruption planning. The proposed model is a novel DAD model determining (i) which component needs to be protected prior to the disruptive event, (ii) which component is critical in terms of its failure by itself along with causing other parts failures defined as cascading failures, and (iii) what restoration crew schedule is efficient following a disruptive event. To verify the model for cascading failures, we focus on interdiction and restoration levels of this formulation. We present a case study of IEEE 9-bus electric power test system consisting of 9 buses, 3 generators, and 3 loads indicated transshipment, supply and demand nodes, respectively. The results indicate how an initial damage could propagate throughout the system resulting in further disruption and system loss.

Chapter 1: INTRODUCTION AND MOTIVATION

1.1 Overview

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 (Homeland Security Presidential 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 et al., 2007; Mendonça & Wallace, 2006; Nurre et al., 2012; Rourke, 2006; Wallace et al., 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 withstand a disruption, adapt to, and recover from it is generally referred to as *resilience* (Aven, 2011; Ayyub, 2014; Haimes, 2009; Hosseini et al., 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. Figure 1.1 depicts system performance, $\varphi(t)$, before and after a disruption, underlining *vulnerability* and *recoverability* as two critical planning dimensions of resilience.

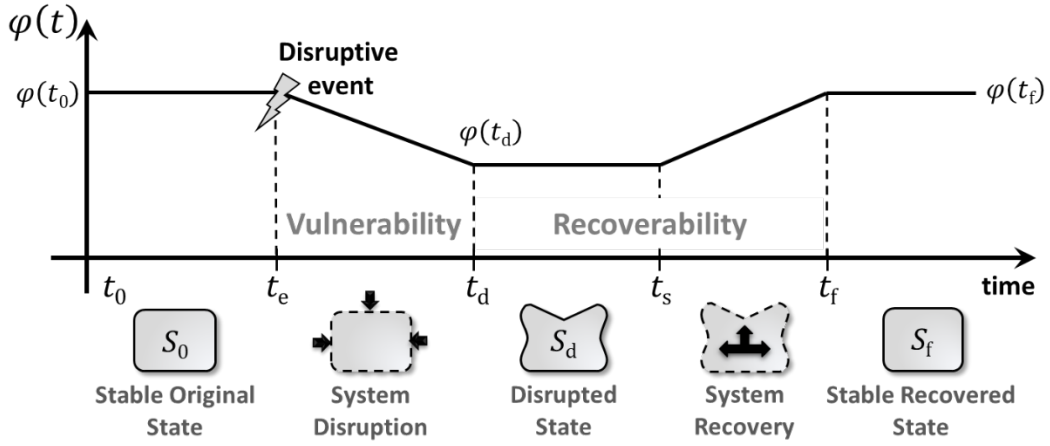


Figure 1.1. System performance trajectory, $\varphi(t)$, following a disruptive event (adapted from Barker et al. (2013)).

The study of critical infrastructure networks under disruption has matured considerably in the past fifteen years, where emphasis has been given to identifying topological descriptors (e.g., Albert and Barabási, 2002; Holmgren, 2006; Nagurney and Qiang, 2009; Newman et al., 2011) and flow-based descriptors (e.g., Larocca et al., 2015; Nicholson et al., 2016; Ouyang, 2013; Rocco et al., 2010) that enable the study of critical network components that lead to network *vulnerability*. Michaud and Apostolakis (2006) proposed a methodology for rating the components of water supply networks and assess the effects of the failure of each of the network components considering their capacity and repair time. Murray et al. (2007) proposed an optimization model for identifying the upper and lower bounds on flow disruption resulting from network interdiction.

Other studies provide methods and algorithms for *recovering* critical infrastructure networks following the occurrence of a disruptive event by determining the set of disrupted network components that need to be restored to maximize the performance of the network, assigning these components to work crews, determining the restoration sequence of these components, or an integrated approach (e.g., Aksu & Ozdamar, 2014; Fang et al., 2016; Kamamura et al., 2015; Matisziw et al., 2010; Morshedlou et al., 2018; Nurre et al., 2012; Vugrin et al., 2014; Xu et al., 2007). In particular, the restoration of interdependent infrastructure networks has recently been addressed by Almoghathawi et al. (2019), González et al. (2017), González et al. (2016), and Sharkey et al. (2015). However, maintaining network performance is of interest from pre-disruption to post-disruption periods. The literature does not sufficiently explore the simultaneous analysis of vulnerability reduction and recoverability improvement in systems of interdependent networks—an important consideration in light of pre-disruption and post-disruption resource allocation. Therefore, we address this important missing area of literature by proposing a tri-level protection-interdiction-restoration model for a system of interdependent networks to balance vulnerability and recoverability before and after a disruption.

The tri-level optimization approach proposed in this dissertation is generally depicted in Figure 1.2. From this figure, the first defender action is to allocate resources (how much and where) to harden the interdependent networks to reduce their collective vulnerability prior to disruption. The attacker action allocates resources to maximize the effects of the disruption, though naturally this stage does not necessarily require a human

"attacker" and could represent a "worst-case" natural disaster or other accidental failures. The second defender action minimizes the long-term effect after the disruption through network component recovery.

Figure 1.2. Notional approach to the protection-interdiction-restoration problem.

Hausken and Levitin (2012) provided a thorough overview of the literature on the defense of and attack on different systems, categorizing 129 journal articles based on the structure of the system and on defense and attack strategies. According to this classification, we focus on the system of interdependent networks defined by a set of nodes connected with a set of links where the service provided by each network is represented by flow through it. We consider physical interdependency for 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. An intelligent attacker, who has complete information about the network, intentionally interdicts the system. The disruption (interdiction) takes the form of a reduction in the capacity of the network components either nodes or links. The protector, on the other hand, defends (fortifies) the system in response to such prospective interdiction by increasing the capacity of the network component or adding redundancy to it as the defense strategy.

However, such formulations (e.g., interdiction models) are computationally challenging to solve. Therefore, efficient solution algorithms are required to address such complex problems in a reasonable time while maintaining a good quality in the proposed solutions. In this dissertation, we address this issue by proposing novel decomposition-based algorithms to deal with a wide range of interdiction models particularly defender-attacker-defender (DAD) models with total or partial protection and interdiction.

1.2 Structure of the Dissertation

This dissertation is organized as follows. Chapter 2 presents a detailed literature review on (i) the development of interdiction models and their application in network-based systems, and (ii) the primary solution methods to solve such models. In Chapter 3, the proposed tri-level protection-interdiction-restoration model is formulated in detail. To solve the proposed tri-level model to optimality, we discuss a tailored extension of the covering decomposition algorithm. To illustrate the proposed tri-level model and the modified covering decomposition algorithm, we present a case-study of the system of interdependent water, gas, and power utilities in Shelby County, TN. In Chapter 4, we present 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 In Chapter 5, we present two hybrid algorithms that solve smaller nested bi-level problems (master problem and subproblem) to cope with the computational burden of tri-level DAD models. The first solution approach integrates Benders decomposition method with a metaheuristic algorithm, while the second combines a set covering approach and metaheuristic algorithm. The two hybrid algorithms are applied to solve the existing DAD model, namely a tri-level protection-interdiction-restoration model. Two systems of interdependent networks with different sizes are studied to demonstrate the efficient solvability of the developed solution approaches for real-sized problems. In Chapter 6, we focus on improving the resilience of a single structured network (e.g., optimizing the network protection plans) against cascading failures caused by an intentional attack building on an existing resilience interdiction model. The proposed formulation is a novel DAD model determining (i) which component needs to be protected prior to the disruptive event, (ii) which component is critical in terms of its failure by itself along with causing other parts failures defined as cascading failures, and (iii) what restoration crew schedule is efficient following a disruptive event. To validate the model for cascading failures, we provided an illustrative example based on the single structured network of IEEE 9-bus power system. Finally, we conclude this dissertation in Chapter 7 by providing the future avenues of this research.

Chapter 2: LITERATURE REVIEW

2.1 Introduction

For several decades, interdiction models have received much attention due to their applicability in different domains, including defense and military applications (Ghare et al., 1971; McMasters & Mustin, 1970; Patterson & Apostolakis, 2007), controlling trafficking illicit materials (Baycik et al., 2018; McLay et al., 2011; Morton et al., 2007; Pan et al., 2003), facility location problems (Akbari-jafarabadi et al., 2017; Akbari-Jafarabadia et al., 2016; Liberatore et al., 2011; Losada et al., 2012; Fathollahi Fard et al., 2018), and project management (Brown et al., 2009), among others.

This dissertation is concerned with (i) the resilience control of interdependent infrastructure networks against adversaries using interdiction models, and (ii) efficient solution approaches to solve the model in a reasonable time. Thus, this dissertation is related to two main areas of research: (i) the application of interdiction models in network-based systems, and (ii) existing solution algorithms for solving the proposed interdiction models. These two sectors will be discussed in this chapter.

2.2 Interdiction Models in Network-based Systems

Network-based systems broadly appear in various service, community, industrial, and economic environments. Infrastructure systems such as power, gas, and water supply are ubiquitous in community health and productivity. Thus, it is essential to have effective decision support tools to assist decision makers in ensuring the security and resilience of such systems under a variety of disruptions (e.g., natural disasters, malevolent attacks, operational failures) (Ma et al., 2013). Particularly, decision makers

should make prudent decisions about allocating finite resources (how much and where?) to harden the system in such a way to (i) mitigate its vulnerability to disruption, and (ii) minimize the long-term effect after the disruption, along with the decisions regarding the post-disruption restoration planning. Such a decision support tool can be effectively achieved using interdiction models. Interdiction models are formulated as a sequential game in the form of multi-level hierarchical framework with a corresponding hierarchy of decisions made at each level. In the following, we discuss interdiction models applied in common network-based systems.

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, interdiction models were considered as a powerful approach for pre-disruption strategies to reduce the vulnerability of network-based systems under intelligent attacks (Zhu et al., 2013). A number of interdiction models have been developed for critical infrastructure networks, particularly power networks. Salmeron et al. (2004) initially assessed power grid vulnerability by developing a bi-level AD formulation. The proposed power grid interdiction model identifies critical system components, the outage of which would result in the maximum disruption to the system for a given attacker budget. Subsequently, Brown et al. (2006) discussed that, although the AD model is applicable for vulnerability analysis of critical infrastructure networks by determining the set of critical components in the system, it does not necessarily determine the best (optimal) pre-disruption defensive strategy against an attacker's decision, which can mislead the decision maker to fortify the system inefficiently.

Therefore, they introduced an additional level of defender action to the previous model, developing the tri-level DAD model for the power grid to enable the system to better withstand failure. In the proposed model, the first defender represents the system planner seeking to determine the best protection plan against the most destructive attacker decision. Subsequently, Yao et al. (2007), Alguacil et al. (2014), and Yuan et al. (2014) explored vulnerability mitigation of the electric power grid through a DAD model. In addition, interdiction models have received considerable attention for reducing the vulnerability of transportation networks under disruption. For example, Alderson et al. (2011) developed a DAD model for defending a transportation network against an intelligent adversary. Likewise, Alderson et al. (2014) and Sarhadi et al. (2015) applied this modeling framework to determine how to improve the operation of a rail network subject to disruption.

As critical infrastructure systems may depend on each other to be operational, a disruption in one can spread to other networks (Sharkey et al., 2015). Therefore, some researchers have been motivated to include interdependency among infrastructure systems in this modeling framework. For example, Ouyang (2017) proposed a tri-level DAD model to address the resilience of interdependent critical infrastructure systems under the worst spatially localized attacks. In this study, the operation of each infrastructure system is modeled by a network flow model with links connecting the interdependent systems. Ouyang (2017) quantifies the resilience of critical infrastructure systems immediately following a disruptive event and before any recovery efforts. Other works have incorporated restoration cost or recovery duration of disrupted components in

interdiction models. For example, Salmeron et al. (2004) considered the cost of repair duration of damaged components in the objective function of an AD model for analyzing electric grid vulnerability. Ouyang and Fang (2017) considered the repair sequence of disrupted components with given recovery resources in a tri-level model.

With the above contributions in mind, we propose a new interdiction model specifically to enhance the resilience of a system of interdependent infrastructure networks under hazard of an intelligent attack by accounting for pre-disruption protection and post-disruption restoration. The proposed model 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.

2.3 Solution Approaches for Solving Interdiction Models

Nabli et al. (2020) analyzed the computational complexity of sequential games formulated by multilevel problems and performed on a network application. Martin (2007) claimed that the general DAD is NP-hard and challenging to solve. Considering the widespread applications of such models, the development of efficient solution methods has captured attention in recent years. Below we discuss primary solution approaches along with their costs and benefits for solving interdiction models.

Israeli and Wood (2002) introduced two decomposition-based algorithms to solve the bi-level shortest path interdiction problem and enhanced them by adding valid inequalities. The first algorithm applies Benders decomposition where the second one utilizes the set covering approach. Motto et al. (2005) exactly solved the bi-level AD model by taking dual of the second level and transforming it to a single-level model. Salmeron et al. (2004) developed a decomposition-based heuristic algorithm to solve the bi-level interdiction model to find an acceptable interdiction plan from the perspective of an intelligent attacker. Likewise, Bier et al. (2007) proposed a heuristic method for dealing with the AD model for assessing power transmission system vulnerability based on a greedy algorithm such that at each iteration, the transmission line with the maximum load is interdicted. Though this approach does not provide an optimal solution, it is an inexpensive and practical method for determining promising interdiction plans in relatively complex systems.

Yao et al. (2007) applied covering decomposition (CD) method to solve the tri-level power grid interdiction formulation. This approach, which is an extension of a set covering decomposition method (Israeli & Wood, 2002), iteratively solves nested bi-level problems to reach the optimal solution. However, this decomposition-based method is computationally expensive and is not applicable to large networks (Alguacil et al., 2014). Ghorbani-Renani et al. (2020) introduced an improvement to the CD algorithm to solve the tri-level DAD model. Although this development increases the efficiency of the algorithm, it still suffers from the computational burden imposed by large-size problems. Ghorbani-Renani et al. (2021) designed a decomposition-based solution approach to

optimally solve tri-level DAD models, demonstrating improvement in computational complexity relative to the CD algorithm, particularly for higher budget scenarios. Yuan et al. (2014) developed the column-and-constraint generation (C&CG) method to solve the tri-level power network model to optimality, outperforming the CD algorithm with respect to computational effort. Note that Zeng and Zhao (2013) originally presented the C&CG algorithm to derive optimal solutions for two-stage robust optimization problems. Curry and Smith (2016) reviewed solution techniques to solve wireless sensor network problems, including the column generation approach. Alguacil et al. (2014) proposed a two-stage solution strategy to find the optimal solution for the DAD problem by converting it to its equivalent bi-level model through dualizing the third level and merging it with the second level. Then, the transformed model was solved to optimality by an implicit enumeration algorithm. While the proposed two-stage solution method is computationally more efficient than CD algorithm, it may not be applicable for multiple attacks and protection decisions (Yuan et al., 2014). On the other hand, the two solution approaches proposed by Yuan et al. (2014) and Alguacil et al. (2014) are based on converting the two levels into a single level by taking the dual of the inner level. Such a conversion can only be applicable for linear programming problems in the lower level since Karush-Kuhn-Tucker optimality conditions are not satisfied for either nonlinear or mixed integer problems (Israeli & Wood, 2002; Wood, 1993). Cappanera and Scaparra (2011) applied an implicit enumeration algorithm to solve the tri-level shortest path interdiction problem. They enhanced the algorithm by utilizing a heuristic approach to generate valid inequalities, leading to a reduction in the search tree size. Ouyang (2017)

solved exactly the proposed tri-level DAD model by iteratively solving nested bi-level models constructed from the original model. The devised algorithm is based on the decomposition algorithm developed by Alderson et al. (2014 & 2011) and incorporates the concept of "maximal component set" and Benders decomposition. However, Ouyang (2017) discussed that utilizing some heuristic algorithms (e.g., genetic algorithm) as alternatives may improve the efficiency of the algorithm. Ouyang and Fang (2017) utilized a decomposition algorithm to solve the developed DAD mathematical framework to optimality. Although the proposed algorithm is an exact solution method, it is applied to a very small illustrative example of nine nodes. However, infrastructure networks are often large-sized problem and, due to the general features of DAD models, the computational complexity of the algorithm grows exponentially in such an application. Note that along with other factors (e.g., complexity of the formulation by itself), the run time of the DAD model is highly sensitive to the amount of budget available for the attacker and protector, since increases in budget result in more possible combinations for interdiction and protection (e.g., the feasibility space is expanded).

From the above discussion, it can be concluded that exact solution methods for solving interdiction models typically have limitations from modeling and computational complexity perspectives. In addition, the computational difficulty of optimizing interdiction models thwarts the decision maker from effectively applying such models to moderate or large-scaled systems. Especially, interdiction models with a nonconvex inner level remain challenging to solve and only particular cases of this type of model have been explored recently. In this regard, hybrid algorithms incorporating exact solution

algorithm and heuristic method can increase the efficiency of the solution approach (Akbari-jafarabadi et al., 2017). Aksen and Aras (2012) solved a bi-level facility location problem with Tabu search. Similarly, Sadati et al. (2020) proposed an AD model for identifying the most critical depots in a vehicle routing context and used Tabu search to solve the lower level. Mahmoodjanloo et al. (2016) solved a DAD model for facility protection with (i) an exact solution approach based on an implicit enumeration algorithm and (ii) a heuristic-based method using a genetic algorithm.

Several contributions have been made to explore hybrid algorithms that are candidates for solving DAD models in reasonable time. However, they could not entirely handle a wide variety of DAD models with different modeling features (e.g., DAD models with partial or total fortification and interdiction, DAD models with a nonconvex inner level). In addition, the quality of solutions is not guaranteed in such solution approaches. Therefore, we are motivated to devise hybrid decomposition-based algorithms to effectively deal with a wide range of interdiction models, particularly DAD models with different modeling characteristics and application sizes, while not sacrificing the quality of the provided solutions.

Chapter 3: PROTECTION-INTERDICTION-RESTORATION: TRI-LEVEL OPTIMIZATION FOR ENHANCING INTERDEPENDENT NETWORK RESILIENCE

3.1 Introduction

In this chapter, we present tri-level protection-interdiction-restoration problem for a system of interdependent networks, to balance vulnerability and recoverability before and after a disruption. In which, the proposed tri-level model represents decisions made (i) by a defender before a disruption to reduce network vulnerability, (ii) by an attacker to effectively disrupt the network, and (iii) by a defender after the disruption to enhance recoverability. The contribution of this model is to consider simultaneously (i) a set of interdependent infrastructure networks, (ii) an optimal defense plan against a set of most destructive attack strategies, (iii) a set of most critical elements through the system, and (iv) allocating and scheduling work crews to recover disrupted elements in the restoration level to return the system to its standard operation.

The remainder of this chapter is organized as follows. In Section 3.2, the proposed tri-level model is formulated in detail. In Section 3.3, we discuss the solution approach for solving the model. To showcase the application of the proposed tri-level model, an illustrative example and computational results are presented in Section 3.4. Finally, Section 3.5 provides concluding remarks and future work.

3.2 Tri-level Optimization Model

This dissertation is concerned with the resilience control (enhancement) of interdependent infrastructure networks (e.g., electric power, water supply) under intelligent attacks. We model this problem as a tri-level DAD hierarchical formulation with a corresponding hierarchy of decisions. 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 affects the decisions of other levels. Figure 3.1 is a general depiction of the three levels involved in this problem: (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.

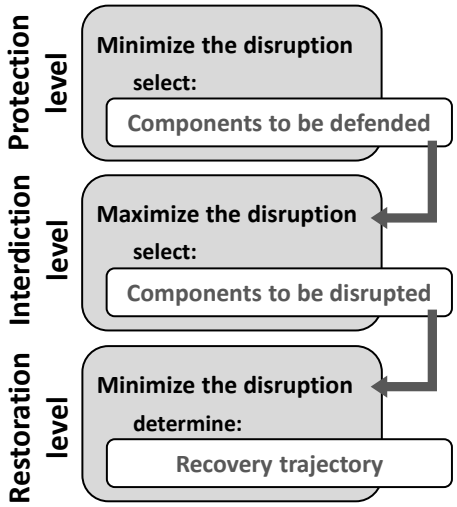


Figure 3.1. Tri-level protection-interdiction-restoration process.

3.2.1 Tri-level Model Assumptions

The proposed optimization model has the following underlying assumptions associated with the structure and operation of the system of networks and their interdependencies, as well as the related costs of protection, interdiction, and recovery, among others.

- Each infrastructure network consists of a set of nodes (including supply, demand and transshipment nodes) connected by a set of links, such that each supply node, demand node, and link have known supply capacity, demand, and flow capacity, respectively.
- There is a known fixed cost associated with protecting or interdicting each network component.

- There are known budgets available for protecting and for interdicting the components of the system of interdependent networks.
- Each component can be fully protected in the first stage of the model such that protected components will be invulnerable to disruption.
- There is a number of work crews (work groups) responsible for repairing disrupted components in each infrastructure network, and this number can vary by network.
- A work crew can only work on a single disrupted component at a time. A disrupted component can be restored by a single work crew (once the disrupted component is assigned to them) until they become operational.
- There is a known restoration rate for each component, λ, representing the proportion of the component restoration per unit time by each work crew.
- Restoration time for each disrupted component is a function of both its failure and its restoration rate, both of which can vary by component.
- Infrastructure networks are physically interdependent such that every "parent" node must be operational for the dependent "child" nodes to be operational.

3.2.2 Notation

An undirected network is denoted by $G = (N, A)$, where N is the set of nodes, and A is the set of links. Assume a set K of networks, each with a set of nodes N^k such that $\bigcup_{k \in K} N^k = N$ and set of links A^k such that $\bigcup_{k \in K} A^k = A$. Nodes can consist of supply nodes ($N_+^k \subseteq N^k$), demand nodes ($N_-^k \subseteq N^k$) and transshipment nodes ($N_=^k \subseteq N^k \setminus \{N_-^k, N_+^k\}$) such that $N_+^k \cap N_-^k = \emptyset$. 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 interdicted or protected in the system of interdependent networks. Note that, even though the proposed model has a multicommodity structure, it assumes that a single commodity flows through each network (i.e., each individual network is in charge of supplying a specific commodity). Ψ represents interdependency among networks such that $\left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi$ denotes node $i \in N^k$ in network $k \in K$ physically depends on node $\bar{\imath} \in N^{\bar{k}}$ in network $\bar{k} \in K$ where $N^k \cap N^{\bar{k}} = \emptyset$, $A^k \cap A^{\bar{k}} = \emptyset$ and $\forall\, k, \bar{k} \in K: k \neq \bar{k}$. Set R^k represents the available work crews in network $k \in K$. Index $t \in T$ provides the set of available time periods. Table 3.1 and Table 3.2 outline the model parameters and decision variables, respectively.

Table 3.1. Model parameters.

w_{it}^k	Importance weight assigned to node $i \in N_-^k$ in network $k \in K$ at time $t \in T$
CP_{ij}^k	Cost of protecting link $(i,j) \in A'^k$ in network $k \in K$
CP_i^k	Cost of protecting node $i \in N'^k$ in network $k \in K$
CI_{ij}^k	Cost of attacking link $(i,j) \in A'^k$ in network $k \in K$
CI_i^k	Cost of attacking node $i \in N'^k$ in network $k \in K$
BP	Total available budget for the protector
BI	Total available budget for the interdictor
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_{ij}^k	Restoration rate of the link $(i,j) \in A'^k$ in network $k \in K$
λ_i^k	Restoration rate of the node $i \in N'^k$ in network $k \in K$
ε	An arbitrarily small positive number, $0 < \varepsilon < 1$
M	An arbitrarily large positive number

Table 3.2. Model decision variables.

m_{it}^k	Amount of demand met at node $i \in N_-^k$ in network $k \in K$ at 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_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is protected, binary
y_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is protected, binary

z_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is interdicted, binary
z_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is interdicted, binary
f_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is disrupted, binary
f_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is disrupted, binary
α_{ij}^k	Equal to 1 if link $(i,j) \in A'^k$ in network $k \in K$ is operational, binary
α_i^k	Equal to 1 if node $i \in N'^k$ in network $k \in K$ is operational, binary
α'^{kr}_{ijt}	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
α'^{kr}_{it}	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
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
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

3.2.3 Objective Function

As discussed in the previous section, the proposed tri-level defender-attacker-defender optimization model consists of three stages successively performing (i) defender protection actions to minimize network vulnerability, (ii) attacker interdiction actions to identify and pursue the most effective disruption, and (iii) subsequent defender actions to restore the networks after the disruption. In particular, the proposed protection-interdiction-restoration model aims to minimize the (weighted) fraction of unsupplied demand over the planning horizon. For this purpose, let us define $\zeta(t)$ as the weighted proportion of unmet demand (relative to the met demand before the disruption) at time t, as shown in Eq. (3.1), where m_{it}^k represents demand being met at node i in network k at time t, d_i^k represents the amount of demand met prior to the disruption at time t_e (from Figure 1.1), and w_{it}^k is the relative importance of node i in network k at time t. 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). As mentioned in Chapter 1, network performance at time t is represented with $\varphi(t)$ which equals to $1 - \zeta(t)$.

$$\zeta(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N^k_{\perp}} w^k_{it} m^k_{it}}{\sum_{k \in K} \sum_{i \in N^k_{\perp}} w^k_{it} d^k_i} \right) \qquad \forall \, \boldsymbol{t} \in \boldsymbol{T} \tag{3.1}$$

Then, the proposed objective function, which seeks to minimize the cumulative weighted fraction of unsupplied demand over the planning horizon for the worst-case disruption scenario, would be defined in Eq. (3.2).

$$\xi = \min_{y} \max_{\mathrm{z}} \min_{m,x,f,\alpha,\alpha',\beta} \sum_{t \in T} \zeta(t) \tag{3.2}$$

3.2.4 Protection and Interdiction Levels

Each stage of the model is represented by its own decision variables and is subject to a set of constraints correlating all three levels, such that the decision at each level is related to the decision made in the previous level. Constraint (3.3) is associated with the defense actions prior to a disruptive event, showing that the total cost of protecting components is limited by the protection budget available. There are multiple defense strategies discussed by various scholars to enhance the interdependent network resilience (Alderson et al., 2015; Ouyang & Fang, 2017). In this dissertation, we consider two pre-disruption strategies widely used in the literature, including hardening (protecting) the components and building redundant equipment as a backup utility (Alderson et al., 2011; G. Brown et al., 2006; Ouyang & Fang, 2017). Constraint (3.4) is related to the

interdictor actions to ensure that the total number of components that can be interdicted is constrained by the interdiction budget. Constraints (3.5)-(3.8) present the nature of the first and second level decision variables.

$$\sum_{k\in K}\sum_{(i,j)\in A'^{k}} CP_{ij}^{k}\, y_{ij}^{k} + \sum_{k\in K}\sum_{i\in N'^{k}} CP_{i}^{k}\, y_{i}^{k} \le BP \tag{3.3}$$

$$\sum_{k\in K}\sum_{(i,j)\in A'^{k}} CI_{ij}^{k}\, z_{ij}^{k} + \sum_{k\in K}\sum_{i\in N'^{k}} CI_{i}^{k}\, z_{i}^{k} \le BI \tag{3.4}$$

$$y_{ij}^{k} \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{3.5}$$

$$y_{i}^{k} \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.6}$$

$$z_{ij}^{k} \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{3.7}$$

$$z_{i}^{k} \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.8}$$

3.2.5 Restoration Level

This level of the model is related to the second defender actions to plan the restoration of interdicted components. In this level, the failure of each disrupted component and its operationality status is determined for the recovery process. Flow balance constraints enable decision variables in this restoration level to connect with the objective function. Therefore, restoration scheduling is automatically set to return the system of networks to a stable operation as rapidly as possible.

The restrictions associated with the restoration level comprise constraints (3.9)-(3.50). Constraints (3.9) and (3.10) generally deliver failure status for candidate links $A'^{k} \subseteq A^{k}$ and candidate nodes $N'^{k} \subseteq N^{k}$ respectively, depending on the protection and interdiction strategies. Constraints (3.11)-(3.14) determine the operationality status of

each link and node based on their failure, where the binary variable α is 1 when its associated link or node is operational (either protected or not interdicted) after the disruption. Constraints (3.15) and (3.16) ensure that operational links and nodes, respectively, are not restored. Constraints (3.17) and (3.18) state that nonoperational links and nodes cannot be functional at period 1, since they require at least one time unit to be reactivated. Constraints (3.19)-(3.22) represent the flow balance constraints at node $i \in N^k$ in infrastructure network $k \in K$ at time $t \in T$. Constraints (3.23) represent the capacity restriction for each link $(i,j) \in A^k$. Constraints (3.24)-(3.26) ensure that a positive flow through any given link can be attained at a period $t \in T$ only if such a link, along with its starting and ending nodes, are operational or were already recovered. Constraints (3.27) ensure that the restoration task of a disrupted link is continued without interruption once it has commenced. Likewise, constraints (3.30) accomplish this for a disrupted node. Constraints (3.28) and (3.29) calculate the total time that a specific work crew should be assigned to restore a nonoperational link. Note that constraints (3.28) and (3.29) together help to deliver integer value for the total required recovery time of an element. Similarly, constraints (3.31) and (3.32) calculate this time for a nonoperational disrupted node. Constraints (3.33) and (3.34) ensure that once the nonoperational disrupted link and node, respectively, are fully restored at time $t \in T$, they are labeled reactivated from the next period ($t + 1 \in T$) to the end of the time horizon of the model. Constraints (3.35) ensure that once the restoration of a disrupted link commences by a work crew at time $t \in T$, that specific work crew completes restoration of that link. Similarly, constraints (3.36) accomplish this same restriction for the disrupted nodes.

Constraints (3.37) and (3.38) state that, at the given time $t \in T$, only one work crew can work on the restoration task of a specific nonoperational disrupted link or node, respectively. Constraints (3.39) ensure that, at the given time $t \in T$, only one nonoperational disrupted component can be restored by a given work crew. Constraints (3.40) establish the interdependency among networks, ensuring that the positive flow through a link can be only available if their corresponding related parent nodes (in other networks) are operational. Finally, constraints (3.41)-(3.50) represent the nature of the decision variables for the restoration level.

$$y_{ij}^k + \left(1 - z_{ij}^k\right)\left(1 - y_{ij}^k\right) = 1 - f_{ij}^k \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{3.9}$$

$$y_i^k + \left(1 - z_i^k\right)\left(1 - y_i^k\right) = 1 - f_i^k \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.10}$$

$$\alpha_{ij}^k \le 1 - f_{ij}^k \qquad \forall\, k \in K, \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{3.11}$$

$$\alpha_{ij}^k + f_{ij}^k \ge \varepsilon \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{3.12}$$

$$\alpha_i^k \le 1 - f_i^k \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.13}$$

$$\alpha_i^k + f_i^k \ge \varepsilon \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.14}$$

$$\alpha_{ij}^k \le 1 - \beta_{ijt}^k \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K, \forall t \in T \tag{3.15}$$

$$\alpha_i^k \le 1 - \beta_{it}^k \qquad \forall\, i \in N'^k, \forall\, k \in K, \forall t \in T \tag{3.16}$$

$$\beta_{ij1}^k = 0 \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{3.17}$$

$$\beta_{i1}^k = 0 \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.18}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k \le s_i^k \qquad \forall\, i \in N_+^k, \forall\, k \in K, \forall\, t \in T \tag{3.19}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k = 0 \qquad \forall\, i \in N_=^k, \forall\, k \in K, \forall\, t \in T \tag{3.20}$$

$$\sum_{(i,j)\in A^k} x_{ijt}^k - \sum_{(j,i)\in A^k} x_{jit}^k = -m_{it}^k \qquad \forall\, i \in N_-^k, \forall\, k \in K, \forall\, t \in T \tag{3.21}$$

$$m_{it}^k \le d_i^k \qquad \forall\, i \in N_-^k, \forall\, k \in K, \forall\, t \in T \tag{3.22}$$

$$x_{ijt}^{k} \leq u_{ij}^{k} \qquad \forall\,(i,j) \in A^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.23}$$

$$x_{ijt}^{k} \leq u_{ij}^{k}\left(\alpha_{ij}^{k} + \beta_{ijt}^{k}\right) \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.24}$$

$$x_{ijt}^{k} \leq u_{ij}^{k}\left(\alpha_{i}^{k} + \beta_{it}^{k}\right) \qquad \forall\,(i,j) \in A^{k}, \forall\, i \in N'^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.25}$$

$$x_{ijt}^{k} \leq u_{ij}^{k}\left(\alpha_{j}^{k} + \beta_{jt}^{k}\right) \qquad \forall\,(i,j) \in A^{k}, \forall\, j \in N'^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.26}$$

$$\sum_{s=1}^{t} \alpha'^{kr}_{ijs} \leq M\left(1 - \left(\alpha'^{kr}_{ij(t+1)} - \alpha'^{kr}_{ijt}\right)\right) \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K, \forall\, t \in T, \forall\, r \in R^{k} \tag{3.27}$$

$$\sum_{r \in R^{k}} \sum_{t \in T} \alpha'^{kr}_{ijt} \geq \frac{f_{ij}^{k}}{\lambda_{ij}^{k}} - M\alpha_{ij}^{k} \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K \tag{3.28}$$

$$\sum_{r \in R^{k}} \sum_{t \in T} \alpha'^{kr}_{ijt} < \left(\frac{f_{ij}^{k}}{\lambda_{ij}^{k}} + 1\right) + M\alpha_{ij}^{k} \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K \tag{3.29}$$

$$\sum_{s=1}^{t} \alpha'^{kr}_{is} \leq M\left(1 - \left(\alpha'^{kr}_{i(t+1)} - \alpha'^{kr}_{it}\right)\right) \qquad \forall\, i \in N'^{k}, \forall\, k \in K, \forall\, t \in T, \forall\, r \in R^{k} \tag{3.30}$$

$$\sum_{r \in R^{k}} \sum_{t \in T} \alpha'^{kr}_{it} \geq \frac{f_{i}^{k}}{\lambda_{i}^{k}} - M\alpha_{i}^{k} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.31}$$

$$\sum_{r \in R^{k}} \sum_{t \in T} \alpha'^{kr}_{it} < \left(\frac{f_{i}^{k}}{\lambda_{i}^{k}} + 1\right) + M\alpha_{i}^{k} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.32}$$

$$\frac{\sum_{r \in R^{k}} \sum_{s=1}^{t-1} \alpha'^{kr}_{ijs}}{f_{ij}^{k}/\lambda_{ij}^{k}} \geq \beta_{ijt}^{k} \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K, \forall\, t \in T \mid t \neq 1 \tag{3.33}$$

$$\frac{\sum_{r \in R^{k}} \sum_{s=1}^{t-1} \alpha'^{kr}_{is}}{f_{i}^{k}/\lambda_{i}^{k}} \geq \beta_{it}^{k} \qquad \forall\, i \in N'^{k}, \forall\, k \in K, \forall\, t \in T \mid t \neq 1 \tag{3.34}$$

$$\sum_{s \in R^{k}} \sum_{t \in T} \alpha'^{ks}_{ijt} \leq M\left(1 - \alpha'^{kr}_{ijt}\right) \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K, \forall\, t \in T, \forall\, r \in R^{k} \tag{3.35}$$

$$\sum_{\substack{s \in R^{k} \\ s \neq r}} \sum_{t \in T} \alpha'^{ks}_{it} \leq M\left(1 - \alpha'^{kr}_{it}\right) \qquad \forall\, i \in N'^{k}, \forall\, k \in K, \forall\, t \in T, \forall\, r \in R^{k} \tag{3.36}$$

$$\sum_{\substack{r \in R^{k} \\ s \neq r}} \alpha'^{kr}_{ijt} \leq 1 \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.37}$$

$$\sum_{r \in R^{k}} \alpha'^{kr}_{it} \leq 1 \qquad \forall\, i \in N'^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.38}$$

$$\sum_{(i,j) \in A'^{k}} \alpha'^{kr}_{ijt} + \sum_{i \in N'^{k}} \alpha'^{kr}_{it} \leq 1 \qquad \forall\, t \in T, \forall\, k \in K, \forall\, r \in R^{k} \tag{3.39}$$

$$x_{ijt}^{k} \le u_{ij}^{k}\left(\alpha_{\bar{\imath}}^{\bar{k}} + \beta_{\bar{\imath}t}^{\bar{k}}\right) \qquad \forall (i,j) \in A^{k}, \forall \bar{\imath} \in N'^{\bar{k}} \mid \left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi or \left((j,k),(\bar{\imath},\bar{k})\right) \in \Psi, \forall k, \bar{k} \in K, \forall t \in T \tag{3.40}$$

$$m_{it}^{k} \ge 0 \qquad \forall i \in N_{-}^{k}, \forall k \in K, \forall t \in T \tag{3.41}$$

$$x_{ijt}^{k} \ge 0 \qquad \forall (i,j) \in A^{k}, \forall k \in K, \forall t \in T \tag{3.42}$$

$$f_{ij}^{k} \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{3.43}$$

$$f_{i}^{k} \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K \tag{3.44}$$

$$\alpha_{ij}^{k} \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{3.45}$$

$$\alpha_{i}^{k} \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K \tag{3.46}$$

$$\alpha'^{kr}_{ijt} \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T, \forall r \in R^{k} \tag{3.47}$$

$$\alpha'^{kr}_{it} \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K, \forall t \in T, \forall r \in R^{k} \tag{3.48}$$

$$\beta_{ijt}^{k} \in \{0,1\} \qquad \forall (i,j) \in A'^{k}, \forall k \in K, \forall t \in T \tag{3.49}$$

$$\beta_{it}^{k} \in \{0,1\} \qquad \forall i \in N'^{k}, \forall k \in K, \forall t \in T \tag{3.50}$$

Before implementing the proposed solution algorithm, nonlinear constraints (3.9), (3.10), (3.33), and (3.34) are linearized. To linearize constraints (3.9) and (3.10), we define three different sets of linear constraints (Taha, 1998). Following this idea, constraint (3.9) can be replaced by constraints (3.51)-(3.53).

$$y_{ij}^{k} + \left(1 - z_{ij}^{k}\right) + f_{ij}^{k} \ge 1 \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{3.51}$$

$$f_{ij}^{k} \le z_{ij}^{k} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{3.52}$$

$$y_{ij}^{k} \le 1 - f_{ij}^{k} \qquad \forall (i,j) \in A'^{k}, \forall k \in K \tag{3.53}$$

Similarly, constraint (3.10) can be replaced by constraints (3.54)-(3.56).

$$y_i^k + \left(1 - z_i^k\right) + f_i^k \geq 1 \qquad \forall\, i \in N'^k\,, \forall\, k \in K \tag{3.54}$$

$$f_i^k \leq z_i^k \qquad \forall\, i \in N'^k\,, \forall\, k \in K \tag{3.55}$$

$$y_i^k \leq 1 - f_i^k \qquad \forall\, i \in N'^k\,, \forall\, k \in K \tag{3.56}$$

Finally, by adopting the big-M method (Taha, 1998), constraints (3.33) and (3.34) can be replaced by constraints (3.57) and (3.58).

$$1 - \left(\frac{\frac{f_{ij}^k}{\lambda_{ij}^k} - \sum_{r \in R^k} \sum_{s=1}^{t-1} \alpha'^{kr}_{ijs}}{M} \right) \geq \beta_{ijt}^k \qquad \forall\, (i,j) \in A'^k, \forall\, t \in T \mid t \neq 1\,, \forall\, k \in K \tag{3.57}$$

$$1 - \left(\frac{\frac{f_i^k}{\lambda_i^k} - \sum_{r \in R^k} \sum_{s=1}^{t-1} \alpha'^{kr}_{is}}{M} \right) \geq \beta_{it}^k \qquad \forall\, i \in N'^k, \forall\, t \in T \mid t \neq 1, \forall\, k \in K \tag{3.58}$$

Parameter M in constraints (3.27)-(3.32) and (3.57)-(3.58) only needs to be greater than the maximum required time for restoring the disrupted components.

To provide some insight regarding the complexity of the proposed model, Table 3.3 represents the total number of decision variables and constraints for each level of the proposed model in terms of the model indices.

Table 3.3. The number of decision variables and constraints in the model.

Model	Number of variables	Number of constraints
Protection	$\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert)$	$\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert) + 1$
Interdiction	$\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert)$	$\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert) + 1$
Restoration	$\lvert T\rvert\left(\sum_{k\in K}\left[\lvert N_d^k\rvert + \lvert A^k\rvert + (\lvert R^k\rvert + 1)(\lvert N'^k\rvert + \lvert A'^k\rvert)\right]\right) + 2\left(\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert)\right)$	$\lvert T\rvert\left(\sum_{k\in K}[3\lvert N_d^k\rvert + 2\lvert A^k\rvert + \lvert R^k\rvert + \lvert N_s^k\rvert + (3\lvert R^k\rvert + 5)\lvert A'^k\rvert + (3\lvert R^k\rvert + 6)\lvert N'^k\rvert]\right) + 10\left(\sum_{k\in K}(\lvert N'^k\rvert + \lvert A'^k\rvert)\right)$

3.3 Solution Approach

A common approach to solve a multi-level network interdiction model is decomposition (Israeli, 1999; Alderson et al., 2011; Israeli & Wood, 2002). With this approach, the multi-level problem is generally transformed into a master problem and a subproblem, where an optimal solution is found by iteratively solving these two problems. There are various types of decomposition approaches, which depend on the form of transformation of the original model and the type of solution elimination inequalities used (Zeng & Zhao, 2013; Alderson et al., 2011; Israeli & Wood, 2002; Israeli, 1999). Given that the lower level of our proposed model is a mixed integer problem, solution methods based on finding the dual of the inner level and merging the other two levels as a single optimization are not applicable since the Karush-Kuhn-Tucker sufficient condition is not satisfied (Gedik et al., 2014; Ouyang & Fang, 2017; Zeng & Zhao, 2013). Given the general features of our model and the different types of decomposition approaches found in literature, we implement a decomposition approach that extends the standard covering decomposition method discussed by Israeli and Wood

(2002). In this algorithm, the smaller nested bi-level problems are iteratively solved, and once the problems become infeasible, the algorithm is terminated. In the standard covering decomposition approach, the subproblem is fundamentally feasibility seeking problem (Israeli, 1999; Israeli & Wood, 2002; Yao et al., 2007). To solve our proposed tri-level model, we modified the subproblems of the standard decomposition algorithm from feasibility seeking problems to optimization problems that maximize the number of protected and interdicted components (in the objective functions of protector and interdictor algorithms, respectively) subject to the budget available. This modification reduces the expected computation time of the algorithm by reducing the number of combinations needed to cover the full space of solutions. Note that, thanks to the particular structure of the proposed tri-level model, this modified covering decomposition algorithm still provides optimality guarantees. This is due to the fact that, for the defender in our model, protecting a given set of components will never be worse than protecting only a subset of such components. Similarly, for the attacker, interdicting a given set of components will never be worse than interdicting only a subset of such components.

3.3.1 Modified Covering Decomposition Algorithm

To implement the modified covering decomposition algorithm, the tri-level model is divided into three different subproblems associated with each level of the model: (i) the Relaxed Protection Problem (RPP), the Relaxed Interdiction Problem (RIP), and the Relaxed Restoration Problem (RRP). Each subproblem is defined by its corresponding decision variables and is subject to its associated constraints in the complete protection-interdiction-restoration model. As discussed earlier, in this modified covering

decomposition approach, the RPP and RIP are defined as maximization problems (instead of feasibility seeking problems). In particular, the objective function of the RPP maximizes the number of protected components, giving priority to components that were interdicted. Similarly, the objective function of the RIP maximizes the number of interdicted components, giving priority to components that were not protected. To model these priorities, for the RPP, protecting a component that was interdicted is considered preferable to protecting all components that were not interdicted. Likewise, for the RIP, interdicting a component that was not protected is considered preferable to interdicting all components that were protected. As such, for both the RPP and the RIP, we give the components with priority a weight $\sum_{k\in K}\left(\left|N'^{k}\right|+\left|A'^{k}\right|\right)+1$, where $\sum_{k\in K}\left(\left|N'^{k}\right|+\left|A'^{k}\right|\right)$ corresponds to the total number of components in the system subject to protection or interdiction. The three problems associated with each level of the model are defined as follows.

Relaxed Protection Problem (RPP):

$$\max_{y}\left(\sum_{k\in K}\left(\left|N'^{k}\right|+\left|A'^{k}\right|\right)+1\right)\left(\sum_{k\in K}\sum_{(i,j)\in A'^{k}|z_{ij}^{k}=1}y_{ij}^{k}+\sum_{k\in K}\sum_{i\in N'^{k}|z_{i}^{k}=1}y_{i}^{k}\right)$$
$$+\left(\sum_{k\in K}\sum_{(i,j)\in A'^{k}|z_{ij}^{k}=0}y_{ij}^{k}+\sum_{k\in K}\sum_{i\in N'^{k}|z_{i}^{k}=0}y_{i}^{k}\right)$$

Subject to:

$$\sum_{k\in K}\sum_{(i,j)\in A'^{k}}CP_{ij}^{k}\,y_{ij}^{k}+\sum_{k\in K}\sum_{i\in N'^{k}}CP_{i}^{k}\,y_{i}^{k}\leq BP$$

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

Relaxed Interdiction Problem (RIP):

$$\max_{z} \left(\sum_{k \in K} \left(\left| N'^{k} \right| + \left| A'^{k} \right| \right) + 1 \right) \left(\sum_{k \in K} \sum_{(i,j) \in A'^{k} | y_{ij}^{k} = 0} z_{ij}^{k} + \sum_{k \in K} \sum_{i \in N'^{k} | y_{i}^{k} = 0} z_{i}^{k} \right) + \left(\sum_{k \in K} \sum_{(i,j) \in A'^{k} | y_{ij}^{k} = 1} z_{ij}^{k} + \sum_{k \in K} \sum_{i \in N'^{k} | y_{i}^{k} = 1} z_{i}^{k} \right)$$

Subject to:

$$\sum_{k \in K} \sum_{(i,j) \in A'^{k}} CI_{ij}^{k} \, z_{ij}^{k} + \sum_{k \in K} \sum_{i \in N'^{k}} CI_{i}^{k} \, z_{i}^{k} \leq BI$$

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

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

Relaxed Restoration Problem (RRP):

$$\min_{m,x,f,\alpha,\alpha',\beta} \sum_{t \in T} \zeta(t)$$

Subject to:

Constraints (3.9)-(3.50)

The modified covering decomposition algorithm consists of two different algorithms, both protection and interdiction, which are solved iteratively. The purpose of the first algorithm is to solve the protection problem for an optimal solution set Y^{*} and objective value $\bar{P}$, and it begins with the initial feasible solution such that no components are protected ($Y^{s} = 0$ is the initial solution set for the protection problem). Since the protection problem is a relaxed problem in comparison with the complete tri-level model,

its algorithm provides an upper bound value for the objective function RRP (Yuan et al., 2014; Zeng & Zhao, 2013). The purpose of the second algorithm is to solve the interdiction problem for an optimal solution set Z^* and objective value $\underline{P}$. Like the protection problem, the interdiction algorithm begins with the initial feasible solution set $Z^s = 0$, meaning that there are no attacked components at this step. Mentioned previously, the interdiction model is also a relaxed problem, and its algorithm provides a lower bound value for the objective function RRP (Yuan et al., 2014; Zeng & Zhao, 2013).

Note that at each iteration, a constraint known as the super-valid inequality is added to RPP and RIP to tighten the feasible region until problems become infeasible and algorithms are terminated. This inequality enables the interdiction algorithm to find at least one component to be interdicted at each iteration subject to the interdictor budget availability. However, this inequality in the protection algorithm helps the model to minimize the effect of disruption by protecting at least one interdicted component at each iteration until the protector budget is spent. Due to the budget restriction for the protector, at one iteration, RPP cannot satisfy all cuts added to the model, and it becomes infeasible. In other words, the protector cannot cover all attacked components at this iteration, and the whole algorithm is terminated with the optimal defense plan Y^* and optimal attack plan Z^*.

At each iteration, both protection and interdiction algorithms try to keep the best solution in their records by solving RRP while comparing the objective value with the previous iteration (referring to steps 7 and 8 and steps 8 and 9 for protection and

interdiction algorithms respectively). The interdictor tends to find the larger value of RRP at each iteration to decrease the resilience of the set of networks. On the other hand, the protector tries to find the smaller value of RRP to improve the resilience of the system. The implementation steps of the algorithm are presented as follows.

Algorithm 1: Protection algorithm

Input:

BP $\Longrightarrow$Total available budget for the protector

$CP_{ij}^{k}, (i,j) \in A'^{k}, k \in K$ $\Longrightarrow$ Cost of protecting each link

$CP_{i}^{k}, i \in N'^{k}, k \in K$ $\Longrightarrow$ Cost of protecting each node

1. **If** protector budget is enough to protect all components subject to be attacked ($N'^{k} \cup A'^{k}$) **then**
2. $Y^{*} \leftarrow 1, Z^{*} \leftarrow 0, \bar{P} = \underline{P} \leftarrow 0$ and go to step 15
3. Create initial RPP; $s \leftarrow 1$, $Y^{s} \leftarrow 0$ and $\bar{P} \leftarrow \infty$
4. **While** $Y^{s} \neq \emptyset$ **do** (the RPP is feasible)
5. Solve **Algorithm 2** for Z^{*} and objective value $\underline{P}$ (Referring to the **Algorithm 2**)
6. $P^{s} \leftarrow \underline{P}$
7. **If** $P^{s} < \bar{P}$ **then**
8. $Y^{*} \leftarrow Y^{s}$ and $\bar{P} \leftarrow P^{s}$
9. **If** $Z^{*} = 0$ **then**
10. Solve **RPP** for Y^{*} and go to step 15
11. Add the following cut to **RPP**:

$$\sum_{k \in K} \sum_{(i,j) \in A'^{k} | z_{ij}^{*k} = 1} y_{ij}^{k} + \sum_{k \in K} \sum_{i \in N'^{k} | z_{i}^{*k} = 1} y_{i}^{k} \geq 1$$

12. $s \leftarrow s + 1$
13. Solve **RPP** for Y^{s}
14. Solve **Algorithm 2** for Z^{*} and objective value $\underline{P}$ (Referring to the **Algorithm 2**)
15. **Return** Y^{*}, Z^{*} (optimal solution with objective value $\bar{P} = \underline{P}$)

Algorithm 2: Interdiction algorithm

Input:

BI $\Longrightarrow$Total available budget for the interdictor

$CI_{ij}^{k}, (i,j) \in A'^{k}, k \in K$ $\Longrightarrow$ Cost of interdicting each link

$CI_{i}^{k}, i \in N'^{k}, k \in K$ $\Longrightarrow$ Cost of interdicting each node

1. **If** attacker budget is enough to interdict all components subject to be attacked ($N'^{k} \cup A'^{k}$) **then**
2. $z^{*} \leftarrow 1 | y^{s} = 0$ and $z^{*} \leftarrow 0 | y^{s} = 1$
3. Solve **RRP** for objective value P^{s}
4. $\underline{P} \leftarrow P^{s}$ and go to step 13
5. Create initial RIP; $s \leftarrow 1$, $Z^{s} \leftarrow 0$ and $\underline{P} \leftarrow -\infty$
6. **While** $Z^{s} \neq \emptyset$ **do** (the RIP is feasible)
7. Solve **RRP** for objective value P^{s}
8. **If** $P^{s} > \underline{P}$ **then**
9. $Z^{*} \leftarrow Z^{s}$ and $\underline{P} \leftarrow P^{s}$
10. Add the following cut to **RIP**

$$\sum_{k \in K} \sum_{(i,j) \in A'^{k} | z_{ij}^{sk} = 0} z_{ij}^{k} + \sum_{k \in K} \sum_{i \in N'^{k} | z_{i}^{sk} = 0} z_{i}^{k} \geq 1$$

11. $s \leftarrow s + 1$
12. Solve **RIP** for Z^{s}
13. **Return** Z^{*} (optimal solution and its objective value $\underline{P}$)

3.4 Illustrative Example: Interdependent Networks in Shelby County, TN

To illustrate the application and capabilities of the proposed model, we study the system of water, gas, and power networks in Shelby County, TN, USA. Figure 3.2 shows the general illustration of (a) the water, (b) gas, and (c) power networks individually, along with (d) their superposition (adapted from González et al., 2016).

As mentioned in Section 3.1, this model considers the physical interdependency for networks in which the functionality of a set of nodes in one or more networks enable the functionality of a node in another network. In this case study, the power is dependent on the water network, which enables cooling in the power network (Zhang et al., 2016). The interdependent system of networks consists of 125 nodes and 164 links. Table 3.4 presents the general structure of the network components particularly in this case study. In the water network, storage tanks and water pumps represent demand and supply nodes, respectively, and water pipelines are considered as the links. For the power network, gate stations (customers or loads) are demand nodes, and substations (generators) are supply nodes, where the power transmission lines are the links. For the gas network, pipelines and gas distribution stations represent links and nodes, respectively.

For the experiment, to solve each instance we used Python 3.6.5 with Gurobi 8.0.1, on a 64-bit Intel® Core ™ m3-6Y30 CPU @ 0.90GHZ laptop computer.

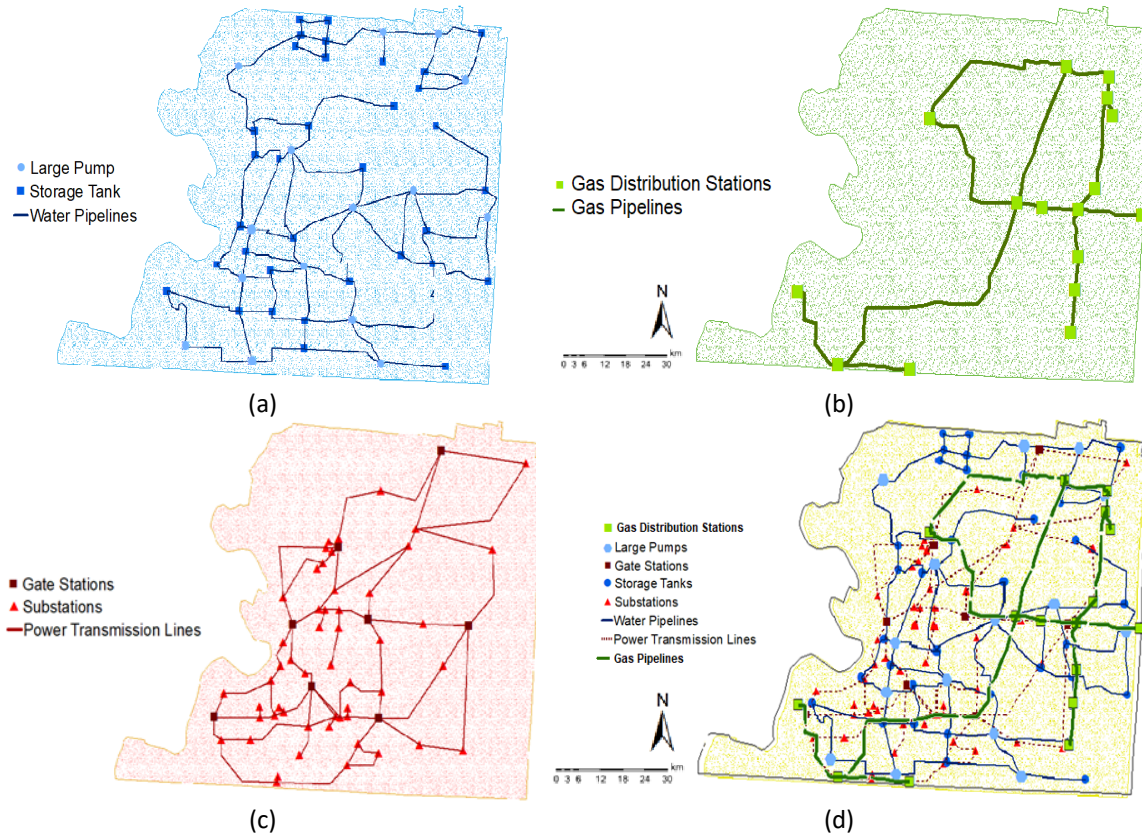


Figure 3.2. General depiction of the (a) water, (b) gas, and (c) power networks, and (d) the interdependency among networks in Shelby County, TN (adapted from González et al. (2016))

Table 3.4. General formation of the water, gas, and power networks components in Shelby County, TN.

Network	Nodes	Supply nodes	Demand nodes	Links
Water	49	34	15	71
Gas	16	3	13	17
Power	60	37	8	76

3.4.1 Critical Components

In this computational experiment, we assume that nodes are the only components that can be interdicted. Also, to determine the set of nodes subject to be attacked, N'^{k}, we selected the most critical nodes based on their degree (i.e., the number of connections to other nodes). Table 3.5 shows the average node degree for each network as well as the

number of candidate nodes that can be interdicted or protected in this experiment (nodes with degree greater than or equal 3 are selected). Note that the interdependency relationships between networks are not considered for the node degree calculation, and the degree of every node $i \in N$ is defined as the number of actual connections it has with other nodes in the network. While a topological approach to determine the set N'^{k} (component criticality) was used in this experiment, other approaches could be explored to perhaps more effectively capture the importance of components to the performance of the networks (e.g., flow-based component importance measures, (Almoghathawi et al., 2017; Nicholson et al., 2016; Rocco et al., 2010; Wang et al., 2012, 2013)). In addition, Boccaletti et al. (2014) characterized the structure of multilayer networks and studied parameters that determine the structural relevance of each node (e.g., node degree, closeness, betweenness) for multilayer networks in particular.

Table 3.5. The number of candidate components of the water, gas, and power networks in Shelby County, TN.

Network	Node No.	⟨deg⟩
Water	20	1.92
Gas	3	1.93
Power	10	1.87

3.4.2 Model Parameters

At the time of crisis, the timely restoration of the water network is highly emphasized, as the loss of clean drinking water and sanitation infrastructure can significantly endanger millions of humans' lives (American Water Works Association, 2011; Ozcelik, 2017). In addition, recovery of water and sanitation facilities are generally less expensive than other systems that simultaneously enable the functionality of other

dependent systems at the lowest cost (Grogan & Tserenkhuu, 2018). In this case study, the power network depends on the water network for operation. Furthermore, according to Karakoc et al. (2019), demand nodes in the water network in Shelby County are generally located in the more socially vulnerable areas. Therefore, for the weight assigned to demand nodes, w_{it}^{k}, we give more relative priority to the water network, with equal weights given to demand nodes within each network individually. For the cost of protecting and interdicting links and nodes, and restoration rate for each component, we consider the following distributions for experimental purposes (Almoghathawi et al., 2019): $CP_{ij}^{k}, CP_{i}^{k} \sim U(20, 40)$, $CI_{ij}^{k}, CI_{i}^{k} \sim U(50, 70)$, $\lambda_{ij}^{k}, \lambda_{i}^{k} \sim U(0.1, 1)$. Note that these parameters can vary by the network. In this dissertation, 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_{ij}^{k} and λ_{i}^{k}, can be also indexed by the type of work crews available at each network. Finally, the time horizon was chosen to be $T = \{1, \dots, 20\}$. Different scenarios account for the resource available for protector and interdictor as discussed in the computational results section. According to Table 3.3, the total number of decision variables and constraints of the tri-level model for this example are 6706 and 20490, respectively.

3.4.3 Computational Results

Since the proposed tri-level model accounts for both vulnerability reduction and recoverability enhancement, respectively, through the first and second defender actions, the number of available work crews affect the protector's plan to neutralize the interdictor's decision. Hence, the model can be solved for different scenarios with respect

to the number of available work crews, for example: (i) a single work crew for each interdependent network in which restoration tasks cannot start simultaneously, therefore components are consecutively assigned to the single work group with respect to their priority, and (ii) multiple work crews in which all or some disrupted components (depending on the number of available work crews for each interdependent network) can begin to be recovered immediately after the disruption in a parallel manner. In the following, we present outcomes of the algorithm for the single work crew scenario in detail.

Table 3.6 shows an optimal solution for the protection-interdiction-restoration model and results of each step until the protector algorithm is infeasible, by considering protection and interdiction budgets of 160 and 210, respectively. The notation (k, i) used to describe the components in Table 3.6 refers to node $i \in N'^{k}$ in network $k \in K$, where water, gas, and power networks are denoted by 1, 2, and 3, respectively. The values shown in the right column correspond to the upper bounds of the objective function calculated at each step, using their respective protection and interdiction strategies. In each step, the interdictor offers the most disruptive combination with respect to its budget and the current protection plan. Subsequently, the protector seeks the best strategy to counter the attacker's decision in an effective way, for which the interdictor again offers the corresponding most disruptive plan. The table shows how the upper bound decreases until the model has no additional feasible solution to check, thus guaranteeing that an optimal solution to the tri-level model has been found (the protection and interdiction

strategies described in step 26, as the solutions in steps 27-29 did not improve the upper bound).

Table 3.6. Interdictor and protector decisions in each step of the algorithm.

Protection step	Protected components	Interdicted components	Upper bound
Step 1	{-}	{(3,2), (3,6), (3,15)}	1.21
Step 2	{(1,16), (2,14), (3,2), (3,6), (3,15)}	{(1,5), (1,9), (1,26)}	0.77
Step 3	{(1,5), (1,9), (1,26), (2,14), (3,2)}	{(3,7), (3,6), (3,15)}	0.647
Step 5	{(1,5), (1,9), (2,14), (3,2), (3,7)}	{(1,26), (1,16), (3,6)}	0.646
Step 6	{(1,16), (1,26), (2,14), (3,2), (3,6)}	{(1,9), (1, 5), (2, 6)}	0.54
Step 9	{(1,5), (1,26), (2,14), (3,2), (3,7)}	{(2,6), (3,6), (3,15)}	0.52
Step 20	{(1,5), (1,26), (2,14), (3,2), (3,15)}	{(2,6), (3,6), (3,7)}	0.50
Step 26	{(1,5), (1,26), (2,14), (3,2), (3,6)}	{(1, 9), (1, 16), (2, 6)}	0.47
Step 30	Model is infeasible	-	-

By considering the particular protection and interdiction budgets of 160 and 210, we can conclude that by protecting nodes 5 and 26 in the water network, 14 in the gas network, and 2 and 6 in the power network, we would minimize the disruptive effects of the interdiction.

As shown in step 1 (Table 3.6), since the value of the objective function (which refers to the weighted summation of unmet demand over time) is 1.21 in absence of a protection strategy, we can conclude that the worst-case interdiction effects are reduced approximately 60% by adding the first defender level (i.e., protection of components).

This shows the value of using the proposed tri-level model as opposed to a bi-level interdiction-restoration model, emphasizing how pre-disruption investments to harden critical network components are imperative to enhance the resilience of the system.

Figure 3.3 shows network performance trajectories of water, gas and power networks for the optimal solution discussed in Table 3.6. In the initial step, there is a drop in the performance of each network after the interdiction. Then, the restoration procedure begins until the whole system is fully recovered. The optimal interdictor plan deals with nodes 9 and 16 in the water network and node 6 in the gas network. Although no element in the power network is interdicted, its corresponding performance is less than 1 until time 3. It is because of the interdependency between node 9 in the power network and node 16 in the water network for the functionality. Thus, demand nodes in the power network are not fully satisfied until its dependent nodes in the water network become operational which is at time 3. The whole system returns to its normal operation at time 5.

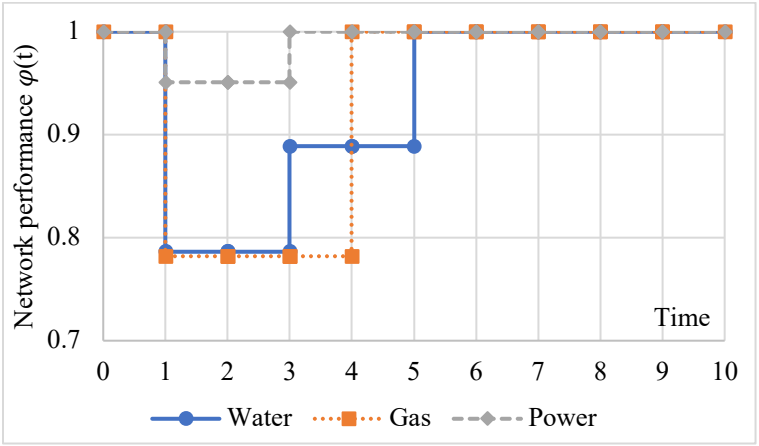


Figure 3.3. Network performance ($\varphi(t)$) trajectories of water, gas, and power networks.

The number of components that can be protected or interdicted varies according to the amount of budget available for the protector and the interdictor. Hence, by altering the budget parameter in the model, planners can effectively assess the best pre-disruption strategies with respect to budgetary constraints. Table 3.7 illustrates the optimal protection, SP, and interdiction, SI, strategies under a protector budget of 0 to 160 and interdictor budget of 70 to 350. Note that maximum budget required for defending and interdicting a component is 40 and 70, respectively. As such, under a protector budget of 160 and a defender budget of 350, at least four components can be protected and five components can be interdicted (Yuan et al., 2014).

Table 3.7. Protection and interdiction decisions under different budget scenarios.

BP	*BI* = 70	*BI*= 140	*BI*= 210	*BI* = 280	*BI*= 350
0	*SI*: (3,2) *SP*: -	*SI*: (3,2), (3,6) *SP*: -	*SI*: (3,2), (3,6), (3,15) *SP*: -	*SI*: (3,2), (3,6), (3,15), (3,7), (1,46) *SP*: -	*SI*: (3.2), (3,6), (3,15), (3,7), (2,6), (1,26) *SP*: -
40	*SI*: (1,26) *SP*: (3,2)	*SI*: (1,26), (1,5) *SP*: (3,2)	*SI*: (1,26), (1,5), (1, 16) *SP*: (3,2)	*SI*: (1,26), (1,5), (1,16), (1,9) *SP*: (3,2)	*SI*: (1,26), (1,5), (1,16), (1,9), (2,14) *SP*: (3,2)
80	*SI*: (2,14) *SP*: (3,2), (1,26)	*SI*: (1,5), (1,16) *SP*: (3,2), (1,26)	*SI*: (1,5), (1,16), (1,9) *SP*: (3,2), (1,26)	*SI*: (1,5), (1,16), (1,9), (2,14) *SP*: (3,2), (1,26)	*SI*: (1,5), (1,16), (1,9), (2,14), (2,6) *SP*: (3,2), (1,26)
120	*SI*: (3,6) *SP*: (1,5), (1,26), (2,14), (3,2)	*SI*: (3,6), (3,15) *SP*: (1,5), (1,26), (2,14), (3,2)	*SI*: (1,5), (2,6), (2,14) *SP*: (1,26), (3,2), (1,16), (3,15)	*SI*: (1,5), (2,6), (2,14), (1,9) *SP*: (1,26), (3,2), (1,16), (3,6)	*SI*: (1,5), (2,6), (2,14), (1,9), (3,15) *SP*: (1,26), (3,2), (1,16), (3,6)

160	*SI*: (2,6) *SP*: (1,5), (1,26), (2,14), (3,2), (3,6)	*SI*: (1,9), (1,16) *SP*: (1,5), (1,26), (2,14), (3,2), (3,6)	*SI*: (1,9), (1,16), (2,6) *SP*: (1,5), (1,26), (2,14), (3,2), (3,6)	*SI*: (1,9), (1,16), (3,7), (3,15) *SP*: (1,5), (1,26), (2,14), (3,2), (3,6)	*SI*: (1,9), (1,16), (3,7), (3,15), (2,6) *SP*: (1,5), (1,26), (2,14), (3,2), (3,6)

Table 3.8 shows the objective value for the optimal solution corresponding to each budget scenario, and Figure 3.4 illustrates the trend of objective value changes under different protector and interdictor budget scenarios. The trend suggests that by adding defensive resources, the system resilience measure over time regularly improves. Specifically, for a given protector budget, the objective value deteriorates as the amount of budget available for the attacker increases. In other words, the summation of unmet demand over the time in the system continues to increase as the attacker can interdict more components. On the other hand, for a given attacker budget, the objective value continues to improve as the protector budget grows. For example, when the attacker budget is 350, the summation of system performance over time improves by more than 60%, from 1.98 to 0.76, by increasing the protection budget from 0 to 160. Note that as the protector budget increases, the effect of interdictor continues to reduce. The length of vertical dashed lines represents this relationship for each protector budget. As it can be seen, there is a less substantial difference among objective values for different interdictor budgets while protector budget is 160.

Table 3.8. Objective value (ξ) under different budget scenarios.

BP	*BI* = 70	*BI* = 140	*BI* = 210	*BI* = 280	*BI*= 350
0	0.51	0.87	1.21	1.64	1.98
40	0.22	0.53	0.94	1.23	1.43
80	0.19	0.45	0.71	0.91	1.14
120	0.16	0.37	0.61	0.81	0.92
160	0.15	0.32	0.47	0.61	0.76

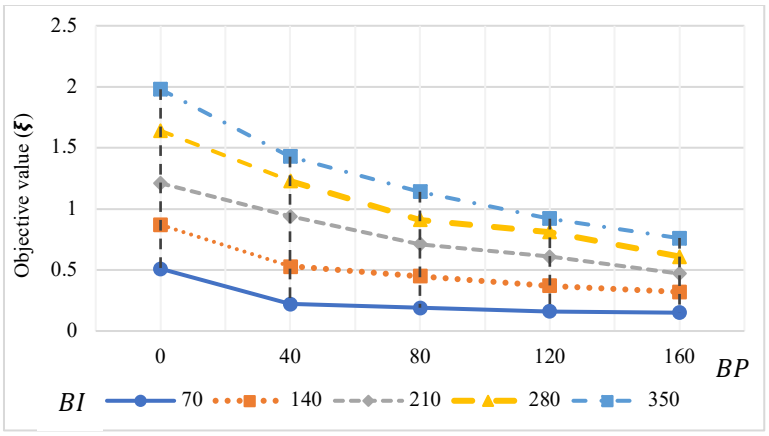


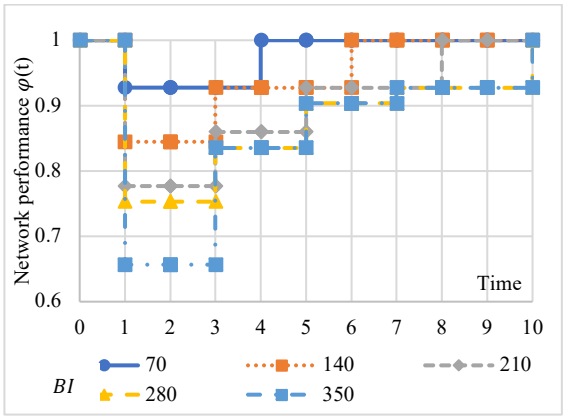
Figure 3.4. Change of objective value (ξ) under different budget scenarios.

Table 3.9 shows the proportion of network performance immediately after failure, $t = 1$, for the optimal solution corresponding to its budget scenario when the restoration process has not yet commenced. Clearly, the proportion of the system vulnerability at time $t = 1$ does not necessarily reduce by increasing the defender budget. For example, for BI=210, although the protector budget increases from 80 to 120, system vulnerability does not mitigate. This is because in the objective function in Eq. (3.2), the restoration process over time is also considered. Thus, 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 interdictors' 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 also does not only defend those components that result in the highest vulnerability reduction immediately after interdiction, but also simultaneously considers those components that require more restoration time.

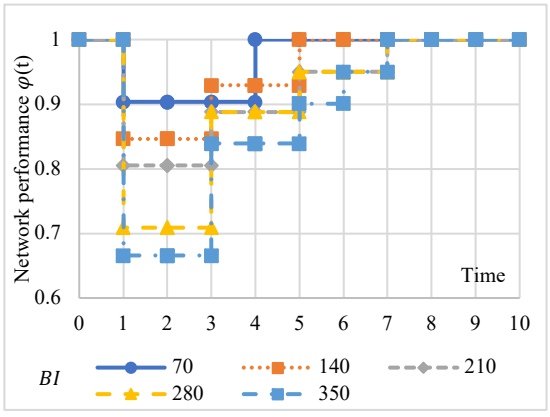
Table 3.9. Network performance ($\varphi(t=1)$) immediately after failure for different budget scenarios.

BP	*BI*= 70	*BI* = 140	*BI* = 210	*BI* = 280	*BI* = 350
0	0.93	0.88	0.83	0.78	0.67
40	0.93	0.84	0.78	0.75	0.66
80	0.90	0.85	0.81	0.71	0.67
120	0.95	0.89	0.77	0.72	0.66
160	0.95	0.89	0.84	0.79	0.74

Figure 3.5 illustrates the trajectories of network performance under different interdictor resources for protector budgets of (a) 40, (b) 80, (c) 120, and (d) 160. As the budget available to the protector increases, the system returns to its normal operation faster. Further, for protector budgets of 120 and 160, the system is fully restored at $t = 6$ and $t = 5$, respectively, for all interdictor budget scenarios except for *BI*=70, indicating that growth in protection resources would make the interdictor action ineffective regardless of the budget spent.



(a)



(b)

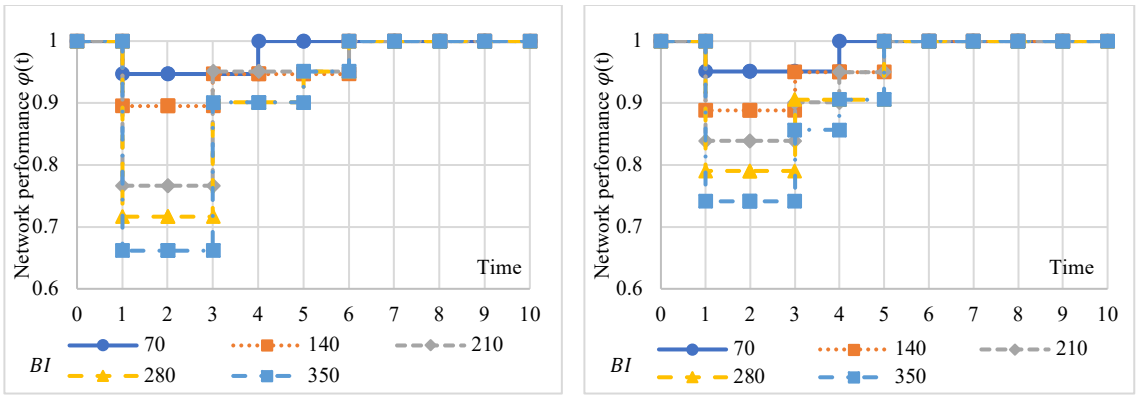


Figure 3.5. Trajectories of network performance ($\varphi(t)$) for protection budgets of (a) 40, (b) 80, (c) 120, and (d) 160.

To showcase the value of the proposed tri-level model with respect to a bi-level model, we compare protection plans suggested by the two models and their corresponding objective values. The bi-level interdiction-restoration model is constructed by setting the protector budget to zero in constraint (3.3). Table 3.10 shows protected components and the objective value for three different protection states: (i) no protection, (ii) protection based on the bi-level model, and (iii) protection based on the tri-level model. In the first case, the bi-level model is solved to find the most destructive plan under different interdictor budgets (no components are protected in this case). In the second case, interdicted components are protected, and the bi-level model is solved again to obtain the worst-case interdiction decision under current protection plan. In the third case, the complete tri-level model is solved to find the optimum protection plan with the same protector budget considered in the second case (Brown, et al., 2006; Yao et al., 2007). According to the results, both bi-level and tri-level models provide better (lower) objective value with respect to no protection case. For example, for the attacker budget

210, the objective value decreases by around 25%, from 1.21 to 0.94, by protecting interdicted components in the bi-level model. However, the tri-level model reduces this value from 1.21 to 0.65 which shows 85% improvement in compared to the second case. As the interdictor budget continues to increase, the tri-level model substantially outperforms the bi-level model.

Table 3.10. Comparison between bi-level and tri-level models.

BI	No protection	Bi-level model		Tri-level model	
	Objective value (ξ)	Protected components	Objective value (ξ)	Protected components	Objective value (ξ)
70	0.51	{(3,2)}	0.22	{(3,2)}	0.22
140	0.87	{(3,2), (3,6)}	0.53	{(3,2), (1,26)}	0.45
210	1.21	{(3,2), (3,6), (3,15)}	0.94	{(3,2), (1,9), (1,26)}	0.65
280	1.68	{(3,2), (3,6), (3,15), (3,7), (1,46)}	1.23	{(3,2), (3,6), (3,15), (1,5), (1,16)}	0.13
350	1.98	{(3,2), (3,6), (3,15), (3,7), (2,6), (1,26)}	0.98	{(3,2), (3,6), (3,15), (1,5), (1,16), (1,45)}	0.14

3.5 Concluding Remarks

In this chapter, we propose a tri-level protection-interdiction-restoration model, depicted as a defender-attacker-defender model, to enhance the resilience of a system of interdependent infrastructure networks under hazard of intelligent attack. This model could also be used to study the worst-case natural disruption scenario under a given disaster level (measured with the budget used by the attacker). The proposed model considers two different agents, an attacker and a defender, acting in three successive steps: (i) first the defender attempts to minimize the vulnerability of the system prior to disruption by protecting network components, (ii) the attacker tries to maximize the effect of disruption by the interdiction of critical components, and (iii) then defender aims

to maximize recoverability of the system of networks in the aftermath of the disruption, by allocating and scheduling work crews to recover disrupted components in a timely manner.

Analytically, multi-level models often cannot be solved directly, and decomposition methods represent a natural approach to address them. In this chapter, we used a tailored modification of the standard covering decomposition algorithm (Israeli & Wood, 2002; Yao et al., 2007) that builds upon iteratively solving nested bi-level protector and interdictor subproblems. The proposed modified covering decomposition algorithm replaces the feasibility seeking objective functions (associated with each subproblem) with subproblems that seek to maximize the number of protected and interdicted components at each iteration. This modification reduces the expected number of iterations and required computation, as it avoids checking protection and interdiction strategies that are redundant, related with an underuse of the available protection and interdiction budgets. At each iteration, the algorithm explores the most critical components that the attacker should target to maximize the disruption (subject to an interdiction budget), and subsequently the protector reacts to minimize the impact of the current interdiction strategy.

To showcase the application and capabilities of the proposed model, we present a case study based on the system of water, gas, and power networks in Shelby County, TN, USA. The results show the importance of adequately considering simultaneously both pre-disruption investments (to reinforce critical network components) and post-disruption

resource assignment and crew scheduling, not only to reduce the vulnerability of the system but also to enhance its recoverability and its overall resilience.

For future work, to reduce the expected solution time of the proposed decomposition algorithm, the protector subproblem could be modified using Benders' decomposition. Additionally, there may be additional multiple valid inequalities (cuts) to the interdictor model that could be developed to further enhance the associated solution times. From a modeling point of view, this study represents with binary variables both defender and attacker decisions. However, future work will focus on considering various levels of protection and interdiction. Also, in the current model, each component can be assigned to only a single work crew, but for future work we plan on extending the model to also consider assigning multiple work crews to the same component. Furthermore, the demand nodes can be prioritized based on different criteria that may affect the restoration process of the disrupted networks. For example, Karakoc et al. (2019) studied the social aspects and demographics for the restoration of a disrupted network to reduce the adverse impacts to socially vulnerable populations. Gomez et al. (2019) addressed perspectives between utility companies and consumers, while considering time-dependent penalties and resource costs. Finally, the proposed tri-level model considers the physical interdependency between networks, but additional types of interdependencies (e.g., geographical interdependency) could also be considered to further enhance the model's applicability.

Chapter 4: A DECOMPOSITION APPROACH FOR SOLVING TRI-LEVEL DEFENDER-ATTACKER-DEFENDER PROBLEMS

4.1 Introduction

In this dissertation, we address simultaneous actions of vulnerability reduction and recoverability enhancement through interdiction model, particularly defender-attacker-defender (DAD) model to enhance the resilience of a system against disruption. However, interdiction models or broadly multi-level problems are challenging to solve. Therefore, efficient solution algorithms are required to address such complex problems in a reasonable time.

In this chapter, we study the interdiction model discussed in Chapter 3 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.

The rest of the chapter is structured as follows. In Section 4.2, the proposed solution approach for solving the DAD models is represented. An illustrative example is provided in Section 4.3, based on the system of interdependent infrastructure networks in Shelby County, TN. We applied the proposed solution technique to the existing interdiction model discussed in Chapter 3 and performed a comparative analysis with respect to the previously discussed solution method (covering decomposition method).

Additionally, we introduce an updated tri-level protection-interdiction-counteraction formulation to assess the resilience of the system under two DAD models, for which the proposed solution technique is also used. Finally, Section 4.4 provides concluding remarks and future work.

4.2 Decomposition-based Solution Approach

For the illustrative purposes, the proposed solution technique is demonstrated with the resilience interdiction model discussed in Chapter 3, namely a tri-level protection-interdiction-restoration model, denoted by M-I in this chapter. 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.

4.2.1 Tri-level Formulation: Protection-Interdiction-Restoration Model (M-I)

In Chapter 3, we 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. 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 Figure 3.1: (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 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 $G^k = (N^k, A^k)$, 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 ($N_=^k \subseteq N^k \setminus \{N_+^k, N_-^k\}$) such that $N_+^k \cap N_-^k = \emptyset$. 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 BP and BI, respectively, suggesting that the protector could protect up to BP components and the attacker could interdict up to BI 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 d_i^k represent the demand should be met at every node $i \in N_-^k$, where decision variables m_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 $T = \{1\}$, $T = \{1, 2, \dots, 5\}$, and $T = \{1, 2, \dots, 23\}$ 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 (3.28), (3.29), (3.31), and (3.32) in Chapter 3. 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 $\left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi$ denotes node $i \in N^k$ in network $k \in K$ physically depends on node $\bar{\imath} \in N^{\bar{k}}$ in network $\bar{k} \in K$ to be operational, where $N^k \cap N^{\bar{k}} = \emptyset$, $A^k \cap A^{\bar{k}} = \emptyset$ and $\forall\, k, \bar{k} \in K: k \neq \bar{k}$.

To demonstrate various steps of the proposed solution algorithm, we represent an abstract form of M-I as shown by Eqs. (4.1)-(4.11). 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. (4.1) and (4.2). Constraints (4.3) and (4.4) represent the budget restrictions for the first defender and attacker decisions, respectively. Constraints (4.5)-(4.8) show the nature of the decision variables for the first and second levels of M-I. Constraints (4.9) and (4.10) deliver the functionality status of every node and link, respectively. Set of constraints (4.11) 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 Chapter 3, 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 (3.27), (3.30), (3.35), (3.36), (3.57), and (3.58) represents a big number, it need be only greater than the maximum required time for restoring the disrupted components.

$$\zeta_{\mathrm{M-I}}(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N_{\underline{t}}^k} w_{it}^k m_{it}^k}{\sum_{k \in K} \sum_{i \in N_{\underline{t}}^k} w_{it}^k d_i^k} \right) \qquad \forall\, t \in T \tag{4.1}$$

$$\xi_{\mathrm{M-I}} = \min_{y} \max_{\mathrm{z}} \min_{m,x,f,\alpha,\beta} \sum_{t \in T} \zeta_{\mathrm{M-I}}(t) \tag{4.2}$$

$$\sum_{k \in K} \sum_{i \in N'^k} y_i^k + \sum_{k \in K} \sum_{(i,j) \in A'^k} y_{ij}^k \leq BP \tag{4.3}$$

$$\sum_{k \in K} \sum_{i \in N'^k} z_i^k + \sum_{k \in K} \sum_{(i,j) \in A'^k} z_{ij}^k \leq BI \tag{4.4}$$

$$y_i^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{4.5}$$

$$y_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{4.6}$$

$$z_i^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{4.7}$$

$$z_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{4.8}$$

$$1 + y_i^k - z_i^k \geq f_i^k \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{4.9}$$

$$1 + y_{ij}^k - z_{ij}^k \geq f_{ij}^k \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{4.10}$$

Constraints (3.11)-(3.50) (4.11)

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 et al., 1992; Wood, 1993). Solution methods developed to solve such complex problems can be categorized into reformulation and duality (Alguacil et al., 2014; Saharidis et al., 2013), decomposition (Yao et al., 2007; Yuan et al., 2014), and heuristic-based approaches (Bier et al., 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 et al., 2017). For example, Mahmoodjanloo et al. (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 chapter, 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. Figure 4.1 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.

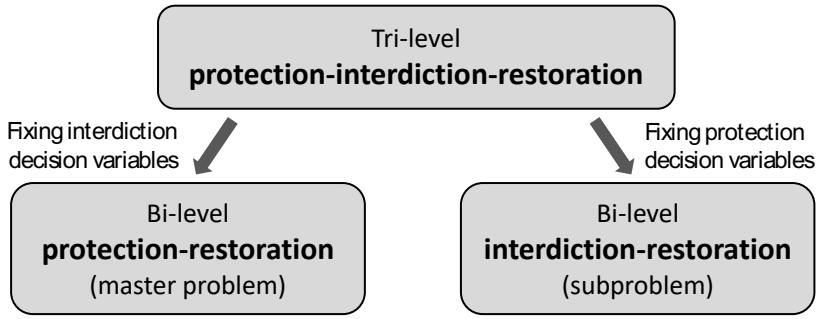


Figure 4.1. Decomposition framework of the tri-level resilience interdiction model.

4.2.2 Master Problem

As depicted in Figure 4.1, the master-problem is constructed by fixing the attacker decision variables in the original model, $z \leftarrow \hat{z}$, 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 (4.12)-(4.18). By solving the mater problem, the protection plan is determined, $y \leftarrow \hat{y}$, 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.

$$\min_{y} \min_{m,x,f,\alpha,\beta} \sum_{t \in T} \zeta_{\mathrm{M-I}}(t) \tag{4.12}$$

$$\sum_{k \in K} \sum_{i \in N'^{k}} y_i^k + \sum_{k \in K} \sum_{(i,j) \in A'^{k}} y_{ij}^k \leq BP \tag{4.13}$$

$$y_i^k \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{4.14}$$

$$y_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{4.15}$$

$$1 + y_i^k - \hat{z}_i^k \geq f_i^k \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{4.16}$$

$$1 + y_{ij}^k - \hat{z}_{ij}^k \geq f_{ij}^k \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{4.17}$$

Constraints (3.11)-(3.50) (4.18)

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

Proof. By fixing the attacker decision variables ($\hat{z}$) 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.

4.2.3 Subproblem

On the other hand, by fixing the protector decision variables found through the master problem, $y \leftarrow \hat{y}$, the subproblem is constructed as the bi-level max-min formulation including attacker and second defender (restoration) levels as represent in constraints (4.19)-(4.25). 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, $z \leftarrow \hat{z}$, which will be the input of the master problem.

$$\max_{z} \min_{m,x,f,\alpha,\beta} \sum_{t \in T} \zeta_{M-\mathrm{I}}(t) \tag{4.19}$$

$$\sum_{k \in K} \sum_{i \in N'^{k}} z_i^k + \sum_{k \in K} \sum_{(i,j) \in A'^{k}} z_{ij}^k \leq BI \tag{4.20}$$

$$z_i^k \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{4.21}$$

$$z_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{4.22}$$

$$1 + \hat{y}_i^k - z_i^k \geq f_i^k \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{4.23}$$

$$1 + \hat{y}_{ij}^k - z_{ij}^k \geq f_{ij}^k \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{4.24}$$

Constraints (3.11)-(3.50) (4.25)

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.

4.2.4 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). Figure 4.2 represents the general framework of the proposed solution algorithm.

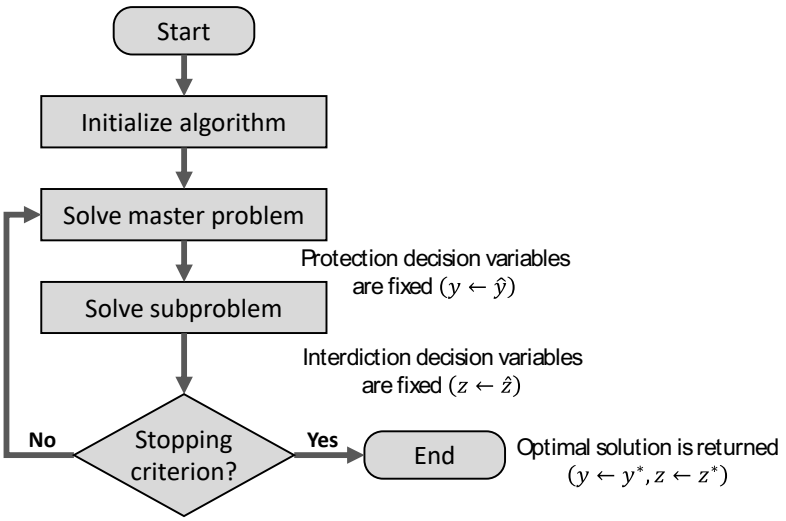


Figure 4.2. The general framework of the proposed solution algorithm.

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 4.1. 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., $\hat{z}^c$) 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 $\underline{P}^c$ 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.

Table 4.1. 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: $\sum_{k\in K} \sum_{i\in N'^k \mid z_i^k=0} z_i^k + \sum_{k\in K} \sum_{(i,j)\in A'^k \mid z_{ij}^k=0} z_{ij}^k \geq 1$
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})

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 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.

4.3 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 Figure 4.3 for each network separately (González et al., 2016b). 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.

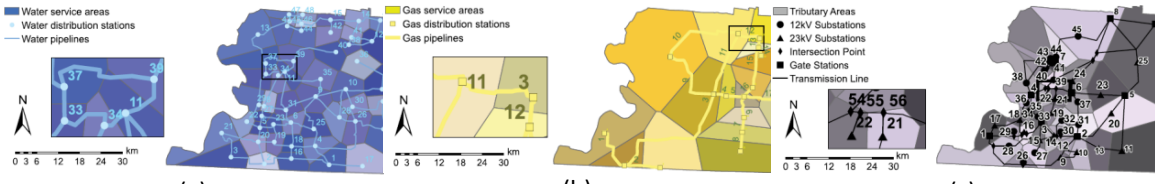


Figure 4.3. Graphical illustration of the (a) water, (b) gas, and (c) power networks (adapted from González et al., 2016b)).

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 @ 3.40GHz 3.41GHz 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., $\varepsilon = 0.01$.

4.3.1 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 chapter, 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 dissertation, 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 hours, and the time horizon of the model is chosen to be one working month defined as 23 working shifts, $T = \{1, 2, \dots, 23\}$. Different scenarios account for the resource available for protector and interdictor (BP and BI as discussed in the computational results section.

4.3.2 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 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'^{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 4.2. 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.

Table 4.2. 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

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 4.3.

Table 4.3. 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

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. Figure 4.4 shows the dendrogram representing different clusters of candidate nodes based on the proximity matrix. The dashed horizontal line in Figure 4.4 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 et al., 2001).

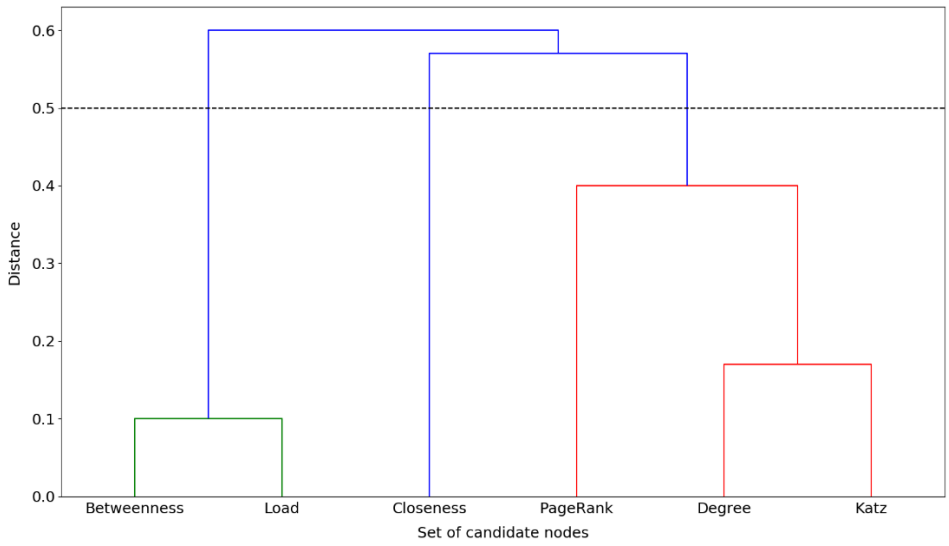
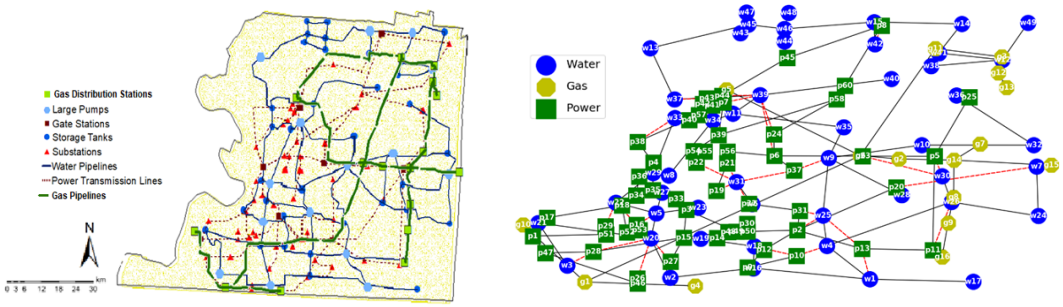


Figure 4.4. The dendrogram of clustering different sets of candidate nodes.

Figure 4.5 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 Figure 4.5b represent the interdependency relationship between water and power networks in this case study.



(a) (b)

Figure 4.5. The (a) map and (b) topology of the interdependent system of water, gas, and power networks in Shelby County, TN, USA.

4.3.3 Computational Results of M-I

In this section, 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.

4.3.3.1 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). Figure 4.6 depicts the computation speed of S-I with respect to S-II for different protector budgets (BP) and attacker budgets (BI). 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 $BI = 4$, 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 $BP = 4$.

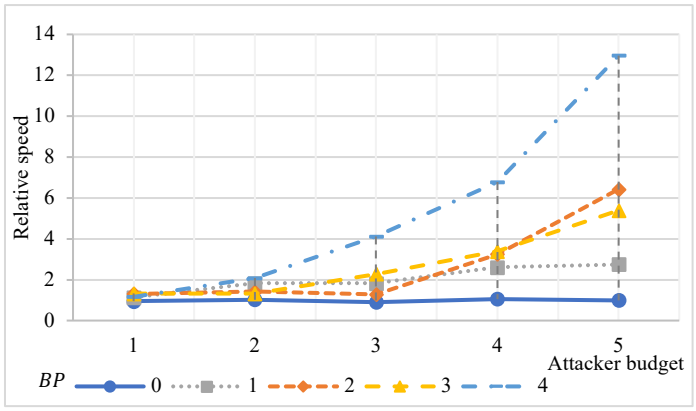
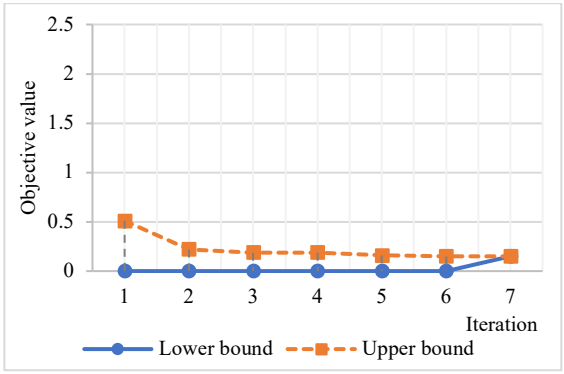


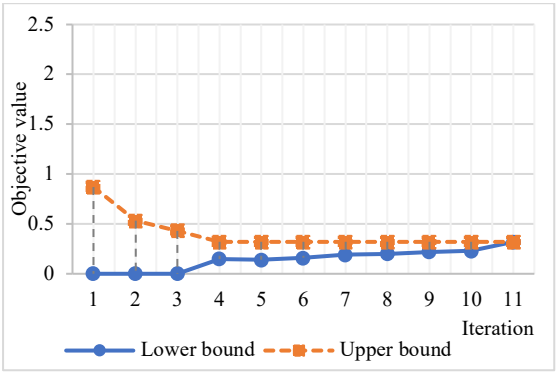
Figure 4.6. Computation speed of S-I with respect to S-II under different budget scenarios.

Figure 4.7 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 $BP = 4$ 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

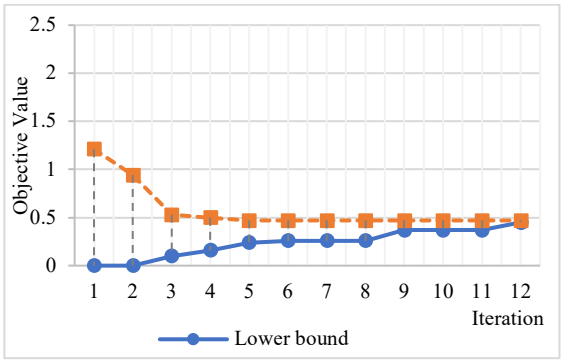
iterations, we witness a noticeable improvement in the solution as the gap between the upper bound and lower bound values reduces rapidly. Then this improvement slows down until the convergence ratio of upper bound and lower bound (i.e., the stopping criterion of the algorithm, ε) is reached and the 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.



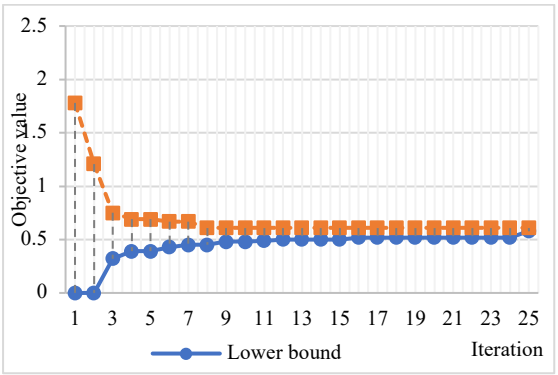
(a)



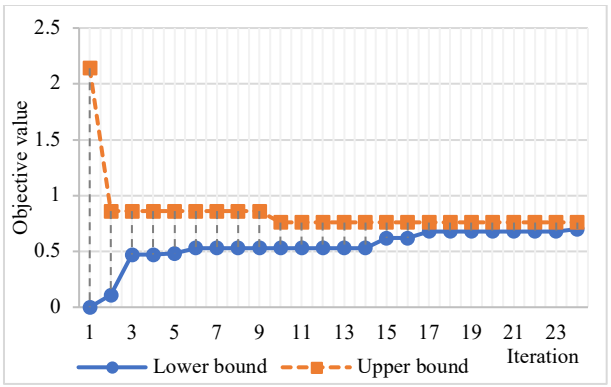
(b)



(c)



(d)



(e)

Figure 4.7. Convergence trend of upper bound and lower bound values in S-I algorithm as for $BP = 4$ under (a) $BI = 1$, (b) $BI = 2$, (c) $BI = 3$, (d) $BI = 4$, and (e) $BI = 5$.

4.3.3.2 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 4.4. As the base scenario, we solve the model assuming that a single work crew is available for each network. Thereafter, different scenarios account for multiple crews for a selected number of budget scenarios, and the results are discussed subsequently. In addition to the objective value of the model ($\xi_{\mathrm{M-I}}$), we record the immediate drop in the system performance following the attack, $t = 1$, when the restoration process has not yet commenced, denoted by $\nu_{\mathrm{M-I}}$ in Table 4.4.

From Table 4.4, the immediate drop in the system performance does not reduce substantially as the protection budget increases. For example, for $BI = 4$, 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. (3.2), 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.

Table 4.4. Computational results of M-I for each set of candidate nodes (generated based on different centrality measures) under different budget scenarios.

Protector budget (BP)	Attacker budget (BI)	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

Figure 4.8 illustrates the trend of the objective value for M-I under different sets of candidate nodes for protection budgets of 0 to 4. Clearly, for a given protection budget, the objective value ($\xi_{\mathrm{M-I}}$), 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 Figure 4.8a to Figure 4.8e. 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 to 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.

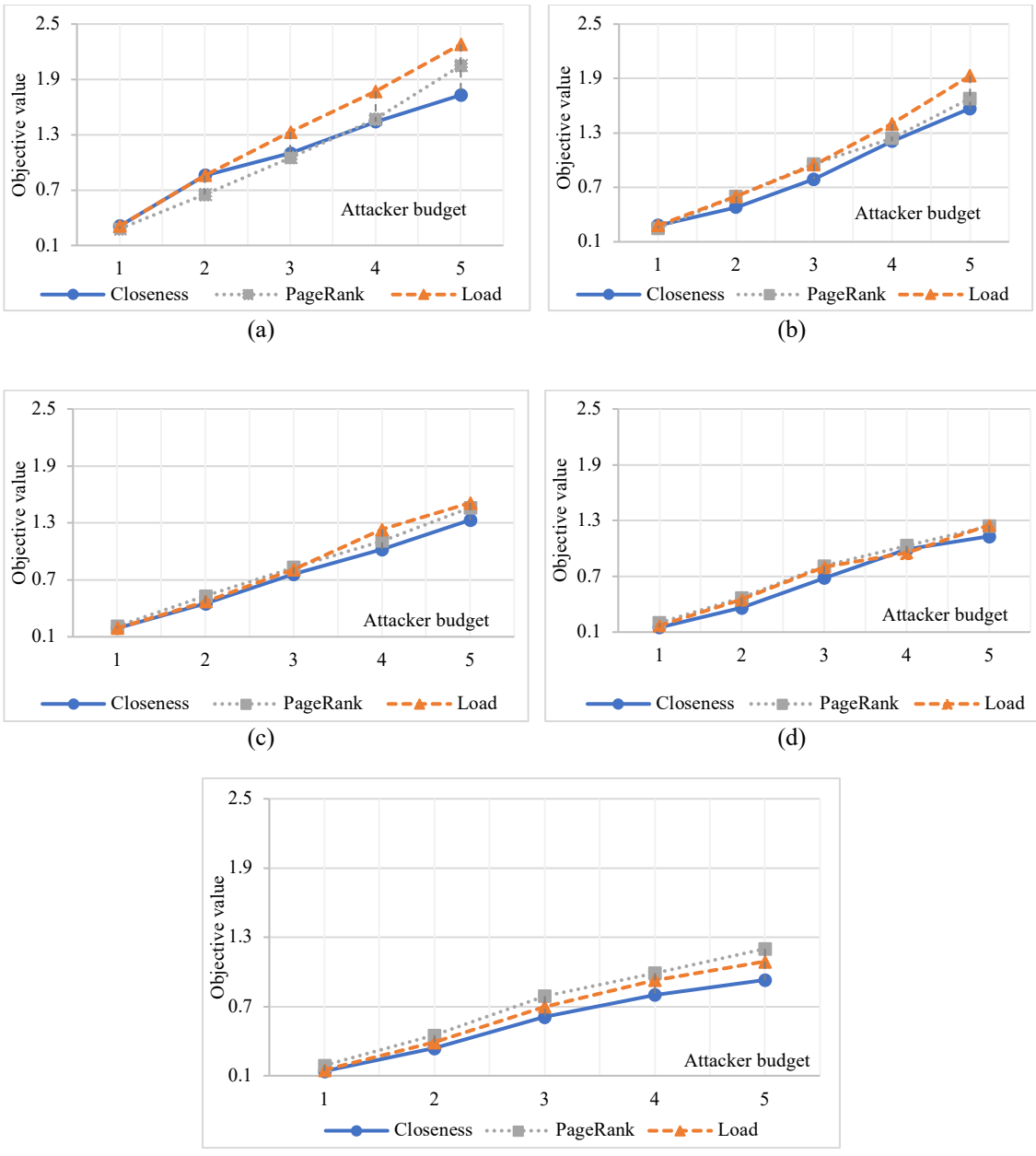


Figure 4.8. Objective value of M-I (ξ_{M-I}) for different sets of candidate nodes (generated based on different centrality measures) for protection budgets of (a) 0, (b) 1, (c) 2, (d) 3, and (e) 4.

4.3.3.3 Computational results of M-I for multiple work crews

One of the advantages of M-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 $BI = 5$ under two protection budgets (i.e., $BI = 5$ and BP =0 and 1).

As mentioned in Chapter 1 and in reference to Figure 1.1, 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. (4.1). Figure 4.9 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 $\nu_{\mathrm{M-I}}$ in Table 4.4. 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 Figure 4.9 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 Figure 4.9a and Figure 4.9b are $\nu_{\mathrm{M-I}} = 0.36$ and $\nu_{\mathrm{M-I}} = 0.29$, 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.

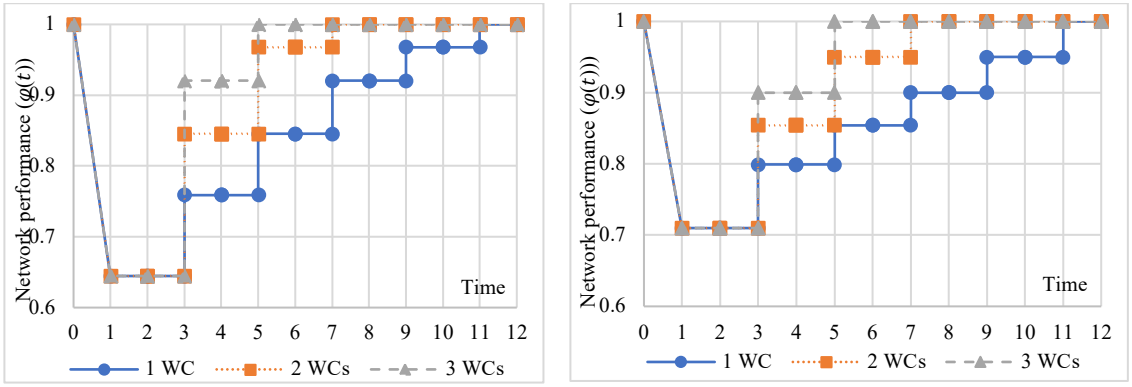


Figure 4.9. Network performance $\boldsymbol{\varphi(t)}$ of M-I as for $\boldsymbol{BI = 5}$ under (a) $\boldsymbol{BP = 0}$ and (b) $\boldsymbol{BP = 1}$.

4.3.4 Tri-level Formulation: Protection-Interdiction-Counteraction Model (M-II)

As discussed in Section 4.2.1, 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 ($\zeta_{\mathrm{M-II}}(t=1)$) 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 $\zeta_{\mathrm{M-II}}(t)$ as the weighted proportion of unmet demand (relative to the met demand before the disruption), as shown in Eq. (4.26). Then, the objective function of M-II is defined as Eq. (4.27), 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 $\nu_{\mathrm{M-II}}$ as shown in Eq. (4.27). Note that the entire parameters and decision variables indexed by time ($t \in T$) are also considered only for one-time unit such that $t=1$.

$$\zeta_{\mathrm{M-II}}(t) = 1 - \left(\frac{\sum_{k \in K} \sum_{i \in N^k} w_{it}^k m_{it}^k}{\sum_{k \in K} \sum_{i \in N^k} w_{it}^k d_i^k} \right) \qquad \forall t \in T \tag{4.26}$$

$$\nu_{\mathrm{M-II}} = \min_{y} \max_{\mathrm{z}} \min_{m,x,f,\alpha} \zeta_{\mathrm{M-II}}(t=1) \tag{4.27}$$

Constraints (3.15)-(3.18), (3.27)-(3.39), and (3.47)-(3.50) in M-I are removed as they correspond to the restoration level. Constraints (3.24)-(3.26) are substituted with constraints (4.28)-(4.30), 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.

$$x_{ij1}^{k} \le u_{ij}^{k}\alpha_{ij}^{k} \qquad \forall\,(i,j) \in A'^{k}, \forall\, k \in K \tag{4.28}$$

$$x_{ij1}^{k} \le u_{ij}^{k}\alpha_{i}^{k} \qquad \forall\,(i,j) \in A^{k}, \forall\, i \in N'^{k}, \forall\, k \in K \tag{4.29}$$

$$x_{ij1}^{k} \le u_{ij}^{k}\alpha_{j}^{k} \qquad \forall\,(i,j) \in A^{k}, \forall\, j \in N'^{k}, \forall\, k \in K \tag{4.30}$$

Finally, constraint (3.40) in M-I is replaced by constraints (4.31), representing the physical interdependency among the networks of a system. In particular, constraints (4.31) state that positive flow through a link is a function of the functionality status of its corresponding related parent nodes (in other networks).

$$x_{ij1}^{k} \le u_{ij}^{k}\alpha_{\bar{\imath}}^{\bar{k}} \qquad \forall\,(i,j) \in A^{k}, \forall\,\bar{\imath} \in N'^{\bar{k}} \mid \left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi \text{ or } \left((j,k),(\bar{\imath},\bar{k})\right) \in \Psi, \forall\, k,\bar{k} \in K \tag{4.31}$$

Note that η_{i1}^{k}, x_{ij1}^{k}, f_{i}^{k}, f_{ij}^{k}, α_{i}^{k}, and $F\alpha_{ij}^{k}$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.

4.3.4.1 Computational results of M-II for different sets of candidate nodes

Table 4.5 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 $\nu_{\mathrm{M-I}}$ in Table 4.4), the system vulnerability in M-II (referring to $\nu_{\mathrm{M-II}}$ in Table 4.5) remarkably continues to reduce as the protection budget increases. This is because in the objective function of M-II, Eq. (4.27), the immediate drop in the system performance is the only resilience component taken into account. Therefore, the optimal

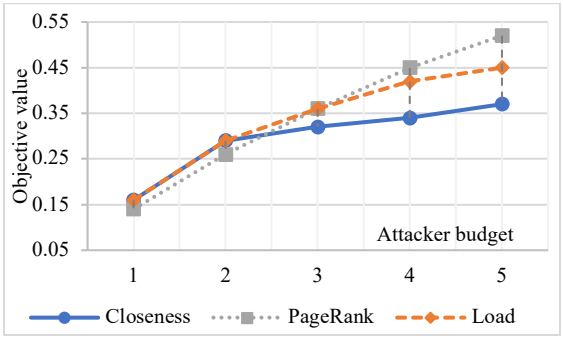
decision made by the attacker is the one that decreases the performance of the system the most at $t = 1$. Likewise, the protector only focuses on the vulnerability reduction immediately after disruption in M-II. In addition, by comparing the objective values of two models, $\xi_{\mathrm{M-I}}$ and $\nu_{\mathrm{M-II}}$, 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.

Table 4.5. Objective value of M-II ($\nu_{\mathrm{M-II}}$) for each set of candidate nodes (generated based on different centrality measures) under different budget scenarios.

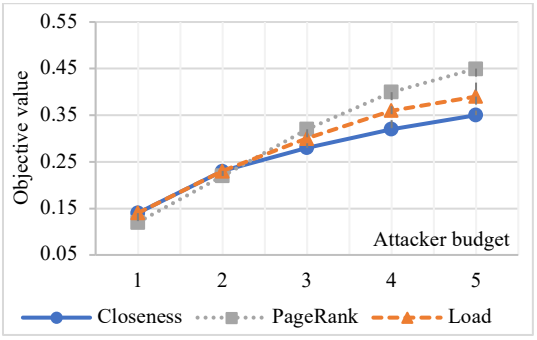
Protector budget (BP)	Attacker budget (BI)	Candidate node sets		
		Closeness	PageRank	Load
0	1	0.16	0.14	0.16
	2	0.29	0.26	0.29
	3	0.32	0.36	0.36
	4	0.34	0.45	0.42
	5	0.37	0.52	0.45
1	1	0.14	0.12	0.14
	2	0.23	0.22	0.23
	3	0.28	0.32	0.30
	4	0.32	0.40	0.36
	5	0.35	0.45	0.39
2	1	0.09	0.10	0.09
	2	0.17	0.20	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

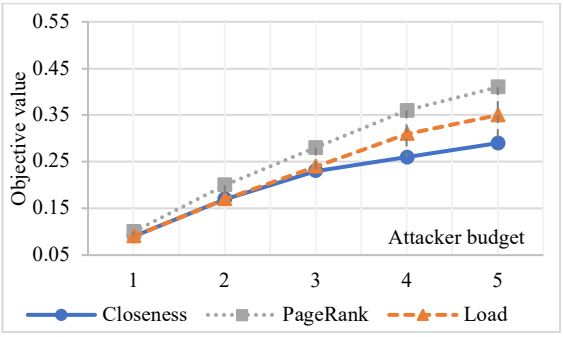
Figure 4.10 illustrates the trend of objective value changes for M-II ($\boldsymbol{\nu_{M-II}}$) under different sets of candidate nodes for protection budgets of 0 to 4. As it can be seen from Figure 4.10a to Figure 4.10e, the highest objective value belongs to the set created based on the PageRank 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.



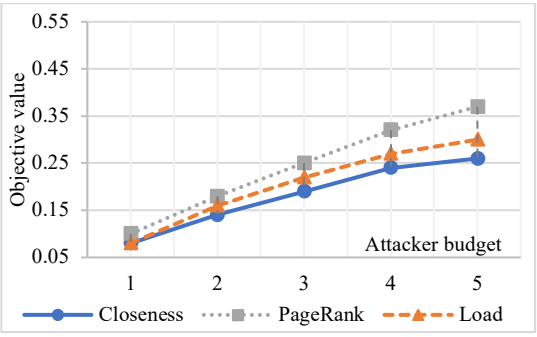
(a)



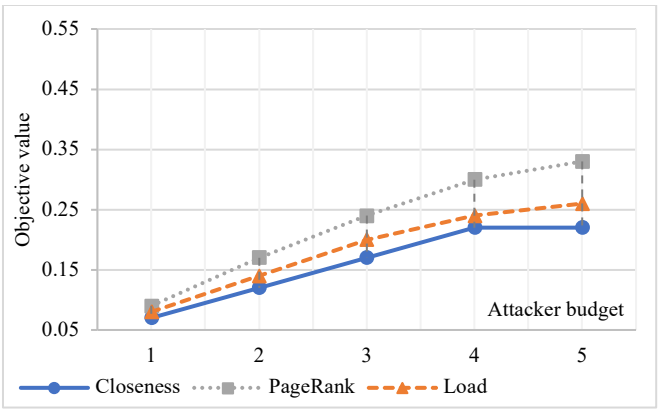
(b)



(c)



(d)



(e)

Figure 4.10. The objective value of M-II (ν_{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.

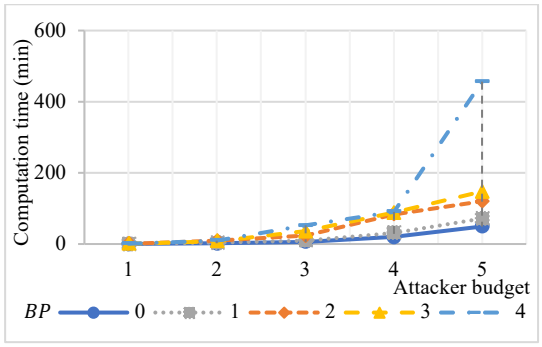
4.3.4.2 Computation time comparison of M-I and M-II

Table 4.6 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). Figure 4.11 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 Figure 4.11a and Figure 4.11b 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 Figure 4.11c, 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

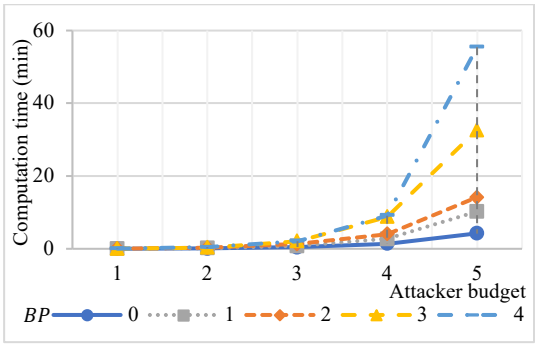
the protector budget changes since the convergence speed of the algorithm reduces for some specific budget scenarios.

Table 4.6. Computational time of M-I and M-II under different budget scenarios.

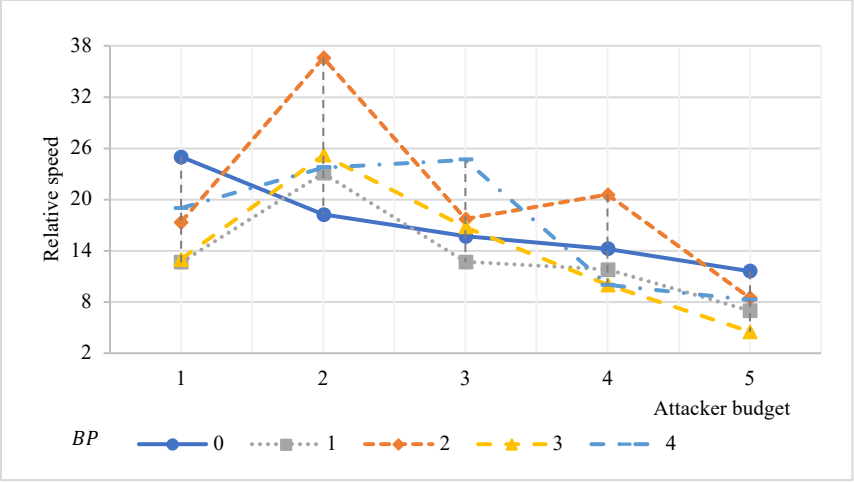
Protector budget (BP)	Attacker budget (BI)	r_{M-I} (min)	r_{M-II} (min)	$\left(\frac{r_{M-I}}{r_{M-II}}\right)$
0	1	0.25	0.01	25.00
	2	1.46	0.08	18.25
	3	6.44	0.41	15.71
	4	19.93	1.4	14.24
	5	49.19	4.24	11.60
1	1	0.38	0.03	12.67
	2	3.92	0.17	23.06
	3	9.66	0.76	12.71
	4	31.64	2.68	11.81
	5	71.51	10.25	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)

Figure 4.11. 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.

4.4 Concluding Remarks

In this chapter, 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 discussed in Chapter 3 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 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.

Chapter 5: HYBRID ALGORITHMS FOR ENHANCED EFFICIENCY AND SCALABILITY OF TRI-LEVEL PROTECTION-INTERDICTION-RESTORATION MODELS

5.1 Introduction

Interdiction models have a wide variety of real-world applications from military to facility location problem to project management. The defender-attacker-defender (DAD) formulation is a type of interdiction model that can be applied to study the resilience of a system against intelligent attacks. However, DAD models are computationally challenging to solve, requiring efficient solution methods to deal with such complex problems. In this chapter, we address this issue by developing two novel hybrid decomposition-based algorithms to deal with a wide range of interdiction models particularly defender-attacker-defender (DAD) models with total or partial protection and interdiction. The first solution approach, which we refer to *hybrid Benders decomposition-based* (HBD) algorithm, integrates Benders decomposition method with a metaheuristic algorithm, while the second, named the *hybrid set covering-based* (HSC) algorithm, integrates the set covering approach and a metaheuristic algorithm. To showcase the capabilities of the proposed methods, we use them to solve the tri-level DAD formulation, namely a tri-level protection-interdiction-restoration model discussed in Chapter 3 to assess the efficient solvability of the methods for two case studies with different network sizes.

The rest of the chapter is structured as follows. Section 5.2 provides a basic network interdiction formulation in which an interdictor seeks to maximize the

cumulative of unmet demand across the system of interdependent networks by disrupting a set of links based on the budget availability. This problem is formulated as a tri-level DAD hierarchical formulation for interdependent network resilience. In Section 5.3, the hybrid solution techniques are presented with the general framework of their algorithms. In Section 5.4, we apply the proposed solution techniques to the tri-level optimization model discussed in Chapter 3 for two systems of interdependent networks with different sizes and compare the solution time and quality of the results with respect to the existing exact solution method. Finally, concluding remarks are provided in Section 5.5.

5.2 Problem Description

This dissertation is concerned with the resilience control (enhancement) of interdependent infrastructure networks (e.g., electric power, water supply) under intelligent attacks. We model this problem as a tri-level DAD hierarchical formulation with a corresponding hierarchy of decisions. 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 affects the decisions of other levels. Figure 5.1 is a general depiction of the three levels involved in this problem: (i) protection, (ii) interdiction, and (iii) counteraction. The protection level implements strategies for hardening network components such as increasing the capacity of the network component, enabling backup capabilities, and burying specific components in the case of electric power networks (Alderson et al., 2011; Ouyang & Fang, 2017). The interdiction level identifies the set of components that would, if disrupted, result in the maximum damage through the system for a given attack budget. This level does not necessarily

require a human “attacker” and could represent a worst-case natural disaster (note that terms related to the disruptive agent such as attacker and interdictor are used interchangeably through this dissertation). The disruption (interdiction) can take the form of a reduction in the capacity of the network components (either nodes or links). Finally, the counteraction level reacts after disruption perceived from the attacker with the aim of minimizing the system loss. The counteraction level can be performed either (i) by solving a generic and simplified optimal network flow problem to minimize the system loss (Alguacil et al., 2014; Yuan et al., 2014), or in a more comprehensive manner (ii) by solving an optimal network flow problem accounting for restoration process of disrupted components to minimizes the long-term effect after the disruption through the network component recovery (Ouyang, 2017).

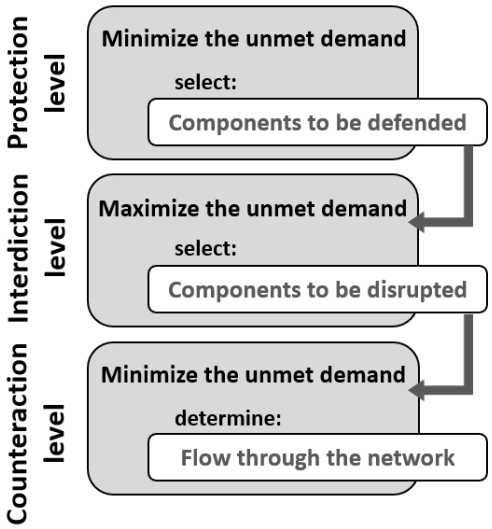


Figure 5.1. Tri-level DAD process.

To properly demonstrate various steps of the proposed hybrid solution algorithms, we first introduce a general and simplified framework for the tri-level DAD model in

which the recovery process has not been considered through the counteraction level. However, for the experimental purposes, we utilize a more comprehensive model discussed in Chapter 3 accounting for the restoration process of disrupted network components through the counteraction level and discuss the results. The comprehensive model, the tri-level DAD model that includes restoration, has been presented in detail in Chapter 3.

5.2.1 Model Assumptions and Notation

In this dissertation, we focus on the system of interdependent networks defined by a set of nodes connected with a set of links where the service provided by each network is represented by flow through it (Lee et al., 2007; Nurre et al., 2012). We assume that each network is responsible for providing a specific type of service (commodity) across the network by satisfying the demand nodes of the network (e.g., the gas network provides gas service, the water supply network provides water requirements). We consider a single commodity flowing through a network, but it can be easily extended to account for multiple commodities. We consider physical interdependency for networks where the functionality of a set of nodes in one or more networks enable the functionality of a node in another network through interdependency links. In this problem, an intelligent attacker, who has complete information about the network, intentionally interdicts the system. The protector, on the other hand, defends (fortifies) the system in response to such prospective interdiction. There are known budgets available for protecting and for interdicting the components of the system of networks. There is a known fixed cost associated with protecting or interdicting each network component. Although

infrastructure networks have different features that are guided by different physical principles, we approximated that infrastructure networks follow the general network flow problem. In the basic formulation in Eqs. (5.1)-(5.9), we assume that links are the only component that can be protected and interdicted, however the model can be easily extended to account for nodes as well.

Assume a set K of infrastructure networks and network $k \in K$ is represented by $G^k = (N^k, A^k)$, 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 ($N_=^k \subseteq N^k \setminus \{N_+^k, N_-^k\}$) such that $N_+^k \cap N_-^k = \emptyset$. Let s_i^k and d_i^k denote the amount of supply and demand in nodes $i \in N_+^k$ and $i \in N_-^k$, respectively. For every link $(i,j) \in A^k$, binary variables y_{ij}^k and z_{ij}^k represent the first defender and attacker actions respectively in the tri-level DAD formulation. Parameters CP_{ij}^k and CI_{ij}^k denote the protection and interdiction cost for every link, respectively, and BP and BI are the total available resources for protection and interdiction, respectively. Also, for each link $(i,j) \in A^k$, binary variables f_{ij}^k show the functionality status for link $(i,j) \in A^k$. 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 provides the flow through the associated link. Decision variables m_i^k denote actual demand being met at node $i \in N_-^k$. Demand nodes can be ranked with the aim of emphasizing on their importance in a network. Therefore, parameters w_i^k show the weight of demand node $i \in N_-^k$, 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). Finally, Ψ represents the interdependency set among networks such that $\left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi$ denotes node $i \in N^k$ in network $k \in K$ physically depends on node $\bar{\imath} \in N^{\bar{k}}$ in network $\bar{k} \in K$ to be operational, where $N^k \cap N^{\bar{k}} = \emptyset$, $A^k \cap A^{\bar{k}} = \emptyset$ and $\forall\, k, \bar{k} \in K: k \neq \bar{k}$.

5.2.2 Mathematical Formulation

The tri-level DAD model aims to deliver the cumulative weighted fraction of unmet demand, such that this value is minimized by the first defender, maximized by the attacker, and minimized by the subsequent defender, as shown in Eq. (5.1). The general formulation of the model is represented in Eqs. (5.1)-(5.9). Constraints (5.2) and (5.3) represent the budget restrictions for the first defender and attacker decisions, respectively. Constraints (5.4) deliver the functionality status of every link. Constraints (5.5) and (5.6) guarantee the flow balance at node $i \in N^k$. Constraints (5.7) ensure that the amount of positive flow through any given link is a function of the functionality status of the corresponding link. Constraints (5.8) represent the physical interdependency among networks such that a positive flow through a link is only attained if their corresponding related parent nodes (in other networks) are operational. Finally, constraints (5.9) show the nature of the decision variables for the model, where y_{ij}^k, z_{ij}^k, and f_{ij}^k are binary variables, however x_{ij}^k and m_i^k can take positive continuous values.

$$\mathfrak{Q} = \min_{y} \max_{z} \min_{m,x,f} \left[\frac{\sum_{k \in K} \sum_{i \in N^{\underline{k}}} w_i^k \left(d_i^k - m_i^k\right)}{\sum_{k \in K} \sum_{i \in N^{\underline{k}}} w_i^k d_i^k} \right] \tag{5.1}$$

Subject to:

$$\sum_{k\in K}\sum_{(i,j)\in A^k} CP_{ij}^k y_{ij}^k \le BP \tag{5.2}$$

$$\sum_{k\in K}\sum_{(i,j)\in A^k} CI_{ij}^k z_{ij}^k \le BI \tag{5.3}$$

$$1 + y_{ij}^k - z_{ij}^k \ge f_{ij}^k \qquad \forall\,(i,j)\in A^k, \forall\, k \in K \tag{5.4}$$

$$\sum_{(i,j)\in A^k} x_{ij}^k - \sum_{(j,i)\in A^k} x_{ji}^k \begin{cases} \le s_i^k & \forall\, i \in N_+^k, \forall\, k \in K \\ = 0 & \forall\, i \in N_=^k, \forall\, k \in K \\ \le -m_i^k & \forall\, i \in N_-^k, \forall\, k \in K \end{cases} \tag{5.5}$$

$$m_i^k \le d_i^k \qquad \forall\, i \in N_-^k, \forall\, k \in K, \tag{5.6}$$

$$x_{ij}^k \le u_{ij}^k f_{ij}^k \qquad \forall\,(i,j)\in A^k, \forall\, k \in K \tag{5.7}$$

$$x_{ij}^k \le u_{ij}^k f_{\bar{i}\bar{j}}^{\bar{k}} \qquad \forall\,(i,j)\in A^k, \forall\, k, \bar{k} \in K, \forall\,(\bar{i},\bar{j})\in A^{\bar{k}} \mid \big((i,k),(\bar{j},\bar{k})\big) \in \Psi \text{ or } \big((j,k),(\bar{j},\bar{k})\big) \in \Psi \tag{5.8}$$

$$y_{ij}^k \in \{0,1\},.\ \ z_{ij}^k \in \{0,1\},.\ \ f_{ij}^k \in \{0,1\},.\ \ x_{ij}^k \ge 0,.\ \ m_i^k \ge 0 \qquad \forall\,(i,j)\in A^k, \forall\, i \in N_-^k, \forall\, k \in K \tag{5.9}$$

5.3 Hybrid Solution Techniques

The two solution methods are decomposition-based in which, by iteratively solving the smaller nested bi-level problems (master problem and subproblem), the final solution for the tri-level DAD model is obtained. Therefore, we first decompose the tri-level DAD model in Eqs. (5.1)-(5.9) to a (i) master problem, and a (ii) subproblem, providing the lower and upper bound values for the model, respectively. By iteratively solving the two problems, the gap between the two bounds is reduced until the final solution is found. The details of constructing the two problems are described subsequently.

To construct the master problem, the attacker decision variables ($\hat{z}$) are fixed. The tri-level DAD model is then transformed to the bi-level min-min formulation as shown in

constraints (5.10)-(5.17). By solving the master problem, the protection plan (y) is determined, which will be the input of the subproblem.

$$\min_{y} \min_{m,x,f} \left[\frac{\sum_{k\in K} \sum_{i\in N_{-}^{k}} w_i^k \left(d_i^k - m_i^k\right)}{\sum_{k\in K} \sum_{i\in N_{-}^{k}} w_i^k d_i^k} \right] \tag{5.10}$$

Subject to:

$$\sum_{k\in K} \sum_{(i,j)\in A^k} CP_{ij}^k y_{ij}^k \le BP \tag{5.11}$$

$$1 + y_{ij}^k - \hat{z}_{ij}^k \ge f_{ij}^k \qquad \forall\, (i,j) \in A^k, \forall\, k \in K \tag{5.12}$$

$$\sum_{(i,j)\in A^k} x_{ij}^k - \sum_{(j,i)\in A^k} x_{ji}^k \begin{cases} \le s_i^k & \forall\, i \in N_{+}^k, \forall\, k \in K \\ = 0 & \forall\, i \in N_{=}^k, \forall\, k \in K \\ \le -m_i^k & \forall\, i \in N_{-}^k, \forall\, k \in K \end{cases} \tag{5.13}$$

$$m_i^k \le d_i^k \qquad \forall\, i \in N_{-}^k, \forall\, k \in K \tag{5.14}$$

$$x_{ij}^k \le u_{ij}^k f_{ij}^k \qquad \forall\, (i,j) \in A^k, \forall\, k \in K \tag{5.15}$$

$$x_{ij}^k \le u_{ij}^k f_{\bar{i}\bar{j}}^{\bar{k}} \qquad \forall\, (i,j) \in A^k\,, \forall\, k, \bar{k} \in K\,, \forall\, (\bar{\imath},\bar{\jmath}) \in A^{\bar{k}} \mid \left((i\,,k),(\bar{\jmath},\bar{k})\right) \in \Psi \text{ or } \left((j\,,k),(\bar{\jmath},\bar{k})\right) \in \Psi \tag{5.16}$$

$$y_{ij}^k \in \{0,1\},.\ f_{ij}^k \in \{0,1\},.\ x_{ij}^k \ge 0,.\ m_i^k \ge 0 \qquad \forall\, (i,j) \in A^k, \forall\, i \in N_{-}^k\,, \forall\, k \in K \tag{5.17}$$

By fixing the attacker decision variables ($\hat{z}$) 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 is considered, the master problem provides a valid lower bound value for the entire tri-level DAD model. And by fixing the protector decision variables ($\hat{y}$) found through the master problem, the subproblem is constructed as a bi-level max-min formulation including attacker and subsequent defender levels as

represented in constraints (5.18)-(5.25). By solving the subproblem, the interdiction plan (z) is determined and serves as the input of the master problem.

$$\max_{z} \min_{m,x,f} \left[\frac{\sum_{k\in K} \sum_{i\in N_{-}^{k}} w_i^k \left(d_i^k - m_i^k\right)}{\sum_{k\in K} \sum_{i\in N_{-}^{k}} w_i^k d_i^k} \right] \tag{5.18}$$

Subject to:

$$\sum_{k\in K} \sum_{(i,j)\in A^k} CI_{ij}^k z_{ij}^k \le BI \tag{5.19}$$

$$1 + \hat{y}_{ij}^k - z_{ij}^k \ge f_{ij}^k \qquad \forall\, (i,j) \in A^k, \forall\, k \in K \tag{5.20}$$

$$\sum_{(i,j)\in A^k} x_{ij}^k - \sum_{(j,i)\in A^k} x_{ji}^k \begin{cases} \le s_i^k & \forall\, i \in N_{+}^k, \forall\, k \in K \\ = 0 & \forall\, i \in N_{=}^k, \forall\, k \in K \\ \le -m_i^k & \forall\, i \in N_{-}^k, \forall\, k \in K \end{cases} \tag{5.21}$$

$$m_i^k \le d_i^k \qquad \forall\, i \in N_{-}^k, \forall\, k \in K, \tag{5.22}$$

$$x_{ij}^k \le u_{ij}^k f_{ij}^k \qquad \forall\, (i,j) \in A^k, \forall\, k \in K \tag{5.23}$$

$$x_{ij}^k \le u_{ij}^k f_{\bar{i}\bar{j}}^{\bar{k}} \qquad \forall\, (i,j) \in A^k\,, \forall\, k, \bar{k} \in K\,, \forall\, (\bar{\imath},\bar{\jmath}) \in A^{\bar{k}} \mid \left((i\,,k),\left(\bar{\jmath},\bar{k}\right)\right) \in \Psi \text{ or } \left((j\,,k),\left(\bar{\jmath},\bar{k}\right)\right) \in \Psi \tag{5.24}$$

$$z_{ij}^k \in \{0,1\},.\ f_{ij}^k \in \{0,1\},.\ x_{ij}^k \ge 0,.\ m_i^k \ge 0 \qquad \forall\, (i,j) \in A^k, \forall\, i \in N_{-}^k, \forall\, k \in K \tag{5.25}$$

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 is considered, the subproblem provides a valid upper bound value for the entire tri-level DAD model.

Based on the general procedure of decomposing the tri-level DAD model discussed above, we detail the proposed solution algorithms in the following sections. Note again that for the purpose of presenting the proposed solution approaches, we first

defined a general and simplified framework for the tri-level DAD model in which the recovery process has not been considered through the counteraction level. However, the two solution methods that will be discussed subsequently can be easily applied to other types of interdiction models with the same procedure presented in this chapter.

5.3.1 Hybrid Benders Decomposition-based (HBD) Algorithm

The HBD algorithm integrates Benders decomposition method (i.e., the C&CG decomposition method (Zeng & Zhao, 2013)) with a metaheuristic algorithm to deal with the master problem and subproblem, respectively.

The bi-level min-min model generated through the master problem can be converted to a single minimization formulation by merging the two levels and adding a set of constraints that can be solved directly using available optimization solvers (Yuan et al., 2014). To implement Benders decomposition to solve the master problem, we assume a set of attack plans $\hat{Z} = \{\hat{Z}^1, \dots, \hat{Z}^C\} \subseteq Z$ that are indexed by the iteration $c = 0,1, \dots, C$, and we define a set of decision variables f_{ij}^{kc}, x_{ij}^{kc}, and m_i^{kc} for the associated attack plan for the given iteration. By defining a new set of decision variables, we transform the bi-level master problem to the single-level optimization based on the Benders framework (Yuan et al., 2014; Zeng & Zhao, 2013) as shown in Eqs. (5.26)-(5.34). Note that the master problem is updated at each iteration and the new set of attacker decisions is generated with the current iteration index. Subsequently, the new set of decision variables f_{ij}^{kc}, x_{ij}^{kc}, and m_i^{kc} and constraints are added to the formulation for the corresponding attacker decision at the given iteration. Note that the first defender decision variables (y) remain unchanged as shown in constraints (5.29) and (5.34). Mentioned previously,

solving the optimization model in Eqs. (5.26)-(5.34) provides the best (optimal) solution for the first defender decision variables (y), which will be the input to the subproblem.

$$\min \delta \tag{5.26}$$

Subject to:

$$\delta \leq \left[\frac{\sum_{k\in K}\ \sum_{i\in N_{-}^{k}} w_i^k\left(d_i^k - m_i^{kc}\right)}{\sum_{k\in K}\ \sum_{i\in N_{-}^{k}} w_i^k d_i^k}\right] \qquad \forall\, c = 0,1,\dots,C \tag{5.27}$$

$$\sum_{k\in K}\ \sum_{(i,j)\in A^k} CP_{ij}^k y_{ij}^k \leq BP \tag{5.28}$$

$$1 + y_{ij}^k - \hat{z}_{ij}^{kc} \geq f_{ij}^{kc} \qquad \forall\,(i,j)\in A^k, \forall\, k\in K, \forall\, c = 0,1,\dots,C \tag{5.29}$$

$$\sum_{(i,j)\in A^k} x_{ij}^{kc} - \sum_{(j,i)\in A^k} x_{ji}^{kc} \begin{cases} \leq s_i^k & \forall\, i\in N_{+}^{k}, \forall\, k\in K, \forall\, c = 0,1,\dots,C \\ = 0 & \forall\, i\in N_{=}^{k}, \forall\, k\in K, \forall\, c = 0,1,\dots,C \\ \leq -m_i^{kc} & \forall\, i\in N_{-}^{k}, \forall\, k\in K, \forall\, c = 0,1,\dots,C \end{cases} \tag{5.30}$$

$$m_i^{kc} \leq d_i^k \qquad \forall\, i\in N_{-}^{k}, \forall\, k\in K, \forall\, c = 0,1,\dots,C \tag{5.31}$$

$$x_{ij}^{kc} \leq u_{ij}^k f_{ij}^{kc} \qquad \forall\,(i,j)\in A^k, \forall\, k\in K, \forall\, c = 0,1,\dots,C \tag{5.32}$$

$$x_{ij}^{kc} \leq u_{ij}^k f_{\bar{\imath}\bar{\jmath}}^{\bar{k}c} \qquad \forall\,(i,j)\in A^k\ , \forall\, k,\bar{k}\in K, \forall\,(\bar{\imath},\bar{\jmath})\in A^{\bar{k}} \mid \left((i\ ,k),(\bar{\jmath},\bar{k})\right) \in \Psi\ or\ \left((j\ ,k),(\bar{\jmath},\bar{k})\right)\in\Psi, \forall\, c = 0,1,\dots,C \tag{5.33}$$

$$y_{ij}^k \in \{0,1\},.\ f_{ij}^{kc} \in \{0,1\},.\ x_{ij}^{kc} \geq 0,. \quad m_i^{kc} \geq 0 \qquad \forall\,(i,j)\in A^k, \forall\, i\in N_{-}^{k}, \forall\, k\in K, \forall\, c = 0,1,\dots,C \tag{5.34}$$

To solve the bi-level max-min formulation through the subproblem in Eqs. (5.18)-(5.25), we utilize a tailored extension of a metaheuristic algorithm. Metaheuristic algorithms are designed to address various kinds of complex models and have received considerable attention for solving bi-level programs. For example, the genetic algorithm (Holland, 1992) is a metaheuristic approach that has been successfully employed in solving bi-level formulations (Arroyo & Fernandez, 2009; Calvete et al., 2008; Hecheng & Yuping, 2008; Wang et al., 2007). In addition, this method can be applied to models

with either integer or continuous decision variables in the first level. The particle swarm optimization algorithm (Kennedy & Eberhart, 1995) is another metaheuristic approach that has been widely applied to bi-level formulations (Gao et al., 2011; Marinakis & Marinaki, 2013). There are other kinds of metaheuristics that can be efficiently utilized in solving bi-level programs (e.g., simulated annealing, ant colony optimization). Talbi (2013) offers a review of the application of metaheuristics for solving bi-level programming problems. The main advantage of metaheuristics is their applicability to a bi-level program regardless of its complexity in the inner level (e.g., a bi-level formulation with a nonconvex inner level). Figure 4.2 illustrates the general structure of the proposed modified metaheuristic algorithm applied to solve the subproblem. The proposed procedure explores the most critical components (which is not necessarily the optimal solution because of the heuristic nature of the algorithm) that the attacker should target to maximize the disruption subject to an interdiction budget. This framework reduces the expected required computation as it avoids checking components that are protected since the subset of unprotected components is the input of the metaheuristic algorithm. Note that if protector decision variables take binary values, construction of the subset of unprotected components is straightforward; otherwise, rules can be defined for constructing this subset (e.g., components that are protected less than 10%). After generating initial feasible attacker decisions, the quality of every solution is evaluated through the second level of the subproblem by calculating its corresponding objective value. Note that the quality of generated solutions is assessed from the perspective of the attacker, so a larger disruption is preferable. Then, the best attacker decision is saved for

the procedure of the metaheuristic operation. The new set of solutions is generated through the metaheuristic operation, and generated solutions are evaluated again for the next iteration of the metaheuristic operation. Note that for every first level feasible solution (satisfying the first level constraints), there exists a feasible solution for the second level decision variables. In other words, for every attacker decision ($\hat{Z}$) satisfying the attacker budget constraint, the subsequent defender level has a feasible reaction. Therefore, every solution generated by the metaheuristic should be checked in terms of the feasibility criterion through the first level of the subproblem (generated solution should satisfy the attacker budget constraint). The metaheuristic algorithm continues until the stopping criteria are reached, and the best attacker decision is returned.

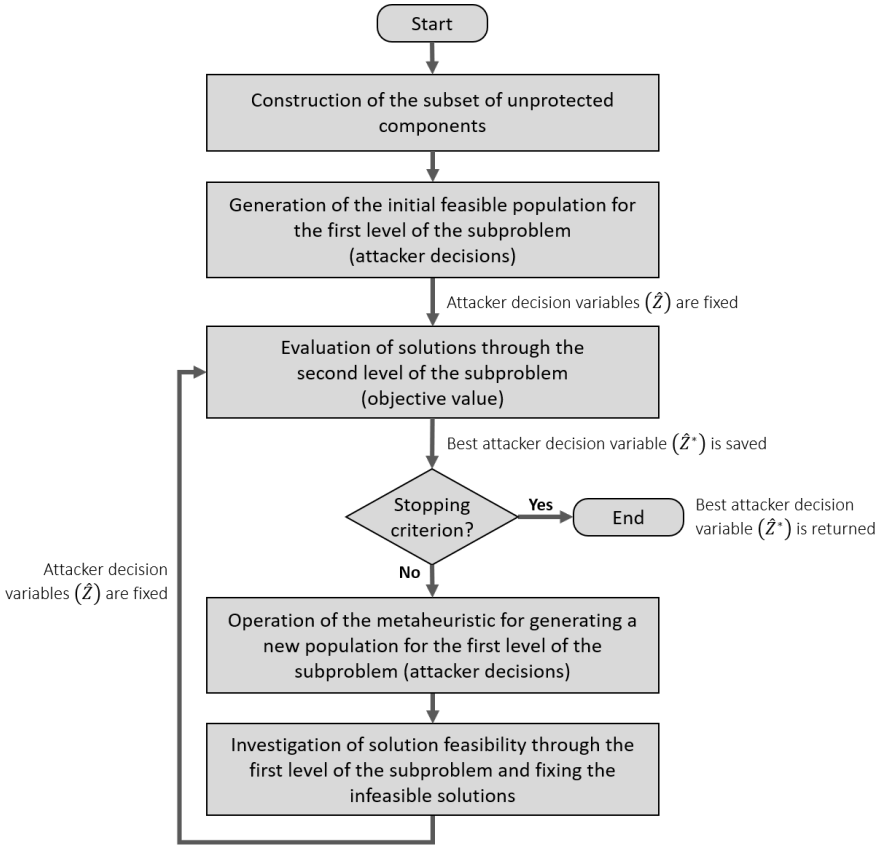


Figure 5.2. A general framework of the proposed modified metaheuristic algorithm for solving the subproblem.

Based on the above discussion for addressing the master problem and subproblem, the implementation steps of the HBD algorithm are represented in Table 5.1. Note that ε is the solution gap set by the decision maker for the algorithm. LB, UB, obj_{MP}, and obj_{SP} refer to the lower bound, upper bound, and master problem (MP) and subproblem (SP) objective values, respectively. $\hat{Y}^*$ and $\hat{Z}^*$ denote the best protection and interdiction decisions, respectively.

At every iteration, the subproblem delivers an effective attack plan for a given protection scenario. Since the subset of unprotected components is fed into the subproblem, the metaheuristic algorithm provides a high-quality solution in a shorter amount of time in comparison to the case of exploring the whole set of components. The master problem is extended with the new attacker scenario accordingly. By iteratively generating a new set of variables and constraints and solving the updated master problem the upper and lower bound values continue to converge until the final solution is obtained. However, the metaheuristic algorithm might not return an optimal attack strategy. Therefore, the newly generated inequality constraint may not change the feasible region of the master problem in some iterations. As a result, the gap between the upper and lower bound values might not be reduced. In such a case, the HBD algorithm is terminated if either (i) the gap between the two bounds is close enough (ε) or (ii) the number of times of returning consecutive unimproved solutions is reached (T), which is recorded in Step 4 of the algorithm. In addition, since the metaheuristic algorithm might

not offer the best attack strategy at each iteration, the final solution might not reflect the maximum capacity of the interdictor according to its resource availability. Hence after the attacker and protector interactions, the upper bound value might become less than the lower bound value which results in terminating the algorithm based on the convergence stopping criteria. To solve this issue, we define a new condition to force the algorithm to continue if the convergence stopping criterion is reached but the upper bound value is less than the lower bound value (referring to Step 2: or $UB < LB$).

Note that the proposed solution algorithm is applicable for either total or partial protection and interdiction decisions. For more clarification, in the binary version of the first defender and attacker decision variables, protected components will be totally immune to any attack. However, in the continuous case, in addition to partial decisions for the attacker, the invulnerability of the components is a function of its fortification.

Table 5.1. Implementation steps of HBD algorithm.

Step 1	Initialization: $LB \leftarrow -\infty$, $UB \leftarrow +\infty$ and $\hat{Z}^c \leftarrow 0$ in $c \leftarrow 0, t \leftarrow 0$
Step 2	**While** $\frac{UB-LB}{LB} > \varepsilon$ **and** $t < T$ **or** $UB < LB$ **do**:
Step 3	Solve MP, obtain its value obj_{MP} and protection decision $\hat{Y}$
Step 4	**If** $obj_{MP} > LB$ **then**: $\hat{Y}^* \leftarrow \hat{Y}$, $LB \leftarrow obj_{MP}$, $t \leftarrow 0$ **Else:** $t \leftarrow t + 1$
Step 5	Solve SP, obtain its value obj_{SP} and interdiction decision $\hat{Z}^*$
Step 6	$c \leftarrow c + 1$
Step 7	$\hat{Z}^c \leftarrow \hat{Z}^*$, $UB \leftarrow \max\{UB, obj_{SP}\}$
Step 8	Update MP by generating a new set of variables and constraints
Step 9	**Exit** (protection decision $\hat{Y}^*$, interdiction decision $\hat{Z}^*$, and obj_{SP} are returned)

5.3.2 Hybrid Set Covering-based (HSC) Algorithm

As discussed in HBD algorithm in Section 5.3.1, Benders decomposition is applied to deal with the bi-level formulation in the master problem. In some cases when the complexity of the master problem is high, as the algorithm iteration grows, the computational time for solving the model increases since a new set of decision variables and constraints are generated at each iteration. Therefore, we utilize the set covering approach to deal with the master problem instead of adding a large number of constraints to the model at each iteration. The HSC algorithm is then a combination of the set covering method and a metaheuristic algorithm.

To convert the master problem to the single-level minimization, an inequality is generated and added to the problem at each iteration of the algorithm. This inequality forces the model to protect at least one interdicted component introduced by the attacker at every iteration. By adding this inequality at every iteration, the feasible region of the master problem is tightened until the model become infeasible and algorithm is terminated. In other words, due to the first defender budget constraint, at one iteration, the master problem cannot satisfy all inequalities added to the model, and the whole algorithm is terminated with the optimal protection decision. For more details, we refer the reader to Israeli and Wood (2002) and Nandi et al. (2016). Then, to solve the subproblem, as with the HBD algorithm, we utilize a metaheuristic algorithm. However, doing so may result in an attacker strategy that might not be optimal. Therefore, the generated inequality might not be distinct from the previous inequalities, resulting in an unchanging feasible region of the master problem at some iterations. In such a case, the

HSC algorithm is terminated if either the master problem becomes infeasible or if a defined number of iterations (T) of consecutive unimproved solutions is reached. Table 5.2 represents the implementation steps of the HSC algorithm. The definition of abbreviations in Table 5.2 are similar to those in the HBD algorithm in Table 5.1. Step 8 of the algorithm records the number of consecutive unimproved solutions. Note that although the master problem in this method is easier to solve compared to the HBD algorithm and computational complexity is reduced in some cases, this approach is only applicable for the binary version of the first and second level decision variables, Y and Z.

Table 5.2. Implementation steps of HSC algorithm.

Step 1	**If** protector budget is enough to protect all components, **then**: $\hat{Y}^* \leftarrow 1, \hat{Z}^* \leftarrow 0, UB \leftarrow 0$ and go to **Step 8**
Step 2	Initialization: $LB \leftarrow -\infty, UB \leftarrow +\infty, \hat{Y} \leftarrow 0, t \leftarrow 0$
Step 3	**While** MP is feasible **and** $t < T$ **do**:
Step 4	Solve SP, obtain its value obj_{SP} and interdiction decision $\hat{Z}$
Step 5	**If** $obj_{SP} < UB$ **then**: $\hat{Y}^* \leftarrow \hat{Y}, \hat{Z}^* \leftarrow \hat{Z}, UB \leftarrow obj_{SP}$
Step 6	Add the following inequalities to MP: $\sum_{k \in K} \sum_{(i,j) \in A^k \mid z_{ij}^k = 1} y_{ij}^k \geq 1$
Step 7	Solve MP, obtain its value obj_{MP} and protection decision $\hat{Y}$
Step 8	**If** $obj_{MP} > LB$ **then**: $LB \leftarrow obj_{MP}, t \leftarrow 0$ **Else:** $t \leftarrow t + 1$
Step 8	**Exit** (protection decision $\hat{Y}^*$ and interdiction decision $\hat{Z}^*$, and UB are returned)

5.4 Illustrative Examples

To illustrate the efficient solvability of the proposed solution techniques, we study the existing DAD model, namely a tri-level protection-interdiction-restoration model discussed in Chapter 3 and solve it for two case studies with different network sizes. Note that the tri-level DAD model has been presented in detail in Chapter 3.

Case study I is the interdependent system of water, gas, and power networks in Shelby County, TN, USA, including 125 nodes and 164 links (González et al., 2016; Hernandez-Fajardo & Dueñas-Osorio, 2011; Song & Ok, 2010). The topology of this system is depicted in Figure 5.3, where the notation w, g, and p refer to water, gas, and power networks, respectively. Note that the dashed lines represent the interdependency relationship between water and power networks in this case study. To assess the performance of the proposed solution approaches for a larger problem, we generated an interdependent system of two networks including 252 nodes and 507 links, representing a double in the size of the Shelby County network. The simulated system was generated using the Networkx library in Python according to the Barabási-Albert network model, thus not fully replicating the structure of the Shelby County network. The main characteristic of this model is the preferential attachment, suggesting that the more connected a node is, the more likely it is to receive new links (Chassin & Posse, 2005; Zadorozhnyi & Yudin, 2014). Figure 5.4 demonstrates the topology of the simulated interdependent system of two networks that we assume to arbitrarily represent water and power networks for illustrative purposes. Like case study I, w and p refer to the water and power networks, respectively, and the dashed lines represent the interdependency relationship between the two networks in this system.

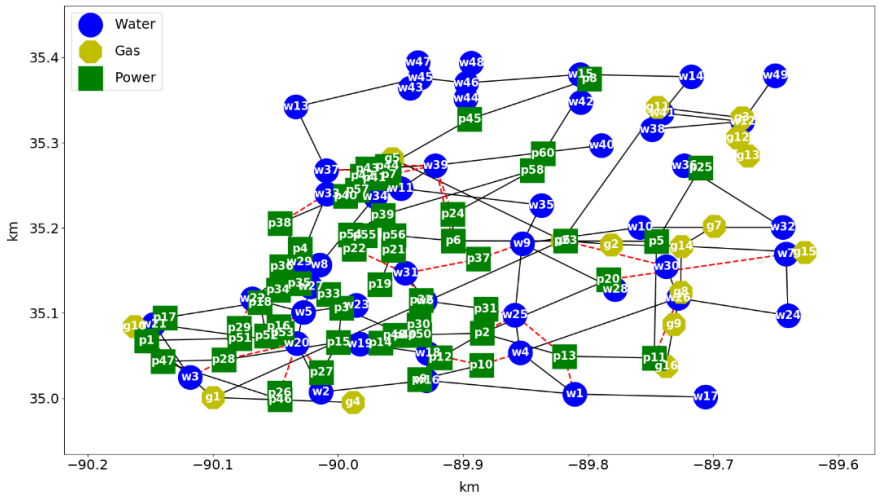


Figure 5.3. The topology of the interdependent system of water, gas, and power networks in Shelby County, TN, USA: case study I.

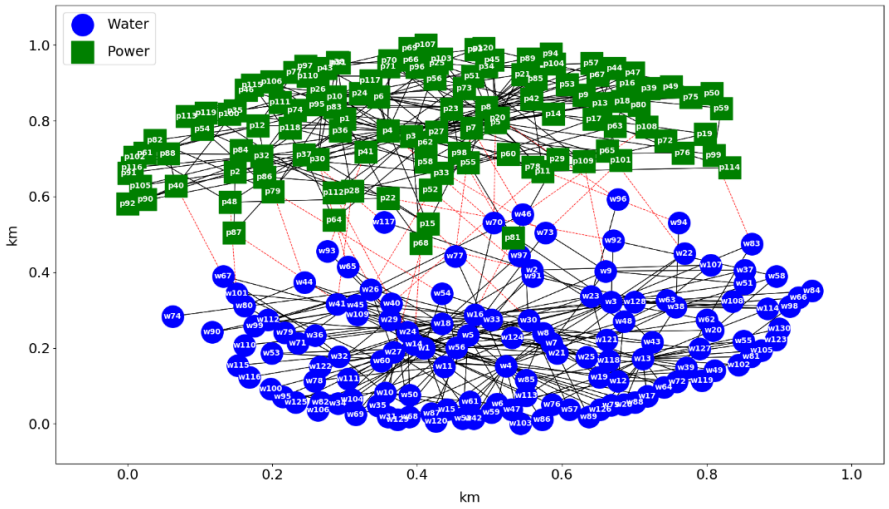


Figure 5.4. The topology of the simulated interdependent system of water and gas networks: case study II.

We implemented the optimization problems and solution algorithms in Python 3.6.5 with Gurobi 8.0.1. Results were conducted on a 64-bit operating system, Intel® Core ™ i7-6700 CPU @ 3.40GHz 3.41GHz desktop computer. In the following sections, we briefly introduce the tri-level DAD formulation discussed in Chapter 3, and we present the results in detail for both case studies.

5.4.1 Computational Results: Case Study I

In this section, we apply the proposed solution techniques to solve the tri-level protection-interdiction-restoration formulation discussed in Chapter 3. To briefly review the model, three levels are involved in this formulation including (i) protection, (ii) interdiction, and (iii) restoration. The protection level implements strategies for hardening network components. The interdiction level identifies the set of components, the disruption of which would result in the maximum damage through the system for a given attack budget. Finally, the restoration level is responsible for restoring the disrupted network to its baseline performance in a timely manner. Compared to the basic formulation presented in Section 5.2, the tri-level protection-interdiction-restoration formulation is more comprehensive as the recovery process of disrupted system is incorporated through the restoration level of the model. Note that the definition of the model sets, indices, parameters, and decision variables, as well as the formulation of the model, have been presented in detail in Chapter 3. Model parameters of the sample problems are selected according to Chapter 3 as well.

To solve the tri-level protection-interdiction-restoration formulation with HBD and HSC algorithms discussed in Sections 5.3.1 and 5.3.2, respectively, we apply the genetic algorithm in the subproblem. The parameters of the genetic algorithm are selected according to Arroyo and Fernandez (2009). The genetic algorithm is stopped when the number of generations is attained. Note that the convergence ratio of the upper and lower bounds in HBD algorithm (e.g., the stopping criterion of HBD algorithm) is set to $\varepsilon = 0.1$. Therefore, the HBD algorithm is terminated if either the gap between the two bounds

is close enough (ε) or the number of times of returning consecutive unimproved solutions is reached (T). However, the HSC algorithm is terminated if either the bi-level master problem becomes infeasible due to the protection budget constraint or the number of times of returning consecutive unimproved solutions is reached (T).

Two criteria are defined to assess the performance of the proposed solution approaches compared to the CD algorithm: (i) the optimality convergence ratio assesses the quality of the solution, and (ii) the computation time rate assesses computation speed. The results of two case studies are discussed in detail subsequently.

The model is solved for different budget scenarios. Table 5.3 and Table 5.4 show the efficiency of HBD and HSC algorithm, respectively, in comparison with the CD algorithm for different protector and attacker budget scenarios. According to the convergence criterion, both solution methods solve the model to optimality for almost all budget scenarios or the percentage of optimality gap is too small to be considered (e.g., 0.01, 0.03). Based on the results, it can be concluded that the proposed solution methods are successful to provide the high-quality solutions for such a complex model and are able to compete with exact solution methods in terms of the accuracy of the solution. Since the convergence ratio of upper bound and lower bound in HBD algorithm is set to 0.1 (e.g., $\varepsilon = 0.1$), the algorithm terminates when the stopping criterion is reached therefore the returned solution might be less than the optimum solution retuned by the CD algorithm.

Table 5.3. Performance evaluation of HBD algorithm with respect to the CD algorithm under different budget scenarios for case study I.

Protector budget (BP)	Attacker budget (BI)	HBD algorithm		CD algorithm		$\left(\frac{\xi^{CD}-\xi^{HBD}}{\xi^{CD}}\right)$	$\left(\frac{r^{CD}}{r^{HBD}}\right)$
		ξ^{HBD}	r^{HBD} (min)	ξ^{CD}	r^{CD} (min)		
0	70	0.51	3.73	0.51	0.08	-	0.02
	140	0.87	3.81	0.87	0.42	-	0.11
	210	1.21	3.83	1.21	1.37	-	0.36
	280	1.78	4.19	1.78	3.63	-	0.87
	350	2.14	4.66	2.14	5.32	-	1.14
40	70	0.22	5.52	0.22	0.15	-	0.03
	140	0.53	5.65	0.53	1.19	-	0.21
	210	0.94	6.11	0.94	4.18	-	0.68
	280	1.21	6.40	1.21	12.74	-	1.99
	350	1.36	6.84	1.40	18.77	0.03	2.74
80	70	0.19	7.47	0.19	0.23	-	0.03
	140	0.45	11.35	0.45	1.56	-	0.14
	210	0.71	13.81	0.71	6.69	-	0.48
	280	0.90	14.76	0.90	29.40	-	1.99
	350	1.13	16.83	1.14	81.53	0.01	4.84
120	70	0.16	11.56	0.16	0.38	-	0.03
	140	0.37	20.11	0.37	3.13	-	0.16
	210	0.59	23.00	0.59	18.76	-	0.81
	280	0.80	49.05	0.80	100.87	-	2.06
	350	0.94	64.04	0.94	291.72	-	4.56
160	70	0.15	13.03	0.15	0.44	-	0.03
	140	0.32	21.04	0.32	4.73	-	0.23
	210	0.47	31.88	0.47	48.72	-	1.53
	280	0.61	65.40	0.61	269.82	-	4.13
	350	0.76	94.84	0.76	1021.61	-	10.77

Table 5.4. Performance evaluation of HSC algorithm with respect to the CD algorithm under different budget scenarios for case study I.

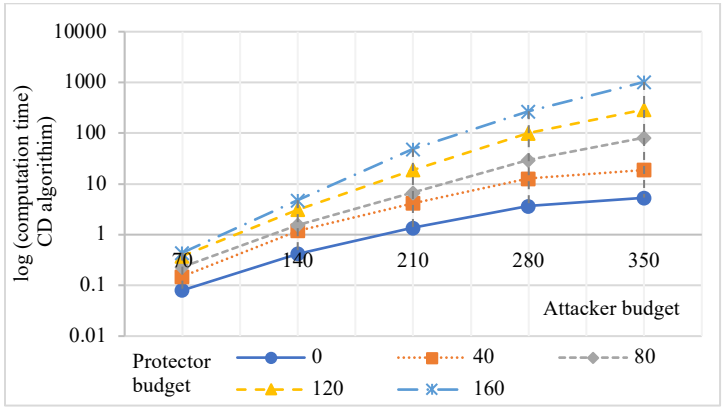
Protector budget (BP)	Attacker budget (BI)	HSC algorithm		CD algorithm		$\left(\frac{\xi^{CD}-\xi^{HSC}}{\xi^{CD}}\right)$	$\left(\frac{r^{CD}}{r^{HSC}}\right)$
		ξ^{HSC}	r^{HSC} (min)	ξ^{CD}	r^{CD} (min)		
0	70	0.51	1.84	0.51	0.08	-	0.04
	140	0.87	1.95	0.87	0.42	-	0.22
	210	1.21	2.01	1.21	1.37	-	0.68
	280	1.78	2.07	1.78	3.63	-	1.75
	350	2.14	2.13	2.14	5.32	-	2.50
40	70	0.22	3.66	0.22	0.15	-	0.04
	140	0.53	3.79	0.53	1.19	-	0.31
	210	0.94	3.86	0.94	4.18	-	1.08
	280	1.21	10.04	1.21	12.74	-	1.27
	350	1.40	11.10	1.40	18.77	-	1.69

80	70	0.19	5.35	0.19	0.23	-	0.04
	140	0.45	9.14	0.45	1.56	-	0.17
	210	0.71	11.53	0.71	6.69	-	0.58
	280	0.87	19.82	0.90	29.40	-	1.48
	350	1.13	46.41	1.14	81.53	0.01	1.76
120	70	0.16	9.13	0.16	0.38	-	0.04
	140	0.37	13.04	0.37	3.13	-	0.24
	210	0.59	26.50	0.59	18.76	-	0.71
	280	0.80	73.55	0.80	100.87	-	1.37
	350	0.94	160.88	0.94	291.72	-	1.81
160	70	0.15	10.93	0.15	0.44	-	0.04
	140	0.32	18.17	0.32	4.73	-	0.26
	210	0.47	75.96	0.47	48.72	-	0.64
	280	0.61	161.45	0.61	269.82	-	1.67
	350	0.76	512.60	0.76	1021.61	-	1.99

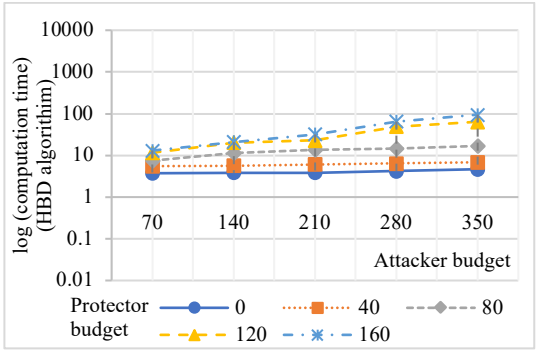
Figure 5.5 depicts the computation time of each solution technique to solve the model under different budget scenarios for case study I. Note that to easily comprehend the comparison for smaller attacker budgets, we alter the vertical axes to a standard logarithmic scale, which is also applied to the remaining figures in this section. The trend indicates that the run times of all three algorithms are affected by the resources available to both protector and attacker. This is likely because, by increasing the budget, possible combinations (feasible solutions) for interdiction and protection grow, therefore the algorithms require more search effort to find the solution and terminate. According to Figure 5.5, the run time of the CD algorithm is more affected by changes in budget relative to the HSC algorithm and then the HBD algorithm, whose run time demonstrates the least susceptibility to budget changes.

Further, with the CD algorithm, the attacker algorithm finds the best strategy based on the component evaluations in a systematic search (implicit enumeration), which guarantees optimality in a finite number of iterations (i.e., component evaluations). To provide further insight regarding this search algorithm, assume that $|N' \cup A'|$ represents

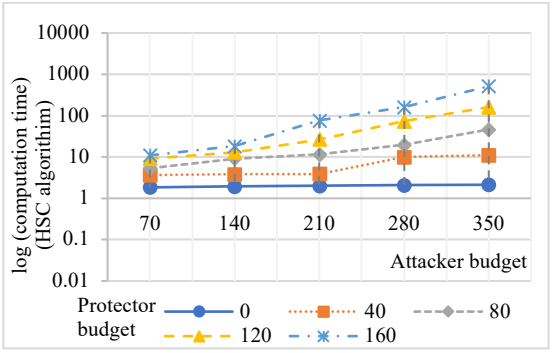
the total number of candidate components subject to interdiction and the attacker can interdict up to n components (cardinality budget for the attacker). Therefore, the total number of node evaluations in this search is $\binom{|N' \cup A'|}{n}$, which grows exponentially with a larger number of candidate components and higher available budget. This is where the advantages of the metaheuristic algorithm, namely the proposed hybrid solution approaches, stand out since all possible combinations are not evaluated.



(a)



(b)



(c)

Figure 5.5. Logarithm of computation time of (a) CD, (b) HBD, and (c) HSC algorithms under different budget scenarios for case study I.

Figure 5.6 illustrates the computation speed of each algorithm with respect to the CD algorithm under different budget scenarios. Mentioned previously, we consider the

standard logarithm of relative speed to enable comparing the result for smaller attacker budgets. The trend reveals that, in general, both HBD and HSC algorithms significantly outperform the CD algorithm with respect to computation time, particularly for higher budget scenarios. For example, for $BP = 80$ and $BI = 350$, the HBD algorithm method solves the model to optimality in about 16 minutes, and HSC method finds the solution in around 46 minutes with an optimality gap ratio of 0.01. This compares with 81 minutes to find the optimal solution with the CD algorithm, which is approximately 5 times slower than HBD and 2 times slower than HSC. For the scenario of $BP = 160$ and $BI = 350$, the computation speed of HBD and HSC algorithms are respectively around 11 and 2 times faster than the CD algorithm. Although the CD algorithm solves the model to optimality, the computational performance of the algorithm decreases exponentially by increasing the size of the problem or the amount of available budget, which is the main shortcoming of the CD solution method. Note that for the lower budget scenarios, the CD algorithm finds the solutions slightly faster than other two solution methods, but the differences in computation time of all three algorithms are small and negligible. In addition, the computational complexity of DAD models emerges when we are dealing with a large-sized problem with higher budget availabilities therefore an algorithm is known to be efficient if it can find the solution for such circumstances with an acceptable accuracy in a reasonable time.

Furthermore, the results indicate that HBD algorithm surpasses HSC in terms of computation speed in case study I. Although the master problem in the second solution algorithm is easier to solve in comparison with the Benders approach in the first

algorithm, it requires more iterations with the addition of new cuts to the model until it becomes infeasible. At each iteration of the algorithm, the best protector solution is recorded by comparing the objective value with the previous iteration (referring to steps 4 and 5 in Table 5.2). Therefore, it may require more iterations relative to Benders approach. With Benders approach, the master problem at each iteration finds the best protection plan by considering all attack strategies proposed to that point, leading to the growth of the master problem by increasing the iteration index. Therefore, there is a tradeoff between the complexity of the master problem in HBD algorithm and the number of iterations of HSC algorithm.

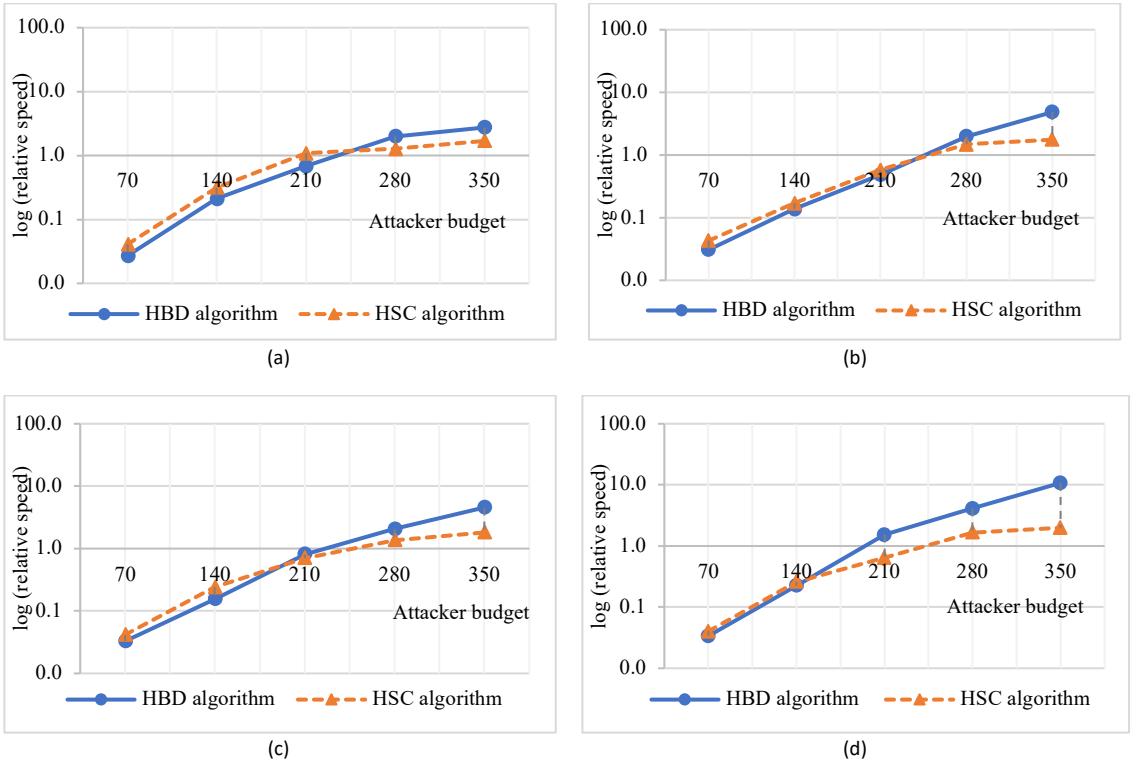


Figure 5.6. Logarithm of relative computation speed of HBD and HSC algorithms with respect to CD algorithm for (a) $BP = 40$, (b) $BP = 80$, (c) $BP = 120$, and (d) $BP = 160$ for case study I.

5.4.2 Computational Results: Case Study II

Table 5.5 and Table 5.6 represent the performance of HBD and HSC algorithms, respectively, compared to the CD algorithm for case study II. Although the size of the network is doubled, both hybrid algorithms perform efficiently in providing high quality results as the optimum solution is returned for almost all scenarios or otherwise the optimality gap is negligible (e.g., 0.05, 0.06).

Table 5.5. Performance evaluation of HBD algorithm with respect to the CD algorithm under different budget scenarios for case study II.

Protector budget (BP)	Attacker budget (BI)	HBD algorithm		CD algorithm		$\left(\frac{\xi^{CD}-\xi^{HBD}}{\xi^{CD}}\right)$	$\left(\frac{r^{CD}}{r^{HBD}}\right)$
		ξ^{HBD}	r^{HBD} (min)	ξ^{CD}	r^{CD} (min)		
0	70	0.26	10.46	0.26	0.25	-	0.02
	140	0.58	10.59	0.58	1.22	-	0.12
	210	0.94	11.09	0.94	4.05	-	0.37
	280	1.51	25.86	1.51	9.23	-	0.36
	350	2.14	29.21	2.14	15.7	-	0.54
40	70	0.21	15.64	0.21	0.47	-	0.03
	140	0.43	26.76	0.43	3.50	-	0.13
	210	0.78	33.80	0.78	15.88	-	0.47
	280	1.18	57.21	1.18	52.82	-	0.92
	350	1.59	178.96	1.69	90.4	0.06	0.51
80	70	0.18	21.53	0.18	0.70	-	0.03
	140	0.39	44.14	0.39	4.78	-	0.11
	210	0.73	47.78	0.73	19.57	-	0.41
	280	1.04	125.46	1.04	81.72	-	0.65
	350	1.30	115.47	1.30	247.45	-	2.14
120	70	0.15	26.92	0.15	0.92	-	0.03
	140	0.35	61.46	0.35	10.25	-	0.17
	210	0.52	69.45	0.52	59.03	-	0.85
	280	0.67	80.60	0.67	239.20	-	2.97
	350	0.86	98.49	0.86	718.75	-	7.30
160	70	0.12	31.92	0.12	1.13	-	0.04
	140	0.26	83.55	0.26	20.00	-	0.24
	210	0.44	131.25	0.44	124.63	-	0.95
	280	0.55	178.11	0.55	618.45	-	3.47
	350	0.68	381.59	0.68	2758.20	-	7.23

Table 5.6. Performance evaluation of HSC algorithm with respect to the CD algorithm under different budget scenarios for case study II.

Protector budget (BP)	Attacker budget (BI)	HSC algorithm		CD algorithm		$\left(\frac{\xi^{CD}-\xi^{HSC}}{\xi^{CD}}\right)$	$\left(\frac{r^{CD}}{r^{HSC}}\right)$
		ξ^{HSC}	r^{HSC} (min)	ξ^{CD}	r^{CD} (min)		
0	70	0.26	5.34	0.26	0.25	-	0.05
	140	0.58	5.48	0.58	1.22	-	0.22
	210	0.94	5.86	0.94	4.05	-	0.69
	280	1.51	6.39	1.51	9.23	-	1.44
	350	2.14	7.64	2.14	15.7	-	2.06
40	70	0.21	11.10	0.21	0.47	-	0.04
	140	0.43	16.83	0.43	3.50	-	0.21
	210	0.78	23.80	0.78	15.88	-	0.67
	280	1.18	31.81	1.18	52.82	-	1.66
	350	1.60	44.20	1.69	90.4	0.05	2.05
80	70	0.18	16.23	0.18	0.70	-	0.04
	140	0.39	27.64	0.39	4.78	-	0.17
	210	0.73	28.37	0.73	19.57	-	0.69
	280	1.04	68.87	1.04	81.72	-	1.19
	350	1.30	134.72	1.30	247.45	-	1.84
120	70	0.15	22.13	0.15	0.92	-	0.04
	140	0.35	43.96	0.35	10.25	-	0.23
	210	0.52	82.91	0.52	59.03	-	0.71
	280	0.67	165.57	0.67	239.20	-	1.45
	350	0.86	509.68	0.86	718.75	-	1.41
160	70	0.12	26.11	0.12	1.13	-	0.04
	140	0.26	69.91	0.26	20.00	-	0.29
	210	0.44	196.28	0.44	124.63	-	0.64
	280	0.55	484.75	0.55	618.45	-	1.28
	350	0.68	1396.73	0.68	2758.20	-	1.98

As a result of increasing the size of the case study, computation times of all three solution algorithms naturally rise for all budget scenarios. Figure 5.7 illustrates the behavior of computational time by increasing the budget availability for each solution algorithm for case study II. Like case study I, we use the standard logarithmic scale for the vertical axes of the figures to clearly see the comparison for smaller attacker budgets. In particular, this trend signifies how the budget change affects the growth of computational burden for each solution algorithm. Like case study I, we see the

substantial sensitivity of the CD algorithm to changes in budget, highlighting the deficiency of this method for higher budget scenarios, as shown in Figure 5.7(a). However, like case study I, the computational complexity of the HBD algorithm is not greatly influenced by the change of budget. This is also true, though less so, for the HSC algorithm.

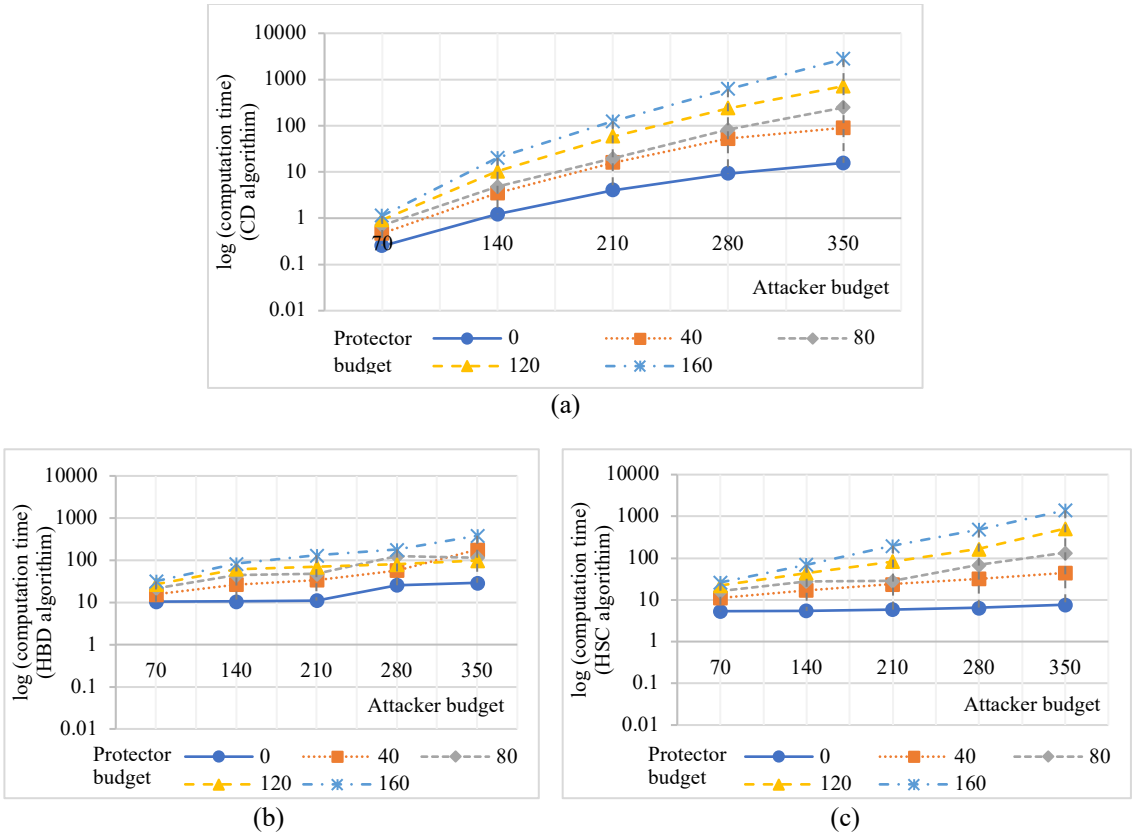


Figure 5.7. Logarithm of computation time of (a) CD, (b) HBD, and (c) HSC algorithms under different budget scenarios for case study II.

Figure 5.8 illustrates the logarithm of computation time of each algorithm relative to the CD algorithm. As shown in the first case as well, the computational times are generally sensitive to the budget availability. In addition, the upward trends for all budget

scenarios indicate the advantages of both HBD and HSC algorithms relative to the CD algorithm in terms of computational burden. Particularly for a given protection budget, as the attacker resource continues to grow, the supremacy of the proposed solution approaches in compared to the CD algorithm enhances remarkably. Like case study I, the HBD algorithm is superior to HSC in terms of computation speed in case study II for higher budget scenarios, as shown in Figure 5.8(c) and (d). However, for the lower budget scenarios, Figure 5.8(a) and (b) suggest that the HSC algorithm outperforms the HBD algorithm. This is because of the significant growth in the complexity of Benders decomposition algorithm applied in HBD algorithm as a result of increasing the size of the network. As we discussed in Section 4.1, at each iteration of HBD algorithm, the master problem is updated by receiving the new set of attacker decisions generated by the subproblem leading to exponential growth of the master problem by increasing the iteration index. However, in the HSC algorithm, the set covering algorithm is applied to solve the bi-level master problem, in which at each iteration only one inequality (cut) will be added to the master problem, enforcing that at least one interdicted component from the recent attacker strategy should be defended. On the other hand, the HSC algorithm requires more iterations to be terminated, which leads to the HBD algorithm outperforming it for higher budget scenarios, shown in Figure 5.8(c), and (d).

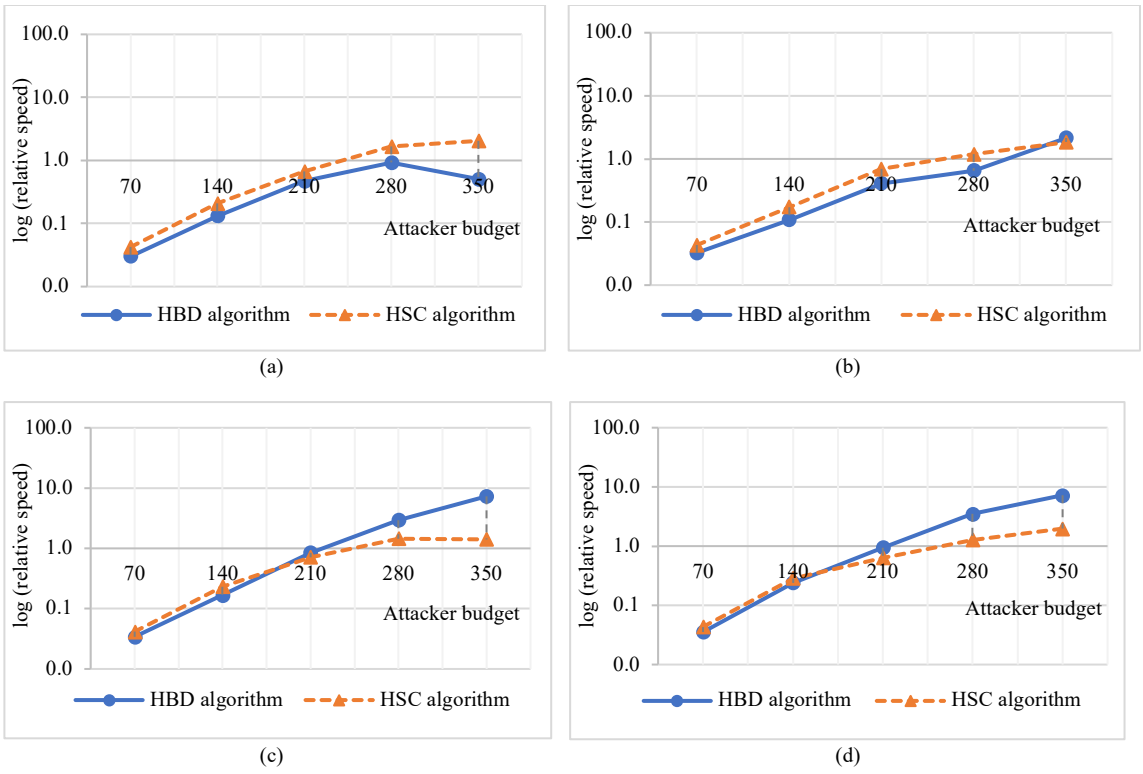


Figure 5.8. Logarithm of relative computation speed of HBD and HSC algorithms with respect to CD algorithm for (a) $BP = 40$, (b) $BP = 80$, (c) $BP = 120$, and (d) $BP = 160$ for case study II.

Note that the accuracy of the proposed solution approaches is affected by the parameters designated for the metaheuristic algorithm, which clearly alter the computational speed of the solution techniques. For example, an additional stopping criterion can be defined for the genetic algorithm in which the difference of the solutions returned by two consecutive generations is zero. Doing so could significantly reduce the run time of the genetic algorithm since it may reach a good solution much earlier than the number of generations allowed. Therefore, this stopping criterion avoids the repetition of the same solution until the number of generations is obtained. However, it might affect the efficiency of the solution in some cases.

5.5 Concluding Remarks

Interdiction models are generally a form of multi-level problems including a series of nested optimization models controlled by a set of constraints and decision variables in which the value of decision variables at each level affect the objective function of other levels (Rahdar, 2016). This kind of models has a wide variety of real-world applications such as defense and military applications, traffic management, and infrastructure networks. However, they are NP-hard problems by nature and challenging to solve. Currently available solution techniques are not successful enough to deal with such a complex model for moderate- or large-size systems. Therefore, considering the widespread applications of interdiction models, development of efficient and effective solution techniques for this problem is the interest of the researchers in recent years. This chapter addressed this by proposing two hybrid solution techniques to overcome the computational complexity of interdiction models particularly DAD formulations. This chapter has provided a comprehensive framework for solving a wide range of tri-level models. The proposed solution approaches are decomposition-based, so tri-level models are broken down into two bi-level formulations including master problem and subproblem. Two methods are combined to deal with the two smaller bi-level problems (master problem and subproblem) iteratively, and subsequently the hybrid solution algorithm is constructed to find the solution for the whole tri-level model. The first solution approach is the HBD algorithm, which combines Benders decomposition method with a metaheuristic approach. The main advantage of this solution technique is its applicability to the broad variety of interdiction models with integer or continuous

decision variables. The second approach is an integration of a set covering method and a metaheuristic algorithm, referred to here as the HSC algorithm.

The proposed solution techniques were demonstrated with the protection-interdiction-restoration model discussed in Chapter 3 as applied to two case studies with different network sizes: (i) the interdependent system of water, gas, and power networks in Shelby County, TN, USA including 125 nodes and 164 links, and (ii) the simulated interdependent system of two networks, including 252 nodes and 507 links. Comparing the results with the exact solutions obtained from the CD algorithm highlight the performance of both HBD and HSC algorithms in providing a high-quality solution, typically the optimal solution for almost all budget scenarios for the tri-level DAD model studied in this dissertation. Particularly for higher budget scenarios, the advantages of both HBD and HSD algorithms are highlighted relative to the CD algorithm. By increasing the size of the problem, we witness that the performance of HSC surpasses HBD solution technique with respect to the computational time for lower budget scenarios. This is because of distinct approaches employed to deal with the bi-level master problem which imposes different levels of complexity to the algorithm. However, this supremacy becomes opposite for the higher budget scenarios. In summary, both solution methods indicated an excellent computational performance compared to the CD algorithm. In addition, the optimality gap for each budget scenario demonstrated the efficient solvability of the two solution approaches for both case studies.

For illustrative purposes, we explored a genetic algorithm to solve the subproblem. However, other metaheuristic approaches can be efficiently incorporated in

both HBD and HSC solution frameworks to deal with the bi-level subproblem. Despite a broad applicability of interdiction models in real world problems and grand challenges, computational complexity is the bottleneck in optimizing such models which make them difficult to employ in moderate- to large-sized cases. Therefore, the development of efficient inexact solution methods is still under investigation and has captured considerable attention for making further improvement to cope with the computational burden of the interdiction models. As an example of additional improvement in HBD algorithm, the master problem is updated at each iteration of the algorithm by receiving the new set of attacker decisions generated by the subproblem, which leads to exponential growth of the master problem by increasing the iteration index. Further, the complexity of the master problem is intensified for large-sized problems. However, the metaheuristic algorithm may not offer the best attack strategy at each iteration which makes the generated constraints (cuts) redundant for the master problem. This redundancy raises the complexity of the problem unnecessarily without tightening the feasible region. For future work, it would be worth to modify the algorithm to deal with the set of redundant constraints (cuts) added to the master problem which could enhance the efficiency of the solution approach. This modification could also be applied to the master problem of the HSC algorithm for additional improvement in computation time. From the modeling point of view, the value of defender secrecy and deception is useful to explore as considering a fully informative interdictor about the system may not be reasonable in some circumstances. In addition, as infrastructure networks have different features that are represented by different physics properties (e.g., Kirchhoff's laws for the power

network, Pascal's principle for the water supply), it would be beneficial to develop a formulation reflecting the general principles of each infrastructure network. We are also interested in extending the formulation by incorporating uncertainty through the model parameters (e.g., available budget, required time for recovering the components). This development could considerably enhance the applicability of the DAD models. Furthermore, in a practical setting, a disruption in one network component may trigger other components resulting in cascading failure throughout the network, and including these cascading characteristics is an area of future research.

Chapter 6: A NETWORK PROTECTION-INTERDICTION-RESTORATION MODEL FOR CASCADING FAILURES

6.1 Introduction and Motivation

Numerous and diverse sources can disrupt critical infrastructure networks, thus potentially interrupting personal lives, societal activity, and economic productivity for extended periods. Cascading failures in infrastructure networks can be especially problematic, as small disruptions have the potential to spread quickly and cause larger scale outages. Cascading failures to critical infrastructures can be originated by just a few initiating incidents such as overloading a line in a power system, closing a road in a transportation system, hindering a pipe in a fluid distribution network, or cutting off a router in an information system. There have been numerous examples of large-scale cascading failures in electric power transmission systems as well as other critical infrastructures. The originating incidents can be result of interruption in load/generation balances inside the network or among networks whose functionalities are dependent. In 2003, a massive power outage occurred in northeast US due to a fault in 3 transmission lines in which multiple critical infrastructure systems were severely impacted (Abraham et al., 2004; Zhou et al., 2021). The 2001 California electricity disruptions is a further example of this incident in power network (Kotzanikolaou et al., 2013). In addition, road networks are extremely susceptible to cascading failures in flood channels because of the co-location dependencies between channels and road networks (Dong et al., 2020). Such a phenomenon occurred in Beijing, when the heaviest rain caused flood channels overloaded resulting in blocking several routes which spread quickly (Huang et al.,

2015). Such domino effects can also arise in computer networks (e.g., the Internet) triggered by failing or disconnected hardware or software in which network traffic is severely diminished or ceased to or between larger segments of the network (Wang et al., 2014). A similar case happened in December 2012, where the Gmail service was severely slowed down for 18 minutes affecting around 40% of users. This loss of service was triggered by an update of load balancing software which contained flawed logic (The Google Apps Team, 2012).

Although cascading events might be rare, they result in catastrophic consequences to multiple critical infrastructures, because of interdependencies, in which large numbers of people are affected in addition to extensive economic loss imposed. As such, the analysis of cascading failures along with deriving effective critical infrastructure protection plans are crucial to prevent or alleviate such an incident and enable resuming system operation as quickly as possible following disruption. Several researchers have investigated network protection techniques to hamper/mitigate the effect of cascading failures through critical infrastructures (e.g., power grids, telecommunication networks, and computer networks). For example, Zio et al. (2012) proposed three protection plans to minimize the effect of cascading failures throughout the system of critical infrastructure networks. To define the initial disruption causing cascading failures, they considered the network interdiction problem producing the worst-case disruption scenario by eliminating one single component (e.g., a component whose removal imposed the maximum loss to the system). However, protecting the network is not performed through network interdiction model like defender-attacker-defender formulations which is used

for optimizing the protection plan. In addition, Li et al. (2013) extended the existing optimization approach (Zio et al., 2012) to enhance cascading failures protection. In this study, line switching was employed to minimize the propagation of failures. Network protection strategies generally fall into two main categories (Zio et al., 2012): (i) enhancing components or allocating redundancies, which improves the tolerance of components against failure or even make them invulnerable to the attack (Ramirez-Marquez et al., 2011; Rocco S., Ramirez-Marquez et al., 2010; Rocco S. & Ramirez-Marquez, 2010; Rocco S & Ramirez-Marquez, 2009), and (ii) switching the lines, which impedes the potential directions to avoid or lessen component overloads (Arroyo & Fernandez, 2009; Fisher et al., 2008; Li et al., 2012; Shao & Vittal, 2005).

Cascading failures is a dynamic incident which may not be halted by human intervention once started (Abraham et al., 2004). Several mathematical models have been proposed to capture the complex mechanisms during the cascading occurrence (Bialek et al., 2016; Papic et al., 2011; Vaiman et al., 2012). Guo et al. (2017) provided a thorough overview of the literature on the treatment and analysis of cascading failures. Chen et al. (2020) proposed a mixed-integer mathematical formulation to specify optimal mitigation and restoration strategies for the system of two interdependent networks subject to cascading failures. However, this study viewed the process of cascading failure from the perspective of physical dependencies in and between the two networks such that the functionality of a set of nodes in one network enables the functionality of a node in or within the networks. In addition, in this study, only a subset of nodes, referred to as "seed nodes," are subject to outage as the initial failures in the model that set about the

cascading failure. Zhou et al. (2021) assessed different restoration strategies for network systems prone to cascading failures. Dueñas-Osorio and Vemuru (2009) investigated the effect of cascading failures in resilience assessment of complex infrastructure systems. In this study, increase flow carrying capacity has been assessed to control overloads due to cascading failures. However, the results indicated that improvements in network components tolerance solely do not suffice to increase cascading robustness, and redundant topology along with other consequence reduction plans are required in addition to the tolerance expansion strategy (Dueñas-Osorio & Vemuru, 2009). Henneaux et al. (2018) assessed the performance of numerous commonly used static cascading outage methodologies referred to as Quasi-Steady-State methodologies in literature. They argued that existing methodologies do not imply a standardized approach for the risk and reliability assessment of cascading outage in power systems. Other works have explored diffusion-type models to represent cascading effects (Rocco et al. 2018), as well as component importance measures for networks subject to cascading failures (Hernández-Perdomo et al., 2016; Rocco et al., 2014; Enrico Zio & Sansavini, 2011)

In a network-based system, the outage of an element generally interrupts the balance of the network and redistribute the flow resulting in overload in adjacent components. This incident may cause additional damage which can propagate throughout the network rapidly (Hernández-Perdomo et al., 2016). To analyze such an effect, several studies built upon the assumption that network load on a component is proportional to the number of shortest paths passing through it (Dong & Cui, 2016; Motter & Lai, 2002; Ren et al., 2016; Zhou et al., 2021). However, such an assumption do not always indicate the

actual routes of the flow in a network-based system. As such, in this chapter, we address optimization of protection strategies of a critical infrastructure network which does not rely on this assumption. The proposed model is a network interdiction formulation, particularly defender-attacker-defender (DAD) model, to enhance the resilience of a network, in other words to optimize the network protection plans, subject to cascading failures triggered by an intentional attack. The proposed model builds on an initial DAD model proposed in Chapter 3 such that the defender, attacker, and defender actions represent protection, interdiction, and restoration actions, respectively. As resilience is often defined as an ability to withstand (with protection actions) and recover (with restoration actions) from a disruption (through an attacker's interdiction actions), this chapter addresses network resilience against cascading failures initiated by intentional attack with a model that accounts for both pre- and post-disruption planning. The proposed interdiction model is a novel DAD model determining (i) which component needs to be protected prior to the disruptive event, (ii) which component is critical in terms of its failure by itself along with causing other parts failures defined as cascading failures, and (iii) what restoration crew schedule is efficient following a disruptive event. To illustrate the benefits of the model, we present a case study of IEEE 9-bus electric power system consisting of 9 buses, 3 generators, and 3 loads (Kaur & Kumar, 2016; Loji et al., 2019; Sharma & Patel, 2016; Sharma et al., 2017).

The rest of the chapter is structured as follows, In Section 6.2, the methodological framework is provided, in which we discuss about model assumptions and notation along with the introduction of model formulation. An illustrative example is provided in

Section 6.3, based on the single structured network of IEEE 9-bus power system. Finally, Section 6.4 provides concluding remarks and general extension of this research work.

6.2 Methodological Framework

In this chapter, we focus on improving the resilience of a single structured network (e.g., optimizing the network protection plans) against cascading failures caused by an intentional attack. Building on an existing resilience interdiction model discussed in Chapter 3, we incorporate the cascading effect into the third level of the proposed tri-level protection-interdiction-restoration model. Once an element is intentionally interdicted, the network flow is redistributed, which may cause overloading and subsequent disruptions in neighboring components. To achieve the aim, three actions are performed in this formulation in three levels successively, as depicted in Figure 3.1, including: (i) the protection action in the first level of the model to protect the network to minimize network vulnerability in an efficient manner, (ii) the interdiction action in the second level of the model to inflict the worst case disruption scenario by considering the current situation of the network (e.g., the protection plan employed), and (iii) the restoration action in the third level of the model to enable the disrupted network to resume its normal operation as quickly as possible.

We assume that protecting the network is performed by adding redundancy and surge protection to the system in which the protected component becomes invulnerable to any form of disruption, and it can be temporary deactivated in the unbalanced state. The interdiction level determines the most critical components by considering the current situation of the network (e.g., the protection plan presumed to be employed), which gives

clue to the protector at each turn of their performance. This level does not necessary represent a human-made attack and could refer to a worst-case operational failure or natural disaster, among others. The restoration level proposes the recovery plan for the disrupted network by scheduling and assigning the available work crews. Notably, both protector and interdictor simultaneously account for (i) how much immediate drop imposes to the system because of their decisions and (ii) how long it takes for the disrupted network to return to the standard situation. Clearly, the two mentioned outcomes are intended to be maximized by the attacker, and the protector, on the other hand, aims to minimize them. Despite a limited budgets for protection and interdiction, they both have complete information about the network topology and each other's decisions at each turn of their performance.

In addition, since we deal with a network comprised of interconnected components, the disruption of one or few components may trigger further events in nearby components due to overloading. Hence, in this study, the interdictor not only considers the effect of a direct disruption to the network, but also accounts for cascading failures caused by their decision. The protector, on the other hand, also takes into account the effect of failure by itself as well as its cascading failure impact through the network. Note that the restoration process is required for the disrupted components which are directly targeted by the attacker as well as those that become overloaded due to the cascading failure. In the proposed mathematical model, the protected components will be immune to any direct attack and can be temporary switched off (deactivated) once they receive the excessive load. However, unprotected components can fail as a result of either

the direct attack or overload. In the proposed interdiction model, we consider period 1 as the disruption time when the initial and intentional attack occurs. As a result of this failure, flow is redistributed in such a way that may cause excessive load reaching to adjacent nodes. Therefore, such adjacent nodes subsequently either fail or become deactivated depending on their protection status. Once the network is stabilized and disrupted nodes are determined, the restoration process commences from period 2 up until the network returns to its normal operation defined as the steady state of recovery process in this formulation. This process is depicted in Figure 6.1.

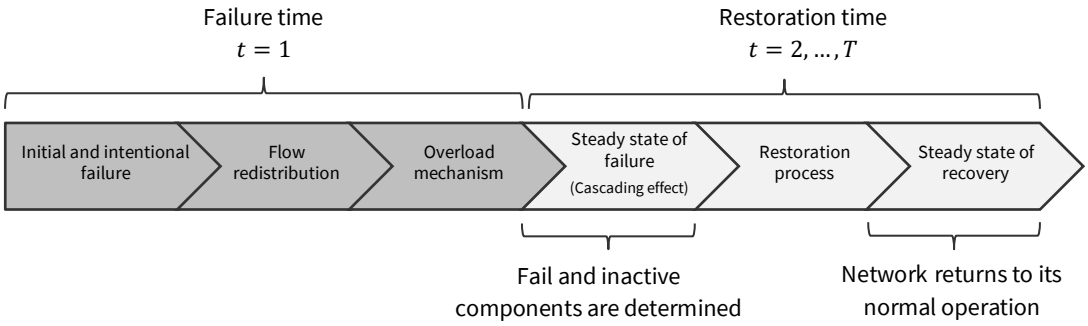


Figure 6.1. The general process of the proposed model following an intentional attack.

Figure 6.2 provides a small illustration of cascading failures process in the proposed model. Initially (period 1), node 4 is intentionally attacked, shown in Figure 6.2a, triggering overload in transshipment node 3, as depicted in Figure 6.2b. As a result, supply nodes 1 and 2, and demand nodes 9, 7, and 8 will be temporarily deactivated in period 2. Figure 6.2c illustrates the steady state of failure at the beginning of period 2 during which the restoration process starts for nodes 3 and 4. While the restoration process continues, supply nodes will be reactivated once they can operate with their

maximum capacity, and demand nodes are labeled reactivated a soon as they can be fully met. It is assumed that the restoration process does not trigger cascading failures.

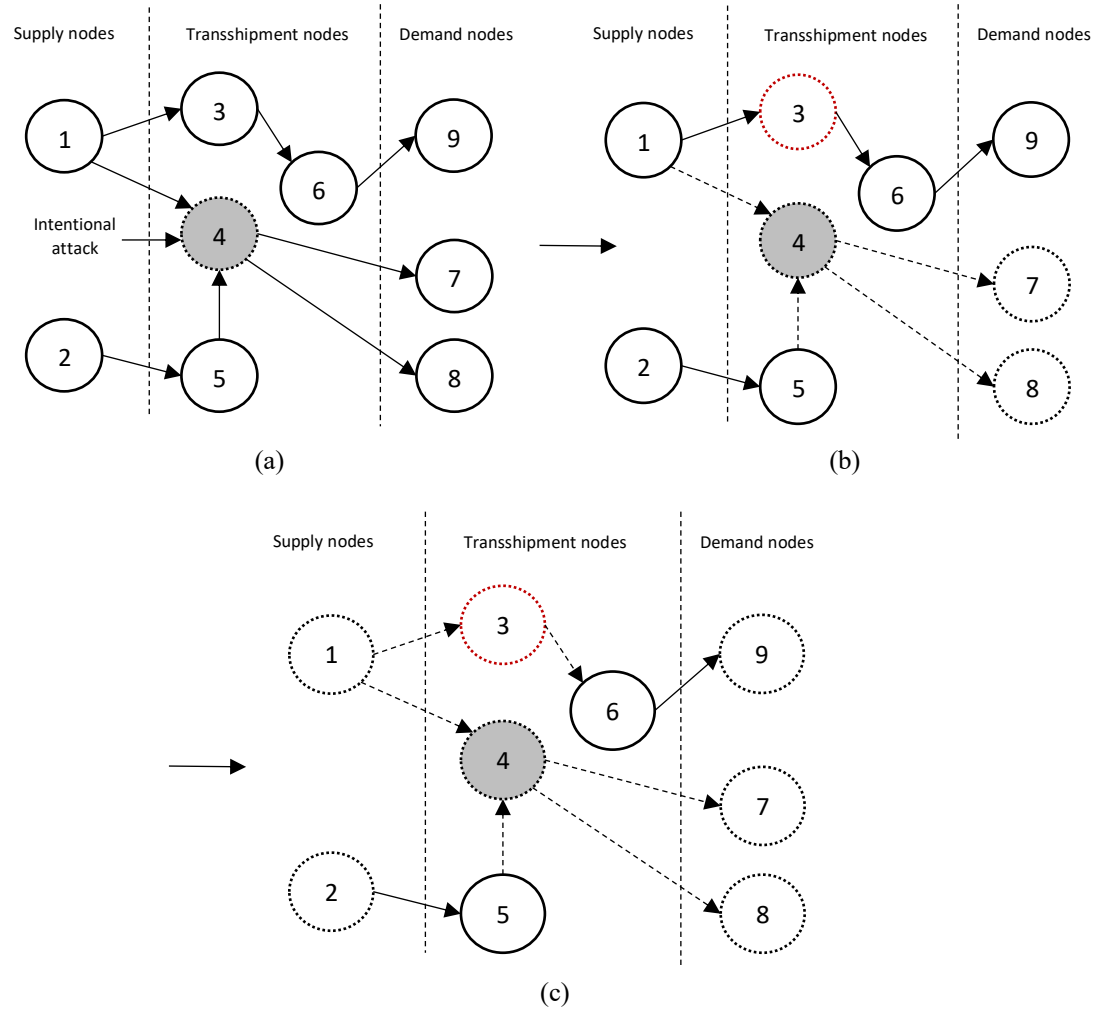


Figure 6.2. A schematic plot of cascading failures initiating by an intentional attack.

6.2.1 Model Assumptions and Notation

We particularly focus on a single critical infrastructure, and we model it as a general network flow problem. In this way, other general cascading failures in infrastructure (or other) networks represented with network flow models could also be

captured with the proposed model. To capture the operation of a critical infrastructure following a disruptive event, the proposed optimization model has the following underlying characteristics associated with the structure and operation of the network, failure (including cascading failure), and recovery process, among others.

- The network consists of a set of nodes (including supply, demand, and transshipment nodes) connected by a set of links, such that each supply node, demand node, transshipment node, and link have known supply capacity, demand, load capacity, and flow capacity, respectively.
- Supply nodes are switched off unless they can supply with their full capacity. Similarly, demand nodes are switched off unless they can be fully satisfied.
- Nodes are the only components that can be protected and interdicted.
- Transshipment nodes are the only nodes prone to overload.
- All nodes are susceptible to cascading failures occurring in two forms: (i) overload of transshipments nodes and (ii) temporary deactivation of supply and demand nodes.
- There are known cardinality budgets available for protecting and for interdicting the nodes.
- Protected nodes will be invulnerable to any forms of failure including intentional attack and overload such that protected transshipment nodes will be temporary switched off (disconnected) because of overload (e.g., recovery is not required for a protected node).

- Unprotected components can fail because of either the direct attack or overload (e.g., excessive load causes cascading failures in transshipment nodes) in which failed nodes need to be restored in either type of failure.
- There are work crews responsible for repairing disrupted components in the network.
- A work crew can only work on a single disrupted component at a time. A disrupted component can be restored by a single work crew (once the disrupted component is assigned to them) until they become operational.
- There is a known restoration rate for each component, λ, representing the proportion of the component restoration per unit time by each work crew.
- Restoration time for each disrupted component is a function of both its failure and its restoration rate, both of which can vary by component.

We denote an undirected network by $G = (N, A)$, where N is the set of nodes, and A is the set of links. Nodes can be supply nodes ($N_+ \subseteq N$), demand nodes ($N_- \subseteq N$), and transshipment nodes ($N_= \subseteq N \setminus \{N_+, N_-\}$) such that $N_+ \cap N_- \cap N_= = \emptyset$. Note that it assumes a single commodity flows through the network. Set R represents the available work crews in the network for the restoration task. Index t refers to the index of time period. Table 6.1 and Table 6.2 outline the model parameters and decision variables, respectively. Note that we do not consider candidate components subject to protection and interdiction. However, all nodes are subject to direct attack and susceptible to cascading failures in this study.

Table 6.1. Model parameters.

w_{it}	Importance weight assigned to node $i \in N_-$ at time t
BP	Cardinality budget for the protector
BI	Cardinality budget for the interdictor
s_i	Amount of supply in node $i \in N_+$
d_i	Amount of demand in node $i \in N_-$
l_i	Number of links connected to node $i \in N_+$
u_i	Capacity of node $i \in N_=$
u_{ij}	Capacity of link $(i,j) \in A$
λ_i	Restoration rate of node $i \in N$
M	An arbitrarily large positive number

Table 6.2. Model decision variables.

v_{it}	Equal to 1 if supply node $i \in N_+$ can supply with its full capacity in time t, binary
o_{it}	Equal to 1 if demand node $i \in N_-$ can be fully met in time t, binary
b_i	Dummy variable holding inflow of node $i \in N_=$ if either inflow is strictly greater than the node capacity or such a node is directly interdicted, continuous
θ_i	Dummy variable holding inflow of node $i \in N_-$ if such a node cannot receive the flow, continuous
x_{ijt}	Flow on link $(i,j) \in A$ in time t, continuous
y_i	Equal to 1 if node $i \in N$ is protected, binary
z_i	Equal to 1 if node $i \in N$ is interdicted, binary
f_i	Equal to 1 if node $i \in N$ is disrupted because of direct attack, binary
cf_i	Equal to 1 if cascading disruption occurs in node $i \in N$, binary
α_{it}^r	Equal to 1 if node $i \in N$ is being restored by work crew $r \in R$ in time t, binary
β_{it}	Equal to 1 if disrupted node $i \in N$ is reactivated at time t, binary
g_i	Equal to 1 if inflow of node $i \in N_=$ is greater than the node capacity, binary
h_i	Variable used to ensure inflow of node $i \in N_=$ traverses if inflow is strictly less than the node capacity, binary
q_{i1}	Variable used for linearizing the product of two binary variables for node $i \in N_+$, binary

6.2.2 Model Formulation

In this section, we present details of the proposed tri-level DAD model shown by constraints (6.1)-(6.57) including the objective function, protection and interdiction actions along with the impact of their interactions, and recovery process of the failed components.

6.2.2.1 Objective Function

As the performance metric for the decision made at each level of the model, we consider the cumulative weighted fraction of unmet demand over a time period $[\boldsymbol{0}, \boldsymbol{T}]$ such that this value is minimized by the first defender, maximized by the attacker, and minimized by the subsequent defender, as shown in Eqs. (6.1) and (6.2). Parameter $\boldsymbol{d_i}$ represents the amount of demand met prior to the disruption. If node $\boldsymbol{i} \in \boldsymbol{N\_}$ can be fully satisfied in time $\boldsymbol{t}$, binary variable $\boldsymbol{o_{it}}$ is forced to set to 1, otherwise the demand node remains switched off (deactivated). Note that parameter $\boldsymbol{w_{it}}$ enables the decision maker to prioritize the demand satisfaction in some nodes relative to others at time $\boldsymbol{t}$.

$$\zeta(t) = 1 - \left(\frac{\sum_{i \in N\_} w_{it} \, (d_i - d_i o_{it})}{\sum_{i \in N\_} w_{it} \, d_i} \right) \quad \forall \, t \tag{6.1}$$

$$\xi = \min \max \min \sum_{t=1}^{T} \zeta(t) \tag{6.2}$$

6.2.2.2 Protection and Interdiction Actions

As we discussed in Section 6.2.1, there are known cardinality budgets available for protecting and for interdicting nodes denoted by parameters BP and BI, respectively. This suggests that the protector could protect up to BP components and the attacker could interdict up to BI components in the network. Accordingly, constraints (6.3) and (6.4) represent the budget restrictions for the protection and interdiction decisions, respectively. Protecting the network component is performed in the form of adding redundancy and installing precocious protection device to the system. Constraints (6.5)

and (6.6) show the nature of the decision variables for the first and second levels of the model.

$$\sum_{i \in N} y_i \leq BP \tag{6.3}$$

$$\sum_{i \in N} z_i \leq BI \tag{6.4}$$

$$y_i \in \{0,1\} \qquad \forall\, i \in N \tag{6.5}$$

$$z_i \in \{0,1\} \qquad \forall\, i \in N \tag{6.6}$$

6.2.2.3 Impact of Protection and Interdiction Interactions: Failure Time

As we discussed previously, unprotected components can fail because of the direct attack. In addition, failure of one or few components can trigger the disruption of other components since the load balance is unexpectedly interrupted through the network. Due to this sudden interruption in the network, further incidents may occur such as overload of transshipment nodes or deactivation of supply and demand nodes which we define them as cascading failures in this study. However, protected transshipment nodes become switched off (deactivated) once they receive excessive load and they remain inactive until the network return to the balanced situation. We consider period 1 as the disruption time when the initial (direct) attack by the interdictor occurs. Once the disruption process (e.g., cascading effects) is stabilized, and the failed components are determined, the restoration process commences from period 2 to return the disrupted network to the balanced situation in a timely manner. Therefore, two sets of constraints are involved in the third level of the formulation representing the failure time taken place

at period 1 and the restoration time performing during a time period $[2, T]$ which we discuss them separately.

In this section, we present the set of constraints involved in failure time occurred at period 1, as shown by Constraints (6.7)-(6.34), to determine the set of components failed either directly or as a result of other parts failures. Then, Section 6.2.2.4 provides the set of constraints employed in restoration scheduling performing during a time period $[2, T]$, as represented by Eqs. (6.38)-(6.57).

Constraints (6.7)-(6.9) deliver failure status for node $\forall\, i \in N$ following an initial attack depending on the protection and interdiction strategies such that the protected components are invulnerable to the attacker. Similarly, protected node $\forall\, i \in N_{=}$ will be immune to cascading failure represented by Constraints (6.10) since it is equipped with a surge protector. Nodes failed either directly or as a result of other parts failure both of which fall into the category of cascading failure for further restoration consideration, as shown by Constraints (6.11). Constraints (6.12) guarantee that supply node $\forall\, i \in N_{+}$ supply with its full capacity at time $t = 1$ only if neither such a node nor its entire connected nodes are not failed directly by the attacker. Note that because of the product of two binary variables v_{i1} and f_i, this equation is nonlinear in which the linearization form of this constraint will be presented at the end of this section. Constraints (6.13) ensure that binary variable v_{i1} is set to one if node $\forall\, i \in N_{+}$ has at least one active connected node, otherwise it obtains the value of zero. Constraints (6.14) are the balance constraints for transshipment node $\forall\, i \in N_{=}$ in period 1. Dummy variable b_i in this constraint holds the inflow of node $\forall\, i \in N_{=}$ only if the inflow cannot traverse due to the

capacity restriction of the given node. Constraints (6.15) guarantee that demand node $\forall\, i \in N_{-}$ is active in period 1 if it can be fully satisfied, otherwise it remains switched off (inactivated). Dummy variable θ_i holds the inflow of demand node $\forall\, i \in N_{-}$ if the inflow is strictly less than the amount of demand required. Constraints (6.16) represent that demand node $\forall\, i \in N_{-}$ can not be active if it is directly failed by the attacker at time $t = 1$. Constraints (6.17) represent the capacity restriction for each transshipment node $\forall\, i \in N_{=}$. Constraints (6.18) and (6.19) together guarantee that if transshipment node $\forall\, i \in N_{=}$ is overloaded, the inflow will be fully carried by variable b_i which is linked to constraints (6.14) as well. Constraints (6.20)-(6.22) together force the inflow of transshipment node $i \in N_{=}$ traverses over link (i, j) if the ending node of such a link is not failed directly by the attacker and the inflow is strictly less than the given node capacity, otherwise variable b_i holds the inflow of the node. Constraints (6.23) ensure that the protected node $\forall\, i \in N_{=}$ does not fail as a result of overload (signified as one form of cascading failure in this study), and it becomes temporary switched off (inactivated) such that recovery is not required (e.g., assume that a protected node is equipped with surge protection). Constraints (6.24) ensure that a positive flow through any given link can be attained at period 1 if the starting node of such a link is not failed (even directly or as a result of other parts failure). Constraints (6.25) ensure that a positive flow through any given link can be attained at period 1 if the ending node of such a link is not directly failed by the attacker. Finally, constraints (6.26)-(6.34) represent the nature of the decision variables for the set of constraints involved in at the failure in period 1 of the third level of the model.

Parameter M in constraints (6.18)-(6.25) represents a big number by some means, and it needs to be greater than the maximum inflow imposed to the transshipment nodes following a disruptive event (e.g., overload occurs once the balance of the network is interrupted). As such, parameter M can be adjusted depending on the scale of the network and the maximum amount of supply nodes.

$$y_i + (1 - z_i) + f_i \geq 1 \qquad \forall\, i \in N \qquad (6.7)$$

$$f_i \leq z_i \qquad \forall\, i \in N \qquad (6.8)$$

$$y_i \leq 1 - f_i \qquad \forall\, i \in N \qquad (6.9)$$

$$y_i \leq 1 - cf_i \qquad \forall\, i \in N_{=} \qquad (6.10)$$

$$f_i \leq cf_i \qquad \forall\, i \in N \qquad (6.11)$$

$$\sum_{(i,j)\in A} x_{ij1} - \sum_{(j,i)\in A} x_{ji1} = s_i v_{i1}(1 - f_i) \qquad \forall\, i \in N_{+} \qquad (6.12)$$

$$l_i v_{i1} \geq \sum_{j\in N} (1 - f_j) \qquad \forall\, (i,j) \in A \,|\, \forall\, i \in N_{+} \qquad (6.13)$$

$$\sum_{(j,i)\in A} x_{ji1} = \sum_{(i,j)\in A} x_{ij1} + b_i \qquad \forall\, i \in N_{=} \qquad (6.14)$$

$$\sum_{(i,j)\in A} x_{ij1} - \sum_{(j,i)\in A} x_{ji1} = -\, d_i o_{i1} - \theta_i \qquad \forall\, i \in N_{-} \qquad (6.15)$$

$$f_i \leq 1 - o_{i1} \qquad \forall\, i \in N_{-} \qquad (6.16)$$

$$\sum_{(i,j)\in A} x_{ij1} \leq u_i \qquad \forall\, i \in N_{=} \qquad (6.17)$$

$$\sum_{(i,j)\in A} x_{ij1} \leq (1 - g_i)M \qquad \forall\, i \in N_{=} \qquad (6.18)$$

$$b_i \leq g_i M \qquad \forall\, i \in N_{=} \qquad (6.19)$$

$$\sum_{(j,i)\in A} x_{ji1} \leq u_i + h_i M \qquad \forall\, i \in N_{=} \qquad (6.20)$$

$$\sum_{(j,i)\in A} x_{ji1} > u_i - (1 - h_i)M \qquad \forall\, i \in N_{=} \qquad (6.21)$$

$$b_i \leq \left(h_i + f_j\right)M \qquad \forall\,(i,j) \in A \mid \forall\, i \in N_{=} \qquad (6.22)$$

$$b_i - u_i \leq (cf_i + y_i)M \qquad \forall\, i \in N_{=} \qquad (6.23)$$

$$x_{ij1} \leq Mu_{ij}(\,1 - cf_i) \qquad \forall\,(i,j) \in A \qquad (6.24)$$

$$x_{ij1} \leq Mu_{ij}\left(\,1 - f_j\right) \qquad \forall\,(i,j) \in A \qquad (6.25)$$

$$f_i \in \{0,1\} \qquad \forall\, i \in N \qquad (6.26)$$

$$cf_i \in \{0,1\} \qquad \forall\, i \in N \qquad (6.27)$$

$$v_{i1} \in \{0,1\} \qquad \forall\, i \in N_{+} \qquad (6.28)$$

$$o_{i1} \in \{0,1\} \qquad \forall\, i \in N_{-} \qquad (6.29)$$

$$g_i \in \{0,1\} \qquad \forall\, i \in N_{=} \qquad (6.30)$$

$$h_i \in \{0,1\} \qquad \forall\, i \in N_{=} \qquad (6.31)$$

$$b_i \geq 0 \qquad \forall\, i \in N_{=} \qquad (6.32)$$

$$x_{ij1} \geq 0 \qquad \forall\,(i,j) \in A \qquad (6.33)$$

$$l_i \geq 0 \qquad \forall\, i \in N_{-} \qquad (6.34)$$

Constraints (6.12) are nonlinear equations. To linearize them, the product of two binary variables, v_{i1} and f_i, is replaced by new binary variables, q_{i1}. These linear constraints are represented in Eqs. (6.35)-(6.37).

$$q_{i1} \leq v_{i1} \qquad \forall\, i \in N_{+} \qquad (6.35)$$

$$q_{i1} \leq f_i \qquad \forall\, i \in N_{+} \qquad (6.36)$$

$$v_{i1} + f_i \leq 1 + q_{i1} \qquad \forall\, i \in N_{+} \qquad (6.37)$$

6.2.2.4 Restoration Scheduling: Restoration Time

This section provides the set of constraints employed in restoration scheduling performing during a time period $[2, T]$ shown by Eqs. (6.38)-(6.57). Once the failure

process reaches at the steady state, both directly failed and overloaded nods pass the restoration process for reactivation which we discuss it in detail subsequently.

Constraints (6.38)-(6.40) guarantee the flow balance at node $i \in N$ over a time period $[2, T]$. Constraints (6.41) represent the capacity in node $\forall\, i \in N_{=}$. Constraints (6.42) ensure that the amount of positive flow through any given link cannot exceed the link capacity. Constraints (6.43) ensure that operational nodes are not restored. Constraints (6.44) and (6.45) ensure that a positive flow through any given link can be attained at a period $t|\, t \neq 1$ only if the starting and ending nodes of such a link are operational or were already recovered. Constraints (6.46) ensure that the restoration task of a disrupted link is continued without interruption once it has commenced. Constraints (6.47) and (6.48) calculate the total time that a specific work crew should be assigned to restore a disrupted node. Note that constraints (6.47) and (6.48) together help to deliver integer value for the total required recovery time of an element. Constraints (6.49) ensure that once the disrupted node is fully restored at time $t|\, t \neq 1$, they are labeled reactivated from the next period $(t+1|\, t \neq 1)$ to the end of the time horizon of the model. Constraints (6.50) ensure that once the restoration of a disrupted node commences by a work crew at time $t|\, t \neq 1$, that specific work crew completes restoration of that node. Constraints (6.51) state that, at the given time $t|\, t \neq 1$, only one work crew can work on the restoration task of a specific disrupted node. Constraints (6.52) ensure that, at the given time $t|\, t \neq 1$, only one disrupted node can be restored by a given work crew. Finally, constraints (6.53)-(6.57) represent the nature of the decision variables for the restoration level during a time period $[2, T]$.

Parameter M in constraints (6.49) and (6.50) only needs to be greater than the maximum required time for restoring the disrupted components.

$$\sum_{(i,j)\in A} x_{ijt} - \sum_{(j,i)\in A} x_{jit} = s_i v_{it} \qquad \forall\, i \in N_+, \forall\, t | \, t \neq 1 \qquad (6.38)$$

$$\sum_{(i,j)\in A} x_{ijt} - \sum_{(j,i)\in A} x_{jit} = 0 \qquad \forall\, i \in N_=, \forall\, t | \, t \neq 1 \qquad (6.39)$$

$$\sum_{(i,j)\in A} x_{ijt} - \sum_{(j,i)\in A} x_{jit} = -\, d_i o_{it} \qquad \forall\, i \in N_-, \forall\, t | \, t \neq 1 \qquad (6.40)$$

$$\sum_{(i,j)\in A} x_{ijt} \leq u_i \qquad \forall\, i \in N_=, \forall\, t \qquad (6.41)$$

$$x_{ijt} \leq u_{ij} \qquad \forall\, (i,j) \in A, \forall\, t | \, t \neq 1 \qquad (6.42)$$

$$\beta_{it} \leq cf_i \qquad \forall\, i \in N, \forall\, t | \, t \neq 1 \qquad (6.43)$$

$$x_{ijt} \leq u_{ij}(\, 1 - cf_i + \beta_{it}) \qquad \forall\, (i,j) \in A, \forall\, t | \, t \neq 1 \qquad (6.44)$$

$$x_{ijt} \leq u_{ij}\big(\, 1 - cf_j + \beta_{jt}\big) \qquad \forall\, (i,j) \in A, \forall\, t | \, t \neq 1 \qquad (6.45)$$

$$\sum_{e=2}^{t} \alpha_{ie}^{r} \leq M\, \Big(1 - \big(\alpha_{i,t+1}^{r} - \alpha_{it}^{r}\big)\Big) \qquad \forall\, i \in N, \forall\, r \in R, \forall\, t | \, t \neq 1 \qquad (6.46)$$

$$\sum_{r\,\in\, R}\ \sum_{t=2}^{T} \alpha_{it}^{r} \geq \frac{cf_i}{\lambda_i} \qquad \forall\, i \in N \qquad (6.47)$$

$$\sum_{r\,\in\, R}\ \sum_{t=2}^{T} \alpha_{it}^{r} < \left(\frac{cf_i}{\lambda_i} + 1\right) \qquad \forall\, i \in N \qquad (6.48)$$

$$1 - \left(\frac{\frac{cf_i}{\lambda_i} - \sum_{r\,\in\, R}\ \sum_{e=2}^{t} \alpha_{ie}^{r}}{M}\right) \geq\ \beta_{it} \qquad \forall\, i \in N, \forall\, t | \, t \neq 1 \qquad (6.49)$$

$$\sum_{\substack{e\,\in\, R \\ e\neq r}}\ \sum_{t=2}^{T} \alpha_{it}^{e} \leq\ M(1 - \alpha_{it}^{r}) \qquad \forall\, i \in N, \forall\, r\ \in\ R, \forall\, t | \, t \neq 1 \qquad (6.50)$$

$$\sum_{r \in R} \alpha_{it}^{r} \leq 1 \qquad \forall\, i \in N, \forall\, t |\, t \neq 1 \tag{6.51}$$

$$\sum_{i \in N} \alpha_{it}^{r} \leq 1 \qquad \forall\, r \in R, \forall\, t |\, t \neq 1 \tag{6.52}$$

$$v_{it} \in \{0,1\} \qquad \forall\, i \in N_{+}, \forall\, t \tag{6.53}$$

$$o_{it} \in \{0,1\} \qquad \forall\, i \in N_{-}, \forall\, t \tag{6.54}$$

$$x_{ijt} \geq 0 \qquad \forall\, (i,j) \in A, \forall\, t \tag{6.55}$$

$$\alpha_{it}^{r} \in \{0,1\} \qquad \forall\, i \in N, \forall\, r \in R, \forall\, t |\, t \neq 1 \tag{6.56}$$

$$\beta_{it} \in \{0,1\} \qquad \forall\, i \in N, \forall\, t |\, t \neq 1 \tag{6.57}$$

6.3 Illustrative Example

To illustrate the efficient solvability of the model and validate it for cascading failure, we focus on interdiction and restoration levels of this formulation. Therefore, we assume that protection budget is zero, so no node can be protected, and the attacker, on the other hand, determines the best plan for initial disruption subject to their budget availability. As we discussed in Section 6.1, the interdictor not only considers the effect of a direct disruption to the network, but also accounts for cascading failures caused by their decision. To optimally solve the bi-level interdiction-restoration model (subproblem), we apply set-covering decomposition approach discussed in Chapter 4 which delivers the best attacker decision. Not again that the protector decision variables are fixed through model.

We apply the model to IEEE 9-bus electric power test system as the case study. This system is depicted in Figure 6.3 consisting of 9 buses, where 3 generators are connected to bus numbers 1, 2 and 3, respectively, and loads 1, 2, and 3 are connected to bus numbers 5, 6, and 8, respectively. This network includes 15 links, 9 transshipment

nodes, 3 supply nodes, and 3 demand nodes indicated as transmission lines, buses, generators, and loads, respectively.

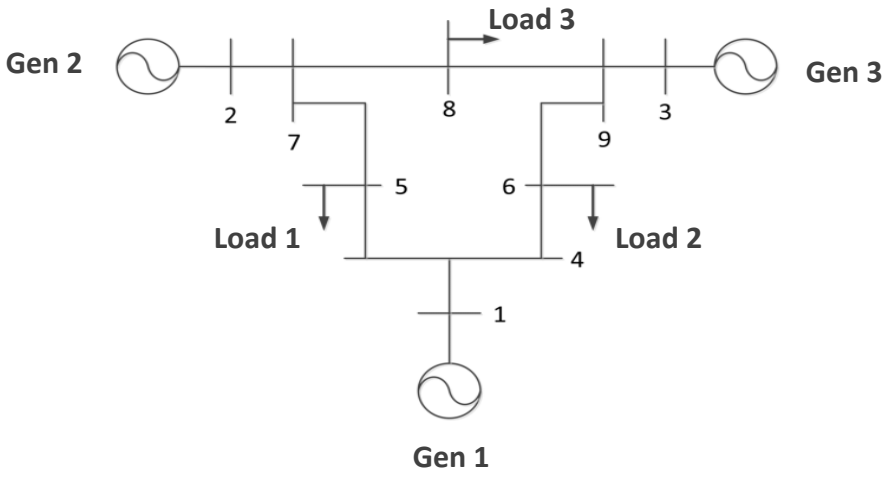


Figure 6.3. Graphical illustration of IEEE 9-bus electric power test system.

Table 6.3 provides load flow report for this system in megawatt (MW) when all generators and loads are operating at rated power. Note that descriptions of the test network are adapted from Kamdar et al. (2014).

Table 6.3. Load flow report of IEEE 9-bus electric power test system (megawatt).

Bus No.	Bus (MW)	Gen. (MW)	Load (MW)
1	75	75	0
2	155	155	0
3	85	85	0
4	75	0	0
5	125	0	125
6	90	0	90
7	155	0	0
8	100	0	100
9	85	0	0

With respect to the model parameters, equal weights (w_{it}) are assigned to the demand nodes, and we consider equal value for the restoration rate (λ_{it}) of the components. Although, in the proposed model, multiple work crews can operate for network recovery, we solve the model assuming a single work crew is available for this system. Different scenarios account for the resource available for interdictor (BI). Finally, the time horizon (T) is chosen in such a way that the network returns to its normal operation. 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 @ 3.40GHz 3.41GHz desktop computer.

6.3.1 Computational Results

Figure 6.4 depicts cascading effects in IEEE 9-bus system following an initial attack in bus 8. The outage of bus 8 interrupts the balance of network and redistributes the flow since transmission lines connecting buses 7 and 9 to bus 8 are no longer available. As a result, bus 5 is overloaded and consequently fails. At the initial period, demand nodes 1 and 2 are deactivated since they cannot be fully satisfied. However, available flow through the network satisfies load 2. In period 2, generators 1, 2, and 3 are switched off as they are not able to operate at their full capacity resulting in unmet demand in loads 1, 2, and 3. This stage represents the steady state of failure in which the restoration process commences for buses 5 and 8. As soon as nodes 5 and 8 are fully recovered, all generators and loads operate at rated power, defined as steady state of recovery process.

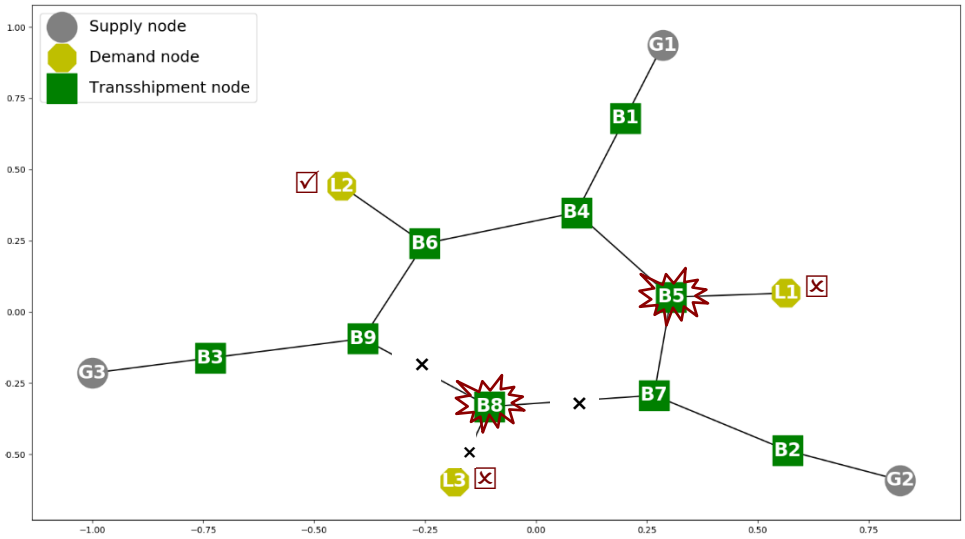


Figure 6.4. Cascading effect in IEEE 9-bus system following an initial damage.

As mentioned in Chapter 3 and in reference to Figure 1.1, network performance at time t is represented with $\varphi(t) = 1 - \zeta(t)$. Note that $\zeta(t)$ stands for the weighted fraction of unmet demand at time t as shown in Equation (6.1). Figure 6.5 illustrates the network performance trajectory, $\varphi(t)$, following an initial outage in bus 8. In the initial step, there is a drop in the performance of network since loads 1 and 2 cannot be fully satisfied. For an unprotected system represented by the blue line, form period 2 up until 6, network performance is zero since no demand node is satisfied because of disruptions to buses 5 and 8. Once the restoration process of damaged nodes is accomplished, demand nodes are fully satisfied since generators can operate at their maximum capacity. However, if bus 5 is protected, it will be invulnerable to disruption, so the system returns to the steady sate of recovery at time 4, shown by the orange line.

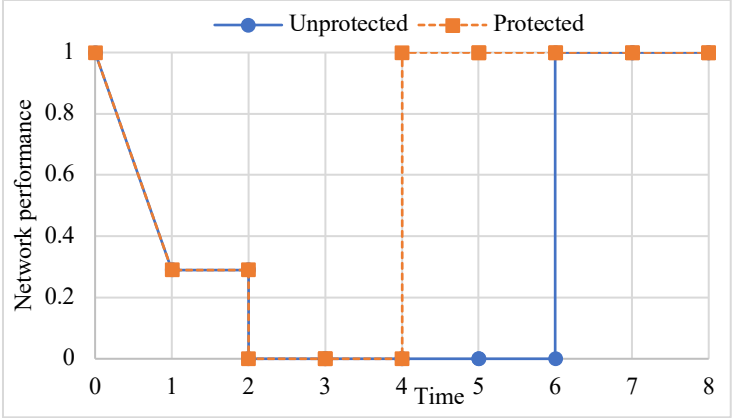


Figure 6.5. Network performance, $\varphi(t)$, following an initial attack in bus 8 for protected system vs unprotected system.

Figure 6.6 shows cumulative fraction of unmet demand over a time period $[0, 8]$, ξ, due to the primary attack to each bus. Buses 5, 6, and 8 are critical in this network since primary outage to each of which causes further disruption defined as cascading failure. Therefore, protecting such nodes enable the network to control total loss inflicted to system.

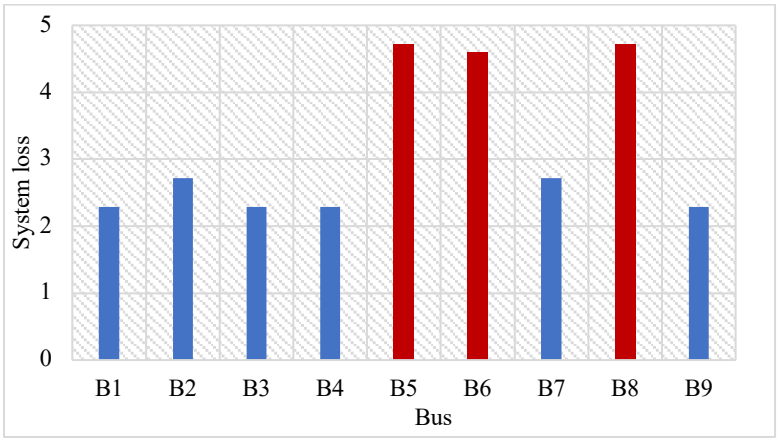


Figure 6.6. Cumulative fraction of unmet demand over time (ξ) following an initial attack to each bus.

Figure 6.7 depicts network performance, $\varphi(t)$, following an initial attack to each bus. As we discussed, initial attack to buses 5, 6, and 8 causes further damage such that recovery process takes longer in addition to initial damage imposed to system.

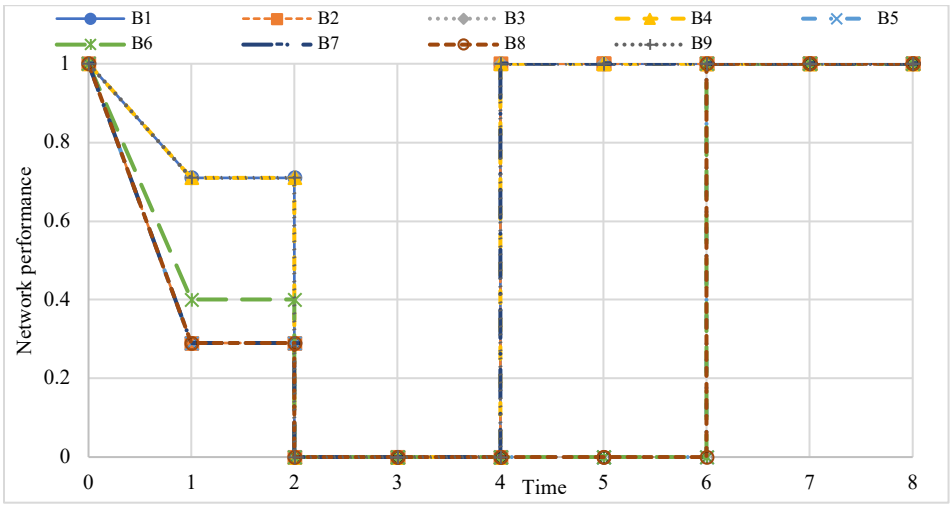


Figure 6.7. Network performance, $\varphi(t)$, following an initial attack to each bus.

Table 6.4 illustrates the optimal interdiction strategies under an interdictor budget of 1 to 6. In addition, this table provides cumulative fraction of unmet demand over time (ξ) for the optimal solution corresponding to each budget scenario. The value of ξ deteriorates as the amount of budget available for the attacker increases. As we discussed in previous chapters, computational time of set-covering solution approach continues to grow as the budget availability increases. For example, computational duration is around 1 minute for $BI = 1$ however this value increases to around 13 minutes for the last budget scenario, $BI = 6$.

Table 6.4. Attacker decision under different budget scenarios.

Attacker budget (BI)	1	2	3	4	5	6
Attacker plan	{B5}	{B5, B6}	{B3, B8, B9}	{B4, B5, B6, B9}	{B1, B3, B4, B6, B8}	{B1, B3, B4, B6, B8, B9}
Network loss (ξ)	4.71	7	9	11	13	15

To validate the proposed model for cascading failures and illustrate the benefits of such a formulation in practical setting, we applied it to IEEE 9-bus system and analyzed the attacker decisions under different budget scenarios. Although this case study is relatively small, the model can be easily applied to different examples with various network sizes. In addition, we targeted power network for the illustrative purposes, however, this interdiction model can be employed to any network-based systems such as transportation network, water supply, and computer network.

6.4 Concluding Remarks

In this Chapter, we focused on improving the resilience of a single structured network (e.g., optimizing the network protection plans) against cascading failures caused by an intentional attack building on an existing resilience interdiction model. In a network-based system, once an element is intentionally interdicted, the network flow is redistributed, which may cause overloading and subsequent disruptions in neighboring components. To assess and deal with such an effect, we incorporated the cascading effect into the third level of the proposed tri-level protection-interdiction-restoration model. Such that, the proposed formulation is a novel DAD model determining (i) which component needs to be protected prior to the disruptive event, (ii) which component is

critical in terms of its failure by itself along with causing other parts failures defined as cascading failures, and (iii) what restoration crew schedule is efficient following a disruptive event.

To illustrate the efficient solvability of the model and validate it for cascading failure, we focused on interdiction and restoration levels of this formulation. To optimally solve the bi-level interdiction-restoration model, we applied set-covering decomposition approach delivering the best attacker decision. We provided an illustrative example based on the single structured network of IEEE 9-bus power system consisting of 9 buses, 3 generators, and 3 loads. The results indicated how an initial damage could propagate throughout the system resulting in further disruption. To control such an effect, we plan to optimize protection strategies of a critical infrastructure network by solving the entire DAD model as the next step of this research applying a decomposition-based solution technique discussed in Chapter 4. In addition, we plan to solve the model for various case studies with different network sizes and analyze the results. Another future consideration will explore the system of interdependent networks for cascading failures which enhances the applicability of the proposed model in a practical setting.

Chapter 7: CONCLUDING REMARKS

7.1 Summary and Conclusions

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). Resilience is often thought of as the ability to withstand a disruption and recover quickly from it. Thus, improving the resilience of an infrastructure system is often associated with reducing its vulnerability (related to the extent to which a network is disrupted), and increasing its recoverability (related to the speed of restoration).

In this dissertation, we address these concerns simultaneously by proposing a tri-level protection-interdiction-restoration problem for a system of interdependent networks, to balance vulnerability and recoverability before and after a disruption. In particular, the proposed tri-level model represents decisions made (i) by a defender before a disruption to make decisions to minimize network vulnerability, (ii) by an attacker to identify and pursue the most effective disruptions, and (iii) by a subsequent defender after the disruption to enhance recoverability. The contribution of this model is to consider simultaneously (i) a set of interdependent infrastructure networks, (ii) an optimal defense plan against a set of most destructive attack strategies, (iii) a set of most critical elements through the system, and (iv) allocating and scheduling work crews to recover disrupted elements in the restoration level to return the system to its standard operation.

However, the proposed DAD model is computationally challenging to solve. To address this issue, 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 the interdiction model proposed in the first part of this dissertation, namely tri-level protection-interdiction-restoration.

Interdiction models generally involve a nonconvex inner level which make them challenging to solve even in their simplest form. Despite guaranteeing optimality, existing exact solution techniques considerably suffer from a large computational complexity that renders them ineffective even in a moderate-size system. Therefore, efficient solution algorithms are still required to address such complex problems in a reasonable time while maintaining a good quality in the proposed solutions. This motivates the need for hybrid solution techniques to cope with the computational burden of tri-level DAD models which are applicable in a wide range of interdiction models. The proposed solution approaches are decomposition-based, so tri-level models are broken down into two bi-level formulations including master problem and subproblem. Two methods are combined to deal with the two smaller bi-level problems (master problem and subproblem) iteratively, and subsequently the hybrid solution algorithm is constructed to find the solution for the whole tri-level model. The first solution approach is the HBD algorithm, which combines Benders decomposition method with a metaheuristic approach. The main advantage of this solution technique is its applicability to the broad variety of interdiction models with integer or continuous decision variables. The second approach is an integration of a set covering method and a metaheuristic algorithm, referred to here as the HSC algorithm.

Furthermore, in a network-based system, the outage of an element generally interrupts the balance of the network and redistribute the flow resulting in overload in adjacent components. This incident may cause additional damage which can propagate throughout the network rapidly defined as cascading failures. Such a phenomenon to critical infrastructures can be originated by just a few initiating events such as overloading a line in a power system, closing a road in a transportation system, hindering a pipe in a fluid distribution network, or cutting off a router in an information system. As such, we address optimization of protection strategies of a critical infrastructure network to tackle such an effect. This work aims to enhance network resilience against cascading failures initiated by intentional attack with a model that accounts for both pre- and post-disruption planning. The proposed model is a novel DAD model determining (i) which component needs to be protected prior to the disruptive event, (ii) which component is critical in terms of its failure by itself along with causing other parts failures defined as cascading failures, and (iii) what restoration crew schedule is efficient following a disruptive event.

7.2 Future Directions

With respect to the study presented in Chapter 5, we explored a genetic algorithm to solve the subproblem for illustrative purposes. However, other metaheuristic approaches can be efficiently incorporated in both HBD and HSC solution frameworks to deal with the bi-level subproblem. Despite a broad applicability of interdiction models in real world problems and grand challenges, computational complexity is the bottleneck in optimizing such models which make them difficult to employ in moderate- to large-sized

cases. Therefore, the development of efficient inexact solution methods is still under investigation and has captured considerable attention for making further improvement to cope with the computational burden of the interdiction models. As an example of additional improvement in HBD algorithm, the master problem is updated at each iteration of the algorithm by receiving the new set of attacker decisions generated by the subproblem, which leads to exponential growth of the master problem by increasing the iteration index. Further, the complexity of the master problem is intensified for large-sized problems. However, the metaheuristic algorithm may not offer the best attack strategy at each iteration which makes the generated constraints (cuts) redundant for the master problem. This redundancy raises the complexity of the problem unnecessarily without tightening the feasible region. For future work, it would be worth to modify the algorithm to deal with the set of redundant constraints (cuts) added to the master problem which could enhance the efficiency of the solution approach. This modification could also be applied to the master problem of the HSC algorithm for additional improvement in computation time. From the modeling point of view, the value of defender secrecy and deception is useful to explore as considering a fully informative interdictor about the system may not be reasonable in some circumstances. In addition, as infrastructure networks have different features that are represented by different physics properties (e.g., Kirchhoff's laws for the power network, Pascal’s principle for the water supply), it would be beneficial to develop a formulation reflecting the general principles of each infrastructure network. We are also interested in extending the formulation by incorporating uncertainty through the model parameters (e.g., available budget, required

time for recovering the components). This development could considerably enhance the applicability of the DAD models.

Furthermore, in a practical setting, a disruption in one network component may trigger other components resulting in cascading failure throughout the network, and including these cascading characteristics were presented in Chapter 6. However, to verify the model for cascading failures, we focused on interdiction and restoration levels of this formulation. As the next step of this research, we plan to optimize protection strategies of a critical infrastructure network by solving the entire DAD model. To optimally solve the model, we apply a decomposition-based solution technique discussed in Chapter 4. In addition, to demonstrate the efficient solvability of the proposed model, we intend to solve the model for various case studies with different network sizes. Another future consideration will explore the system of interdependent networks for cascading failures which increase the applicability of the model in real-world problems.

REFERENCES

Abraham, S., Dhaliwal, H., Efford, R. J., Keen, L. J., McLellan, A., Manley, J., … Al, E. (2004). *Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations*. *U.S.-Canada Power System Outage Task Force* (Vol. 40). Retrieved from https://reports.energy.gov/BlackoutFinal-Web.pdf

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. https://doi.org/10.1016/j.cie.2017.10.003

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. https://doi.org/https://doi.org/10.1016/j.cor.2011.08.006

Aksu, T. D., & Ozdamar, L. (2014). A mathematical model for post-disaster road restoration: Enabling accessibility and evacuation. *Transportation Research Part E: Logistics and Transportation Review*, *61*, 56–67. https://doi.org/10.1016/j.tre.2013.10.009

Albert, R., & Barabási, A.-L. (2002). Statistical mechanics of complex networks. *Rev. Mod. Phys.*, *74*(1), 47–97. https://doi.org/10.1103/RevModPhys.74.47

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2014). Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems. In *Bridging Data and Decisions* (pp. 180–215). https://doi.org/10.1287/educ.2014.0131

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational Models of Infrastructure Resilience. *Risk Analysis*, *35*(4), 562–586. https://doi.org/10.1111/risa.12333

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. https://doi.org/10.1287/ics.2011.0047

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. https://doi.org/10.1016/j.cor.2013.06.009

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. https://doi.org/10.1016/j.ress.2018.12.006

Almoghathawi, Y., Barker, K., Rocco, C. M., & Nicholson, C. D. (2017). A multi-criteria decision analysis approach for importance identification and ranking of network components. *Reliability Engineering and System Safety*, *158*(September 2016), 142–151. https://doi.org/10.1016/j.ress.2016.10.007

American Water Works Association. (2011). *Planning for an Emergency Drinking Water Supplye*. Washington, DC.

Arroyo, J. M., & Fernandez, F. J. (2009). A Genetic Algorithm Approach for the Analysis of Electric Grid Interdiction with Line Switching. In *2009 15th International Conference on Intelligent System Applications to Power Systems* (pp. 1–6). https://doi.org/10.1109/ISAP.2009.5352849

Aven, T. (2011). On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Analysis*, *31*(4), 515–522. https://doi.org/10.1111/j.1539-6924.2010.01528.x

Ayyub, B. M. (2014). Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. *Risk Analysis*, *34*(2), 340–355. https://doi.org/10.1111/risa.12093

Bard, J. F. (1991). Some properties of the bilevel programming problem. *Journal of Optimization Theory and Applications*, *68*(2), 371–378. https://doi.org/10.1007/BF00941574

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability Engineering & System Safety*, *117*, 89–97. https://doi.org/https://doi.org/10.1016/j.ress.2013.03.012

Baycik, N. O., Sharkey, T. C., & Rainwater, C. E. (2018). Interdicting layered physical and information flow networks. *IISE Transactions*, *50*(4), 316–331. https://doi.org/10.1080/24725854.2017.1401754

Bialek, J., Ciapessoni, E., Cirio, D., Cotilla-Sanchez, E., Dent, C., Dobson, I., … Wu, D. (2016). Benchmarking and Validation of Cascading Failure Analysis Tools. *IEEE Transactions on Power Systems*, *31*(6), 4887–4900. https://doi.org/10.1109/TPWRS.2016.2518660

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. https://doi.org/10.1016/j.ress.2006.08.007

Boccaletti, S., Bianconi, G., Criado, R., del Genio, C. I., Gómez-Gardeñes, J., Romance, M., … Zanin, M. (2014). The structure and dynamics of multilayer networks. *Physics Reports*, *544*(1), 1–122. https://doi.org/https://doi.org/10.1016/j.physrep.2014.07.001

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical

infrastructure. *Interfaces*, *36*(6), 530–544. https://doi.org/10.1287/inte.1060.0252

Brown, G., Carlyle, M., Salmerón, J., Wood, K., Brown, G., Carlyle, M., … Wood, K. (2006). Defending Critical Infrastructure, (March 2019). https://doi.org/10.1287/inte.1060.0252

Brown, G. G., Carlyle, W. M., Harney, R. C., Skroch, E. M., Wood, R. K., Brown, G. G., … Wood, R. K. (2009). Interdicting a Nuclear-Weapons Project Interdicting a Nuclear-Weapons Project, (March 2019). https://doi.org/10.1287/opre.1080.0643

Calvete, H. I., Galé, C., & Mateo, P. M. (2008). A genetic algorithm for solving linear fractional bilevel problems. *Annals of Operations Research*, *166*(1), 39. https://doi.org/10.1007/s10479-008-0416-0

Cappanera, P., & Scaparra, M. P. (2011). Optimal Allocation of Protective Resources in Shortest-Path Networks. *Transportation Science*, *45*(1), 64–80. https://doi.org/10.1287/trsc.1100.0340

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. https://doi.org/10.1007/s11069-006-9039-4

Chassin, D. P., & Posse, C. (2005). Evaluating North American electric grid reliability using the Barabási–Albert network model. *Physica A: Statistical Mechanics and Its Applications*, *355*(2), 667–677. https://doi.org/https://doi.org/10.1016/j.physa.2005.02.051

Chen, C.-L., Zheng, Q., Veremyev, A., Pasiliao, E. L., & Boginski, V. (2020). Failure Mitigation and Restoration in Interdependent Networks via Mixed-integer Optimization. *IEEE Transactions on Network Science and Engineering*, *4697*(c), 1–1. https://doi.org/10.1109/tnse.2020.3005193

Dong, H., & Cui, L. (2016). System Reliability Under Cascading Failure Models. *IEEE Transactions on Reliability*, *65*(2), 929–940. https://doi.org/10.1109/TR.2015.2503751

Dong, S., Yu, T., Farahmand, H., & Mostafavi, A. (2020). Probabilistic modeling of cascading failure risk in interdependent channel and road networks in urban flooding. *Sustainable Cities and Society*, *62*(January), 102398. https://doi.org/10.1016/j.scs.2020.102398

Dueñas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural Safety*, *31*(2), 157–167. https://doi.org/https://doi.org/10.1016/j.strusafe.2008.06.007

Fang, Y.-P., Pedroni, N., & Zio, E. (2016). Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. *IEEE Transactions on*

Reliability, *65*(2), 502–512. https://doi.org/10.1109/TR.2016.2521761

Fathollahi Fard, A. M., & 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. https://doi.org/10.1016/j.asoc.2018.04.011

Fisher, E. B., O'Neill, R. P., & Ferris, M. C. (2008). Optimal Transmission Switching. *IEEE Transactions on Power Systems*, *23*(3), 1346–1355. https://doi.org/10.1109/TPWRS.2008.922256

Gao, Y., Zhang, G., Lu, J., & Wee, H.-M. (2011). Particle swarm optimization for bi-level pricing problems in supply chains. *Journal of Global Optimization*, *51*(2), 245–254. https://doi.org/10.1007/s10898-010-9595-8

Gedik, R., Medal, H., Rainwater, C., Pohl, E. A., & Mason, S. J. (2014). Vulnerability assessment and re-routing of freight trains under disruptions: A coal supply chain network application. *Transportation Research Part E: Logistics and Transportation Review*, *71*, 45–57. https://doi.org/10.1016/j.tre.2014.06.017

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. https://doi.org/10.1002/nav.3800180103

Goh, K.-I., Kahng, B., & Kim, D. (2001). Universal Behavior of Load Distribution in Scale-Free Networks. *Phys. Rev. Lett.*, *87*(27), 278701. https://doi.org/10.1103/PhysRevLett.87.278701

Golbeck, J. (2013). Chapter 3 - Network Structure and Measures. In J. Golbeck (Ed.), *Analyzing the Social Web* (pp. 25–44). Boston: Morgan Kaufmann. https://doi.org/https://doi.org/10.1016/B978-0-12-405531-5.00003-1

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. https://doi.org/10.1111/risa.13340

González, A. D., Dueñas-Osorio, L., Sánchez-Silva, M., & Medaglia, A. L. (2015). The Computational Complexity of Probabilistic Interdependent Network Design Problems. In *Proceedings of the 12th International Conference on Applications of Statistics and Probability in Civil Engineering (ICASP12)* (pp. 1–8). Vancouver, Canada. https://doi.org/10.14288/1.0076118

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. https://doi.org/10.1111/mice.12171

Grogan, L., & Tserenkhuu, T. (2018). Water access may be more important than

electricity for sub-Saharan Africa. *The Conversation*.

Guo, H., Zheng, C., Iu, H. H. C., & Fernando, T. (2017). A critical review of cascading failure analysis and modeling of power system. *Renewable and Sustainable Energy Reviews*, *80*(March), 9–22. https://doi.org/10.1016/j.rser.2017.05.206

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis*, *29*(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

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. https://doi.org/10.1137/0913069

Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering*, *8*(4), 355–366.

Hecheng, L., & Yuping, W. (2008). Exponential distribution-based genetic algorithm for solving mixed-integer bilevel programming problems. *Journal of Systems Engineering and Electronics*, *19*(6), 1157–1164. https://doi.org/https://doi.org/10.1016/S1004-4132(08)60213-3

Henneaux, P., Ciapessoni, E., Cirio, D., Cotilla-Sanchez, E., Diao, R., Dobson, I., … Yao, R. (2018). Benchmarking quasi-steady state cascading outage analysis methodologies. *2018 International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2018 - Proceedings*, 1–6. https://doi.org/10.1109/PMAPS.2018.8440212

Hernandez-Fajardo, I., & Dueñas-Osorio, L. (2011). Sequential Propagation of Seismic Fragility across Interdependent Lifeline Systems. *Earthquake Spectra*, *27*(1), 23–43. https://doi.org/10.1193/1.3544052

Hernández-Perdomo, E., Rocco, C. M., & Ramirez-Marquez, J. E. (2016). Node ranking for network topology-based cascade models – An Ordered Weighted Averaging operators' approach. *Reliability Engineering and System Safety*, *155*, 115–123. https://doi.org/10.1016/j.ress.2016.06.014

Holland, J. H. (1992). *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*. MIT Press. Retrieved from https://books.google.com/books?id=5EgGaBkwvWcC

Holmgren, Å. J. (2006). Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis*, *26*(4), 955–969. https://doi.org/10.1111/j.1539-6924.2006.00791.x

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. https://doi.org/10.1016/j.ress.2015.08.006

Huang, A., Zhang, H. M., Guan, W., Yang, Y., & Zong, G. (2015). Cascading Failures in Weighted Complex Networks of Transit Systems Based on Coupled Map Lattices. *Mathematical Problems in Engineering*, *2015*, 1–16. https://doi.org/10.1155/2015/940795

Israeli, E. (1999). *System Interdiction and Defense*. Monterey, CA.

Israeli, E., & Wood, R. K. (2002). Shortest-Path Network Interdiction. *Networks*, *40*(2), 97–111. https://doi.org/10.1002/net.10039

Kamamura, S., Shimazaki, D., Genda, K., Sasayama, K., & Uematsu, Y. (2015). Disaster Recovery for Transport Network through Multiple Restoration Stages. *IEICE Transactions on Communications*, *E98.B*(1), 171–179. https://doi.org/10.1587/transcom.E98.B.171

Kamdar, R., Kumar, M., & Agnihotri, G. (2014). Transient Stability Analysis and Enhancement of IEEE- 9 Bus System. *Electrical & Computer Engineering: An International Journal*, *3*(2), 41–51. https://doi.org/10.14810/ecij.2014.3204

Karakoc, D. B., Almoghathawi, Y., Barker, K., González, A. D., & Mohebbi, S. (2019). Community resilience-driven restoration model for interdependent infrastructure networks. *International Journal of Disaster Risk Reduction*, *38*, 101228. https://doi.org/https://doi.org/10.1016/j.ijdrr.2019.101228

Kaur, R., & Kumar, D. (2016). Transient Stability Improvement of IEEE 9 Bus System Using Power World Simulator. *MATEC Web of Conferences*, *57*, 01026. https://doi.org/10.1051/matecconf/20165701026

Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. *Proceedings of 1995 IEEE International Conference on Neural Networks*, *4*, 1942–1948.

Kettl, D. F. (2013). *System Under Stress: Homeland Security and American Politics*. CQ Press. Retrieved from https://books.google.com/books?id=LDOiWmjyaVkC

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Cascading effects of common-cause failures in critical infrastructures. *IFIP Advances in Information and Communication Technology*, *417*, 171–182. https://doi.org/10.1007/978-3-642-45330-4_12

Larocca, S., Johansson, J., Hassel, H., & Guikema, S. (2015). Topological Performance Measures as Surrogates for Physical Flow Models for Risk and Vulnerability Analysis for Electric Power Systems. *Risk Analysis*, *35*(4), 608–623. https://doi.org/10.1111/risa.12281

Lee II, E. E., Mitchell, J. E., & Wallace, W. A. (2007). Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach. *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*,

37(6), 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859

Li, M., Luh, P. B., Michel, L. D., Zhao, Q., & Luo, X. (2012). Corrective Line Switching With Security Constraints for the Base and Contingency Cases. *IEEE Transactions on Power Systems*, *27*(1), 125–133. https://doi.org/10.1109/TPWRS.2011.2164098

Li, Y. F., Sansavini, G., & Zio, E. (2013). Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. *Reliability Engineering and System Safety*, *111*, 195–205. https://doi.org/10.1016/j.ress.2012.11.002

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. https://doi.org/10.1016/j.cor.2010.06.002

Loji, K., Davidson, I. E., & Tiako, R. (2019). Voltage Profile and Power Losses Analysis on a Modified IEEE 9-Bus System with PV Penetration at the Distribution Ends. In *2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA)* (pp. 703–708). https://doi.org/10.1109/RoboMech.2019.8704802

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. https://doi.org/10.1016/j.ejor.2011.09.044

Ma, C. Y. T., Yau, D. K. Y., Lou, X., & Rao, N. S. V. (2013). Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Transactions on Power Systems*, *28*(2), 1676–1686. https://doi.org/10.1109/TPWRS.2012.2226480

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. https://doi.org/https://doi.org/10.1016/j.cie.2016.11.004

Marinakis, Y., & Marinaki, M. (2013). A Bilevel Particle Swarm Optimization Algorithm for Supply Chain Management Problems. In E.-G. Talbi (Ed.), *Metaheuristics for Bi-level Optimization* (pp. 69–93). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37838-6_3

Martin, P. A. S. (2007). *Tri-Level Optimization Models to Defend Critical Infrastructure*. NAVAL POSTGRADUATE SCHOOL.

Matisziw, T. C., Murray, A. T., & Grubesic, T. H. (2010). Strategic Network Restoration. *Networks and Spatial Economics*, *10*(3), 345–361. https://doi.org/10.1007/s11067-009-9123-x

McLay, L. A., Lloyd, J. D., & Niman, E. (2011). Interdicting nuclear material on cargo containers using knapsack problem models. *Annals of Operations Research*, *187*(1), 185–205. https://doi.org/10.1007/s10479-009-0667-4

McMasters, A. W., & Mustin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly*, *17*(3), 261–268. https://doi.org/10.1002/nav.3800170302

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

Michaud, D., & Apostolakis, G. E. (2006). Methodology for Ranking the Elements of Water-Supply Networks, *12*(December), 230–242. https://doi.org/10.1061/(ASCE)1076-0342(2006)12

Morshedlou, N., González, A. D., & Barker, K. (2018). Work crew routing problem for infrastructure network restoration. *Transportation Research Part B: Methodological*, *118*, 66–89. https://doi.org/10.1016/j.trb.2018.10.001

Morton, D. P., Pan, F., & Saeger, K. J. (2007). Models for nuclear smuggling interdiction. *IIE Transactions*, *39*(1), 3–14. https://doi.org/10.1080/07408170500488956

Motter, A. E., & Lai, Y.-C. (2002). Cascade-based attacks on complex networks. *Phys. Rev. E*, *66*(6), 65102. https://doi.org/10.1103/PhysRevE.66.065102

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. https://doi.org/10.1109/TPWRS.2005.851942

Murray, A. T., Matisziw, T. C., & Grubesic, T. H. (2007). Critical network infrastructure analysis: interdiction and system flow. *Journal of Geographical Systems*, *9*(2), 103–117. https://doi.org/10.1007/s10109-006-0039-4

Murtagh, F. (1983). A Survey of Recent Advances in Hierarchical Clustering Algorithms. *The Computer Journal*, *26*(4), 354–359. https://doi.org/10.1093/comjnl/26.4.354

Murtagh, F., & Contreras, P. (2011). Methods of Hierarchical Clustering. *Computing Research Repository - CORR*. https://doi.org/10.1007/978-3-642-04898-2_288

Nabli, A., Carvalho, M., & Hosteins, P. (2020). Complexity of the Multilevel Critical Node Problem.

Nagurney, A., & Qiang, Q. (2009). *Fragile Networks: Identifying Vulnerabilities and Synergies in an Uncertain World*. Wiley. Retrieved from https://books.google.com/books?id=O9VFIV6CQzUC

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. https://doi.org/https://doi.org/10.1016/j.cor.2016.05.005

Needham, M., & Hodler, A. E. (2019). *Graph Algorithms: Practical Examples in Apache Spark and Neo4j*. O'Reilly Media. Retrieved from https://books.google.com/books?id=z4WZDwAAQBAJ

Newman, M. (2018). *Networks*. OUP Oxford. Retrieved from https://books.google.com/books?id=YdZjDwAAQBAJ

Newman, M., Barabási, A. L., & Watts, D. J. (2011). *The Structure and Dynamics of Networks*. Princeton University Press. Retrieved from https://books.google.com/books?id=xLfQCwAAQBAJ

Nicholson, C. D., Barker, K., & Ramirez-Marquez, J. E. (2016). Flow-based vulnerability measures for network component importance: Experimentation with preparedness planning. *Reliability Engineering and System Safety*, *145*, 62–73. https://doi.org/10.1016/j.ress.2015.08.014

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. https://doi.org/10.1016/j.ejor.2012.07.010

Ouyang, M. (2013). Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. *Chaos*, *23*(2). https://doi.org/10.1063/1.4807478

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

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. https://doi.org/10.1016/j.ejor.2017.04.022

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. https://doi.org/10.1111/mice.12252

Ozcelik, M. (2017). Alternative model for electricity and water supply after disaster. *Journal of Taibah University for Science*, *11*(6), 966–974. https://doi.org/https://doi.org/10.1016/j.jtusci.2017.01.002

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.

https://doi.org/10.1007/0-306-48109-X_1

Papic, M., Bell, K., Chen, Y., Dobson, I., Fonte, L., Haq, E., … Zhang, P. (2011). Survey of tools for risk assessment of cascading outages. In *2011 IEEE Power and Energy Society General Meeting* (pp. 1–9). https://doi.org/10.1109/PES.2011.6039371

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. https://doi.org/https://doi.org/10.1016/j.asoc.2017.08.018

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. https://doi.org/https://doi.org/10.1016/j.ress.2006.08.004

Rahdar, M. (2016). *Three essays on multi-level optimization models and applications*. Iowa State University.

Ramirez-Marquez, J. E., Rocco, C. M., & Levitin, G. (2011). Optimal network protection against diverse interdictor strategies. *Reliability Engineering & System Safety*, *96*(3), 374–382. https://doi.org/https://doi.org/10.1016/j.ress.2010.10.003

Ren, H.-P., Song, J., Yang, R., Baptista, M. S., & Grebogi, C. (2016). Cascade failure analysis of power grid using new load distribution law and node removal rule. *Physica A: Statistical Mechanics and Its Applications*, *442*, 239–251. https://doi.org/https://doi.org/10.1016/j.physa.2015.08.039

Rocco, C. M., Barker, K., Moronta, J., & Ramirez-Marquez, J. E. (2018). Multiobjective Formulation for Protection Allocation in Interdependent Infrastructure Networks Using an Attack-Diffusion Model. *Journal of Infrastructure Systems*, *24*(1), 04018002. https://doi.org/10.1061/(asce)is.1943-555x.0000415

Rocco, C. M., Ramirez-Marquez, J. E., Salazar, D. E., & Zio, E. (2010). A Flow Importance Measure with Application to an Italian Transmission Power System. *International Journal of Performability Engineering*, *6*(1), 53–61.

Rocco, C. M., Ramirez-Marquez, J. E., & Yajure, C. (2014). A Non-Parametric Aggregation Technique for Identifying Critical Nodes in a Network, Using Three Topology-Based Cascade Models. In *Vulnerability, Uncertainty, and Risk* (pp. 668–676). https://doi.org/10.1061/9780784413609.068

Rocco S., C. M., Emmanuel Ramirez-Marquez, J., & Salazar A., D. E. (2010). Bi and tri-objective optimization in the deterministic network interdiction problem. *Reliability Engineering & System Safety*, *95*(8), 887–896. https://doi.org/https://doi.org/10.1016/j.ress.2010.03.008

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

https://doi.org/https://doi.org/10.1016/j.cie.2010.04.004

Rocco S., C. M., Ramirez-Marquez, J. E., Salazar A., D. E., & Zio, E. (2010). A Flow Importance Measure with Application to an Italian Transmission Power System. *International Journal of Performability Engineering*, *6*(1), 53–61.

Rocco S, C. M., & Ramirez-Marquez, J. E. (2009). Deterministic network interdiction optimization via an evolutionary approach. *Reliability Engineering & System Safety*, *94*(2), 568–576. https://doi.org/https://doi.org/10.1016/j.ress.2008.06.008

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

Sadati, M. E. H., Aksen, D., & Aras, N. (2020). The r-interdiction selective multi-depot vehicle routing problem. *International Transactions in Operational Research*, *27*(2), 835–866. https://doi.org/10.1111/itor.12669

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. https://doi.org/10.1007/978-3-642-37838-6_8

Salmeron, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, *19*(2), 905–912. https://doi.org/10.1109/TPWRS.2004.825888

Salmeron, J., Wood, K., & Baldick, R. (2004). Analysis of Electric Grid Security Under Terrorist Threat, *19*(2), 905–912.

Sarhadi, H., Tulett, D. M., & Verma, M. (2015). A defender-attacker-defender approach to the optimal fortification of a rail intermodal terminal network. *Journal of Transportation Security*, *8*(1), 17–32. https://doi.org/10.1007/s12198-014-0152-4

Shao, W., & Vittal, V. (2005). Corrective switching algorithm for relieving overloads and voltage violations. *IEEE Transactions on Power Systems*, *20*(4), 1877–1885. https://doi.org/10.1109/TPWRS.2005.857931

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. https://doi.org/10.1016/j.ejor.2014.12.051

Sharma, P., & Patel, R. N. (2016). Mitigation and wavelet analysis for power swing in IEEE 9 bus system. In *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICACCS.2016.7586325

Sharma, S., Velgapudi, N. S., & Pandey, K. (2017). Performance analysis of IEEE 9 Bus system using TCSC. In *2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE)* (pp. 251–256). IEEE.

https://doi.org/10.1109/RDCAPE.2017.8358277

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. https://doi.org/10.1002/eqe.938

Taha, H. A. (1998). Operations Research: An Introduction. *Journal of Manufacturing Systems*, *17*(1), 78.

Talbi, E. G. (2013). *Metaheuristics for Bi-level Optimization*. Springer Berlin Heidelberg. Retrieved from https://books.google.com/books?id=c0a6BQAAQBAJ

The Google Apps Team. (2012). *Google Apps Incident Report*.

Vaiman, Bell, Chen, Chowdhury, Dobson, Hines, … Zhang. (2012). Risk Assessment of Cascading Outages: Methodologies and Challenges. *IEEE Transactions on Power Systems*, *27*(2), 631–641. https://doi.org/10.1109/TPWRS.2011.2177868

Vugrin, E. D., Turnquist, M. A., & Brown, N. J. K. (2014). Optimal recovery sequencing for enhanced resilience and service restoration in transportation networks. *International Journal of Critical Infrastructures*, *10*(3/4), 218. https://doi.org/10.1504/IJCIS.2014.066356

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.

Wang, G., Wang, X., Wan, Z., & Jia, S. (2007). An adaptive genetic algorithm for solving bilevel linear programming problem. *Applied Mathematics and Mechanics*, *28*(12), 1605–1612. https://doi.org/10.1007/s10483-007-1207-1

Wang, J., Jiang, C., & Qian, J. (2014). Robustness of Internet under targeted attack: A cascading failure perspective. *Journal of Network and Computer Applications*, *40*, 97–104. https://doi.org/https://doi.org/10.1016/j.jnca.2013.08.007

Wang, S., Hong, L., & Chen, X. (2012). Vulnerability analysis of interdependent infrastructure systems: A methodological framework. *Physica A: Statistical Mechanics and Its Applications*, *391*(11), 3323–3335. https://doi.org/10.1016/j.physa.2011.12.043

Wang, S., Hong, L., Ouyang, M., Zhang, J., & Chen, X. (2013). Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Safety Science*, *51*(1), 328–337. https://doi.org/10.1016/j.ssci.2012.07.003

Wollmer, R. (1964). Removing Arcs from a Network. *Operations Research*, *12*(6), 934–940. https://doi.org/10.1287/opre.12.6.934

Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling*, *17*(2), 1–18. https://doi.org/https://doi.org/10.1016/0895-7177(93)90236

Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., & Vaziri, K. (2007). Optimizing scheduling of post-earthquake electric power restoration tasks. *Earthquake Engineering & Structural Dynamics*, *36*(2), 265–284. https://doi.org/10.1002/eqe.623

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. https://doi.org/10.1109/TSMCC.2007.897487

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. https://doi.org/10.1016/j.ress.2013.08.003

Zadorozhnyi, V., & Yudin, E. (2014). Growing Network: Nonlinear Extension of the Barabasi-Albert Model. In A. Dudin, A. Nazarov, R. Yakupov, & A. Gortsev (Eds.), *Information Technologies and Mathematical Modelling* (pp. 432–439). Cham: Springer International Publishing.

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. https://doi.org/10.1016/j.orl.2013.05.003

Zhang, Y., Yang, N., & Lall, U. (2016). Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. *Journal of Systems Science and Systems Engineering*, *25*(1), 102–118. https://doi.org/10.1007/s11518-016-5295-3

Zhou, J., Coit, D. W., Felder, F. A., & Wang, D. (2021). Resiliency-based restoration optimization for dependent network systems against cascading failures. *Reliability Engineering and System Safety*, *207*(October 2020), 107383. https://doi.org/10.1016/j.ress.2020.107383

Zhu, Y., Zheng, Z., Zhang, X., & Cai, K. (2013). The r-interdiction median problem with probabilistic protection and its solution algorithm. *Computers & Operations Research*, *40*(1), 451–462. https://doi.org/https://doi.org/10.1016/j.cor.2012.07.017

Zio, E., Golea, L. R., & Sansavini, G. (2012). Optimizing protections against cascades in network systems: A modified binary differential evolution algorithm. *Reliability Engineering and System Safety*, *103*, 72–83. https://doi.org/10.1016/j.ress.2012.03.007

Zio, E., & Sansavini, G. (2011). Component criticality in failure cascade processes of network systems. *Risk Analysis*, *31*(8), 1196–1210. https://doi.org/10.1111/j.1539-6924.2011.01584.x