UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

# RESILIENCE-BASED TRI-LEVEL OPTIMIZATION FOR MULTI-COMMODITY NETWORKS

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

EMMA KUTTLER

Norman, Oklahoma

2022

RESILIENCE-BASED TRI-LEVEL OPTIMIZATION FOR MULTI-COMMODITY NETWORKS

A THESIS APPROVED FOR THE

SCHOOL OF INDUSTRIAL AND SYSTEMS ENGINEERING

BY THE COMMITTEE CONSISTING OF

Dr. Kash Barker, Chair

Dr. Andrés González Huertas

Dr. Talayeh Razzaghi

## Acknowledgements

I would first like to thank my advisor Dr. Kash Barker. He has been one of my biggest advocates over the past five years, and I am incredibly grateful for all his time and support. He has always been there to provide guidance or reassurance and has given me extensive opportunities to publish and present my work. I can say with 100% confidence that ($p = 0$) that he cares about me and all his students, not only as academics but also as people. Again, I'm incredibly thankful for his support.

I would also like to thank Dr. Andrés González and Dr. Talayeh Razzaghi for being members of my thesis committee. Also, this thesis draws heavily from works by Dr. Nafiseh Ghorbani-Renani, to whom I am very thankful for her guidance, coding expertise, and suggestions. Furthermore, Dr. Jonas Johansson of Lund University has been a great colleague across the pond and has allowed me to use his data sets.

Finally, I would like to thank my family and friends for always being my support system. To my parents and brother, thank you for encouraging me to push myself to be my best, even when I thought I couldn't do it and loving me unconditionally. To my ISE squad and all my roommates (past and present), thanks for keeping me sane and always caring for me. Couldn't have done it without you.

## Table of Contents

## List of Figures

## List of Tables

## Abstract

Interdependent critical infrastructure systems represent substantial financial investments and are vital to maintain a basic level of social and economic well-being, making them attractive targets for malevolent actors. Many of these systems carry multiple products, each with unique needs and importance to different stakeholders. Tri-level optimization models have been proposed to capture the scale of a system's resilience, representing the optimal actions taken by a defender to harden the system, by an attacker to interdict the system, and then by the defender to assign work crews for restoration, all under a limited budget. However, most prior work focuses on networks with a single product. This work extends a tri-level protection-interdiction-restoration model from a single commodity to multiple commodities, solving the model with a Benders' decomposition and set covering decomposition. We propose a method to limit unmet weighted demand across commodities, taking into account unique interdependencies between network components and commodity-specific capacity requirements. An optimal solution is found iteratively by alternately fixing protection and interdiction variables. This work is illustrated with a case study of interdependent Swedish power and railway systems. Results demonstrate the convergent behavior of the master and subproblems, the value of network hardening, and the non-uniform network recovery trajectory. The proposed model is easily adapted to different commodity types, attack and defense budgets, crew availability, and commodity weights.

# Chapter 1: Introduction and Motivation

The resilience of critical infrastructure systems is vital to maintain a basic level of social and economic well-being in the event of partial damage or complete loss of function. Critical infrastructure systems (CIS), as defined by the United States of Homeland Security are systems, networks, or assets whose incapacitation or destruction “would have a debilitating effect on security, national economic security, national public health or safety,” – for example, the defense industrial base, transportation systems, the energy grid, and wastewater systems [1]. Any critical infrastructure system is a major financial investment and the loss of even a few components from random failures or deliberate attack can have catastrophic consequences [2]. Interdependencies between these systems may increase overall efficiency, but may also increase the likelihood of cascading failures or aggravate damage consequences [3]. Some systems may carry multiple products, each with unique values, needs, and importance [4], [5]. There is great value, then, in increasing the resilience of these systems through decreased vulnerability to attack or loss, as well as rapid recovery following a disruption. However, under budgetary, time, and political constraints, system managers and operators must make decisions regarding the allocation of resources between components in these key infrastructure systems, both of hardening resources to minimize disruption and of restoration resources.

Defining, measuring, and improving the resilience of critical infrastructure systems is an increasingly popular topic in the literature, and thus has many definitions, often overlapping with other network qualities such as “robustness, fault-tolerance, flexibility, survivability, and agility, among others” [6]. Ouyang provides guidance for developing a useful definition of system resilience, stating that a definition must specify resilience to a certain type of disruption, as well as noting that system resilience is mainly affected by system robustness, or the performance immediately after an attack or disruption [7]. Others, referring to transportation resilience, claim that resilience includes both proactive and reactive aspects; or planning for resilient systems and protecting against system disruption [8]. Dinh et al. adds non-engineering factors as elements of resilience, including administrative procedures and early detection abilities [9]. Vugrin et al. separates these factors into three segments: absorptive, adaptive, and restorative capacities [10]. Perhaps the most relevant definition is that provided by Haimes and others that defines resilience as the ability the system to withstand, adapt to, and recover in a timely manner from the effects of a disruption [11] [12] [13] [6]. Henry and Ramirez-Marquez represent this concept using a time-dependent function, as shown in Figure 1. For the purposes of this paper, resilience will be defined using Haimes' definition.

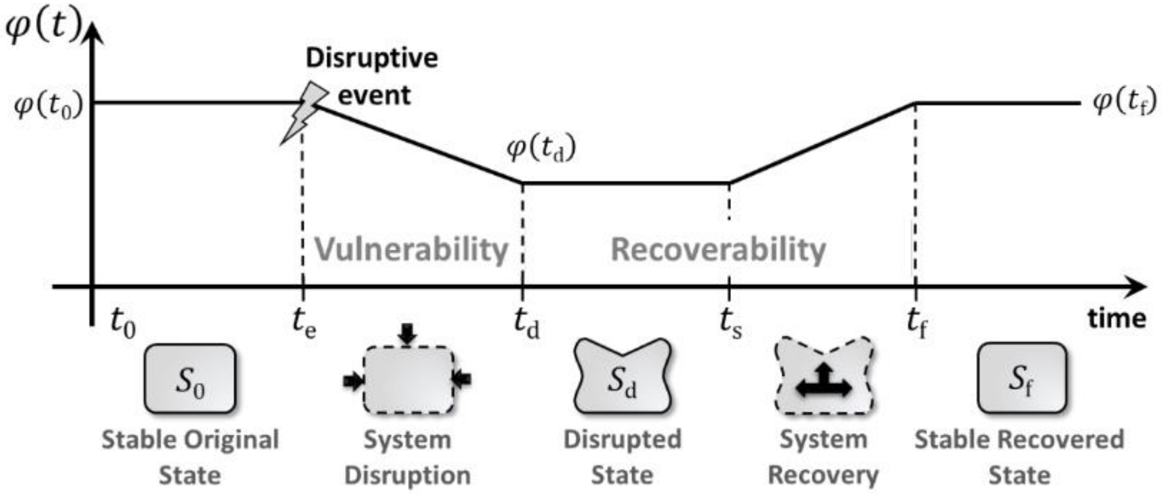

**Figure 1. System performance following a disruptive event. Adapted from [14]**

Tri-level optimization models are a powerful way to capture and enhance the full scope of a system's resilience. These models represent the set of optimal decisions made by (i) a defender to prepare a network for disruption, (ii) an attacker to maximize disruption, and (iii) by the defender to return to a specified level of pre-disruption function as rapidly as possible [15], [16]. These three phases are typically referred to as protection, interdiction, and restoration.

These models may also be referred to as defender-attacker-defender models and are a logical and realistic extension of bi-level defender-attacker models that do not consider recoverability. Each phase of the protection-interdiction-restoration typically has other accompanying analysis. The protection phase often involves consideration of node criticality, centrality, or topographic features [7], [17], [18]. The interdiction phase is heavily reliant on the attack type, such as whether it is committed by a malevolent actor or by a natural disaster [19]. Maximizing damage may be only one goal among several (i.e. terror, intimidation) [20]. Depending on the model type, the attacker may choose between several different attack scenarios, strategies, or intensities [13], [21], [22]. Restoration typically only considers a return to some level of system capability in  the short term, disregarding long term effects [23]. There are methods and algorithms to determine the set or order of components that must be restored as well as general models to determine component importance before a disruption [14], [24], [25]. Considerably fewer models include restoration and recoverability in their optimization [26]. Tri-level optimization is also computationally complex and may specific solution algorithms or metaheuristics to solve [20], [22], [27], [28]. Models for networks and systems with multiple products or commodities may be even more complex and are less represented in the literature [29].

To enhance network resilience, we propose a tri-level optimization method that includes protection, interdiction, and restoration decisions for a multi-commodity network. This becomes a multi-objective optimization problem with  a simple economic measure used to weight the various objectives (unmet demand of each commodity). The rest of this paper is organized as follows. In Chapter 2 we discuss tri-level optimization models and solution algorithms in the current literature, with a focus on multi-commodity optimization. In Chapter 3, the notation and details of the proposed model are presented as well as the computational solution method. In

Chapter 4, an illustrative example is provided to test the model and computational results are discussed. Concluding remarks and potential extensions are provided in Chapter 5.

# Chapter 2: Literature Review

Current research in the area of tri-level optimization includes work related to the allocation of protective resources, analysis of the attacker strategies, and techniques to maximize recoverability. Variations on a basic model exist for unique system interdependencies, multi-commodity systems, and computationally complex problems. There are many proposed protection-interdiction models developed for critical infrastructure systems. Murray, Matisziw, and Grubesic place interdiction problems into four categories, regardless of application: simulation, shortest path, network attributes, and system flow models [30]. Others categorize the models by goal: performance evaluation, design, mitigation, and recovery models [31].

Brown et al. propose both bi- and tri-level models in a homeland security context using mixed-integer linear programming, which is a special case of a static Stackelberg game [32]. Similarly, Israeli and Wood model bi-level attacker-defender interactions as a shortest-path problem also using mixed-integer programming [18], [33]. Bell et al. adapt Wood's defender-attacker-defender approach for a road blockage scenario using the increase in travel cost as an element of the objective function to harden particular routes [21]. Some models may choose how much to allocate for defense instead of making the binary decision to defend or not. Ramirez-Marquez, Rocco, and Levitin found that equal resource allocation is optimal for situations with homogenous component vulnerability [20]. In the attack phase, models may either aggregate attacks to find a robust defense strategy or find unique solutions for each attack strategy [13]. González and others modify the restoration phase by exploiting colocation efficiencies following a natural disaster [31]. Other models choose not to develop optimal protection, interdiction, and restoration decisions in favor of identifying the bounds for best and worst-case impacts on system flow [30].

Fewer models have been directly developed for multi-commodity networks. A particular challenge of multi-commodity models is the changing importance of components in a system between commodities, both in the protection and the restoration stages. Much of the research surrounding multi-commodity networks exists for disaster recovery scenarios, in which the multiple commodities only exist in the interdiction phase, rather than the protection and interdiction phases. Jin, Lu, Sun, and Yin developed a tri-level multi-commodity optimization model for an urban rail transit attack scenario in which commuter evacuation is modeled as a multi-commodity flow problem in the third level [22]. McCarter et al. uses the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to address trade-offs between various attack scenarios and cost in a rail transportation network [17]. Other authors simply treat all commodities as equal and maximize or minimize the total network flow [27]. Commodities may also be weighted using some sort of normalizing metric, like economic impact, cost or weighted unsatisfied demand [5], [22], [34]. Regardless of the method, multi-commodity networks are substantially more computationally complex and cannot be solved by the simplex method or the maximum flow minimum cut theorem [29].

Solution methods for tri-level optimization problems typically fall into two categories, evolutionary metaheuristic search algorithms and decomposition-based approaches. Ahmad et al. employs a genetic algorithm to generate optimal attacks for the interdictor [27]. Qiao et al. also uses a genetic algorithm in a water supply context for a bi-level protection-interdiction problem [28]. Ramirez-Marquez, Rocco, and Levitin note that a continuous probabilistic solution discovery algorithm may also explore regions of the solution space in an effective manner [20]. Variable neighborhood search metaheuristics have also been used [22]. For decomposition, the variation of Benders' decomposition algorithm proposed by Israeli and Wood has been used extensively for network interdiction [18], [33], [35]. This method iteratively solves smaller bi-level problems to avoid the challenge of dualizing a potentially nonlinear problem and to exploit the interaction between the attacker and the defender in the smaller problems [16]. The model is adaptable enough to solve for a variety of network types and is computationally efficient [26], [36]. Covering decomposition is also a popular strategy to produce exact solutions [16], [33], [37]

With the previous contributions in mind, we propose an extension of the well-known interdiction model to improve the resilience of a multi-commodity system under intelligent attack through improvements to pre-interdiction hardening and post-disruption restoration. The proposed model will use set covering decomposition with Benders' decomposition with a weighting measure to account for the importance of the unique commodities.

# Chapter 3: Multi-Commodity Protection-Interdiction-Restoration Model

This paper is concerned with enhancing the overall resilience of multi-commodity critical infrastructure systems under threat of intelligent directed attack. The problem is modeled as a defender-attack-defender series of nested optimization decisions. The problem has three distinct stages. In the first stage, the defender allocates protective resources to specific components to harden the system through the addition of greater capacity or greater redundancy. Essentially, the defender seeks to minimize disruption. In the second stage, the intelligent attacker attempts to maximize disruption to the network by reducing the capacity of selected components in an efficient manner. Both the attacker and the defender have specific, limited budgets and full knowledge of the protection and interdiction costs of the system. In the third and final stage, the defender seeks to minimize the time to restore the system through selection of the sequence of components to repair. There is a specific and constant number of work crews available to perform restoration activities. The problem formulation is then a min-max-min optimization problem. However, the supply, demand, and flow capacity for each node may vary by component, adding another layer of complexity to the decisions in each stage. A particular node may be critical for one commodity, and unimportant for another, which forces both the attacker and the defender to assess the value of that component across commodities.

This section introduces the proposed tri-level optimization model for improving resilience for multi-commodity systems. The formulation draws heavily from prior work by Ghorbani-Renani et al. [26]. First, the assumptions for the model will be presented, followed by the notation that will be used throughout the remainder of this text. Then the unique objective function, constraints, and solution method are presented in the following sections.

### 3.1. Modeling Assumptions

The proposed model operates under the following assumptions:

- Not all components are eligible for protection and interdiction. Only a subset of nodes and links are eligible for protection and interdiction.
- Each node has a known supply capacity, demand capacity, or flow capacity for each commodity. A node may be both a supply node and a demand node for different products.
- There is a known cost to protecting or interdicting each node. There are also known budgets for both the attacker and the defender to use for interdiction and protection, respectively. The protection cost does not vary by commodity.
- Each component can be fully protected so that it is completely resistant to interdiction. If a protected node is attacked there is no loss of flow.
- In the restoration stage, a work crew may only work on one component at a time. A component may not be only partially restored.
- Restoration requires at least one complete time unit to be completed.
- Each component has a specific restoration rate, $\lambda$, that is a function of the loss of capacity and specific component characteristics. This rate represents the proportion of restoration per unit of time by a single work crew and is not a function of the commodities on that component.
- Directed infrastructure networks are physically dependent so that "child" nodes rely on "parent" nodes to be fully operational.
- All commodities are continuous units.
- All the commodities on the network are known to both the attacker and the defender.

### 3.2. Notation

The network is an undirected graph *G = (N, A)* where *N* is the set of nodes, and *A* is the set of links. Commodities are represented by $g \in G$. There is a set *K* of interdependent networks, each containing a smaller set of nodes $N^k$ so that $\cup_{k \forall K} = \ N^k$. We use $N^k$ to represent the set of all nodes across commodities for a particular network. Similarly, there is a set of nodes $A^k$ so $\cup_{k \forall K} = \ A^k$. There are supply nodes ($N_{+g}^{k} \subseteq N_g^k$), demand nodes ($N_{-g}^{k} \subseteq N_g^k$), and transshipment nodes ($N_{=g}^{k} \subseteq N_g^k \backslash \{N_{+g}^{k}, N_{-g}^{k}\}$) for each commodity. And since we assume that not every node is eligible for protection and interdiction, we have smaller sets $A'$ and $N'$ that can be protected or interdicted for $k \in K$ where $N'^k \subseteq N^k$ and $A'^k \subseteq A^k$. This represents the realistic scenario in which some components may be physically inaccessible, prohibitively expensive to attack or defend, or relatively unimportant to both parties. There are also interdependencies between nodes across networks $k \in K$. We use Ψ to indicate interdependencies, where $\left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi$ means that node $i \in N^k$ in $k \in K$ depends on node $\bar{\imath} \in N^{\bar{k}}$ in network $\bar{k} \in K$. Additionally, $N^k \cap N^{\bar{k}} = \emptyset, A^k \cap A^{\bar{k}} = \emptyset$ and $\forall\ k, \bar{k} \in K: k \neq \bar{k}$. Another set $R^k$ represents the work crews available to each network $k \in K$. Time periods are represented by index $t \in T$. Table 1 provides the remaining model parameters and Table 2 contains the model decision variables.

**Table 1. Model parameters**

| | |
|---|---|
| ε | An arbitrarily small positive number in (0,1) |
| *M* | An arbitrarily large positive number greater than time needed for recovery |
| *BP* | Total budget available for protector |
| *BI* | Total budget available for interdictor |
| $\boldsymbol{CP_{ij}^{k}}$ | Cost of protecting link $(i,j) \in A'^k$ in network $k \in K$ |

| | |
|---|---|
| $\boldsymbol{CP_i^k}$ | Cost of protecting node $i \in N'^{k}$ in network $k \in K$ |
| $\boldsymbol{CI_i^k}$ | Cost of interdicting link $(i, j) \in A'^{k}$ in network $k \in K$ |
| $\boldsymbol{CI_i^k}$ | Cost of interdicting node $i \in N'^{k}$ in network $k \in K$ |
| $\boldsymbol{s_{ig}^k}$ | Amount of supply in node $i \in N_{+}^{k}$ in network $k \in K$ of commodity g $\in G$ |
| $\boldsymbol{d_{ig}^k}$ | Amount of demand in node $i \in N_{-}^{k}$ in network $k \in K$ for commodity $g \in G$ |
| $\boldsymbol{\lambda_i^k}$ | Restoration rate of node $i \in N'^{k}$ in network $k \in K$ |
| $\boldsymbol{\lambda_{ij}^k}$ | Restoration rate of link $(i, j) \in A'^{k}$ in network $k \in K$ |
| $\boldsymbol{u_{ijg}^k}$ | Capacity of link $(i, j) \in A^{k}$ in network $k \in K$ for commodity $g \in G$ |
| $\boldsymbol{w_{itg}^k}$ | Weight assigned to node $i \subseteq N_{-g}^{k}$ in network $k \in K$ at time $t \in T$ for commodity $g \in G$ |

**Table 2. Model decision variables**

| | |
|---|---|
| $\boldsymbol{m_{itg}^k}$ | Amount of demand met at node $\boldsymbol{i} \subseteq \boldsymbol{N_{-g}^{k}}$ in network $\boldsymbol{k} \in \boldsymbol{K}$ at time $\boldsymbol{t} \in \boldsymbol{T}$ of commodity $\boldsymbol{g} \in \boldsymbol{G}$, continuous |
| $\boldsymbol{x_{ijtg}^k}$ | Flow on link $(i, j) \in A_l^{k}$ in network $k \in K$ at time $t \in T$ of commodity $g \in G$, continuous |
| $\boldsymbol{y_{ij}^k}$ | Equal to 1 if link $(i, j) \in A'^{k}$ in network $k \in K$is protected, binary |
| $\boldsymbol{y_i^k}$ | Equal to 1 if node $i \in N'^{k}$ in network $k \in K$ is protected, binary |
| $\boldsymbol{z_{ij}^k}$ | Equal to 1 if link $(i, j) \in A'^{k}$ in network $k \in K$is interdicted, binary |
| $\boldsymbol{z_i^k}$ | Equal to 1 if node $i \in N'^{k}$ in network $k \in K$ is interdicted, binary |
| $\boldsymbol{f_{ij}^k}$ | Equal to 1 if link $(i, j) \in A'^{k}$ in network $k \in K$is disrupted, binary |

$\boldsymbol{f_i^k}$ Equal to 1 if node $i \in N'^k$ in network $k \in K$ is disrupted, binary

$\boldsymbol{\alpha_{ij}^k}$ Equal to 1 if link $(i, j) \in A'^k$ in network $k \in K$is operational, binary

$\boldsymbol{\alpha_i^k}$ Equal to 1 if node $i \in N'^k$ in network $k \in K$ is operational, binary

$\boldsymbol{\alpha'^{kr}_{ijt}}$ Equal to 1 if link $(i, j) \in A'^k$ in network $k \in K$ is restored by work crew $r \in R^k$ at time $t \in T$, binary

$\boldsymbol{\alpha'^{kr}_{it}}$ Equal to 1 if node $i \in N'^k$ in network $k \in K$ is restored by work crew $r \in R^k$ at time $t \in T$, binary

$\boldsymbol{\beta_{ijt}^k}$ Equal to 1 if link $(i, j) \in A'^k$ in network $k \in K$ is reactivated at time $t \in T$, binary

$\boldsymbol{\beta_{it}^k}$ Equal to 1 if node $i \in N'^k$ in network $k \in K$ is reactivated at time $t \in T$, binary

### 3.3. Objective Function

As discussed previously, this proposed optimization model seeks to minimize the time needed for restoration following a maximally effective attack on a network protected in such a way as to minimize disruption. To do this, we consider the weighted unmet demand across all time periods and commodities, where the defender minimizes unmet demand, the attacker maximizes it, and the defender minimizes again by restoring in an optimal sequence. Let $t_e$ be the time of the disruption. Let $m_{itg}^k$ represent the demand being fulfilled at time *t* of commodity *g* on network *k* at node *i*. Similarly, $d_{ig}^k$ represents the amount of demand for a commodity *g* before the disruption at time $t_e$. We provide a weighting parameter to allow decision-makers to account for the importance of specific nodes and commodities: $w_{itg}^k$. Let network performance at time *t* be represented by $\varphi(t) = 1 - \zeta(t)$ . Therefore, $\zeta(t)$ represents the proportion of unmet demand.

$$\zeta_{M-1}(t) = 1 - \left( \frac{\sum_{k\in K} \sum_{i\in N\underline{^k}} \sum_{g\in G} w_{itg}^{k} m_{itg}^{k}}{\sum_{k\in K} \sum_{i\in N\underline{^k}} \sum_{g\in G} w_{itg}^{k} d_{ig}^{k}} \right) \qquad \forall\, t \in T \tag{3.1}$$

So, the proposed objective function for the defender minimizes this proportion of unmet demand for a specified time horizon under a worst-case attack strategy. This is defined in Eq. (3.2) as a min-max-min optimization objective. Note that this tri-level problem cannot be solved outright, but a solution method is provided in Section 3.5.

$$\xi_{M-1} = \min_{y} \max_{z} \min_{m,x,f,\alpha,\beta} \sum_{t\in T} \zeta_{M-1}(t) \tag{3.2}$$

## 3.4. Constraints

The model can be represented as a sequence of decisions by the defender, the interdictor, and the defender again. For the first stage, protection, the defender has some budget to protect the network in any way possible. Actual methods of defense are beyond the scope of this work, but could generally be considered as hardening the components to vulnerability (physical, informational, logical, etc.) in a way that addresses the network's specific interdependencies and goals, or through the addition of redundancy by adding systems in parallel [38]. But in this model stage, constraints are all related to the defender's budget and eligibility of nodes and links to defend. The defender's defense strategy must cost less than the budget (3.3) and they may only defend eligible nodes (3.4-3.5).

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

$$y_{ij}^{k} \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{3.4}$$

$$y_{i}^{k} \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.5}$$

There are similar constraints for the next stage, the attacker's. The attacker's strike must cost less than their budget (Constraint 3.6) and only involve eligible nodes and links (Constraints 3.7-3.8).

$$\sum_{k\in K}\sum_{(i,j)\in A'^k} CI_{ij}^k z_{ij}^k + \sum_{k\in K}\sum_{i\in N'^k} CI_i^k z_i^k \leq BI \tag{3.6}$$

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

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

The final stage of the model, restoration, has the most constraints. This stage assesses the damage done based on the interactions of the players in the previous stages, assigns work crews, and aims to restore the network to pre-disruption levels in minimum time. Constraints 3.9 – 3.14 determine the failure and operational status of links and nodes in the network. A value of 1 indicates that a node is operational throughout this formulation.

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

$$1 + y_i^k - z_i^k \geq f_i^k \qquad \forall\ i \in N'^k, \forall\ k \in K \tag{3.10}$$

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

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

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

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

Only nodes that have lost function can be restored. Constraints 3.15 and 3.16 limit restoration to nodes that have been interdicted or those that lost their parent nodes.

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

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

Nodes cannot be functional until after at least one period of time has passed (Constraints 3.17 and 3.18).

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

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

The following constraints create a flow balance of commodities at each node or link for each network at a point in time (Constraints 3.19-3.26). Supply nodes must ship less than or equal to their supply, transshipment nodes must have equal inflow and outflow, and demand nodes may have some measure of unmet demand (3.19-3.22). Constraints 3.23-3.26 limit the capacity of each link and ensure that only operational links carry product.

$$\sum_{(i,j)\in A^{k}} x_{ijtg}^{k} - \sum_{(j,i)\in A^{k}} x_{jitg}^{k} \leq\ s_{ig}^{k} \qquad \forall\ i \in N_{+g}^{k}, \forall\ k \in K, \forall\ t \in T, \forall\ g \in G \tag{3.19}$$

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

$$\sum_{(i,j)\in A^{k}} x_{ijtg}^{k} - \sum_{(j,i)\in A^{k}} x_{jitg}^{k} = -m_{itg}^{k} \qquad \forall\ i \in N_{-g}^{k}, \forall\ k \in K, \forall\ t \in T, \forall\ g \in G \tag{3.21}$$

$$m_{itg}^{k} \leq\ d_{ig}^{k} \qquad \forall\ i \in N_{-g}^{k}, \forall\ k \in K, \forall\ t \in T, \forall\ g \in G \tag{3.22}$$

$$x_{ijtg}^{k} \leq\ u_{ijg}^{k} \qquad \forall (i,j) \in A^{k}\ , \forall\ k \in K, \forall\ t \in T, \forall\ g \in G \tag{3.23}$$

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

$$x_{ijtg}^{k} \leq\ u_{ijg}^{k}(\alpha_{i}^{k} + \beta_{it}^{k}) \qquad \forall (i,j) \in A^{k}, \forall\ i \in N'^{k}, \forall\ k \in K, \forall\ t \in T, \forall\ g \in G \tag{3.25}$$

$$x_{ijtg}^{k} \leq \ u_{ijg}^{k}(\alpha_{j}^{k} + \beta_{jt}^{k}) \qquad \begin{array}{l} \forall (i,j) \in A^{k}, \\ \forall\ i \in N'^{k}, \forall\ k \in K, \\ \forall\ t \in T, \forall\ g \in G \end{array} \tag{3.26}$$

Constraints 3.27 and 3.28 ensure that restoration of a link and node are completed in contiguous time periods (i.e. without interruption), respectively.

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

$$\sum_{s=1}^{t} \alpha'^{kr}_{is} \leq M(1 - \left(\alpha'^{kr}_{i(t+1)} - a'^{kr}_{it}\right)) \qquad \begin{array}{l} \forall\ i \in N'^{k}, \forall\ k \in K, \\ \forall\ t \in T, \forall\ r \in\ R^{k} \end{array} \tag{3.28}$$

The restoration time of a link is calculated using Constraints 3.29-3.30, and the restoration time for a node is calculated similarly (Constraint 3.31-3.32).

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

$$\sum_{r \in R^{k}} \sum_{t \in T} \alpha'^{kr}_{ijt} < \left(\frac{f_{ij}^{k}}{\lambda_{ij}^{k}} + 1\right) + \ M\alpha_{ij}^{k} \qquad \forall\ (i,j) \in A'^{k}, \forall\ k \in K \tag{3.30}$$

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

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

The following constraints label a link or node as “reactivated” once restoration is complete.

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

$$\frac{\sum_{r\in R^k}\sum_{s=1}^{t-1} a'^{kr}_{is}}{\left(\frac{f_i^k}{\lambda_i^k}\right)} \geq \beta_{it}^k \qquad \forall\, i \in N'^k, \forall\, k \in K, \quad \forall\, t \in T \mid t \neq 1 \tag{3.34}$$

The problem is constrained so that only one specific work crew may operate on a interdicted and disrupted component once a crew has been assigned (Constraint 3.35-3.36). Only one crew can work on a component at a time, and a crew can only work on one component (Constraints 3.37-3.39).

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

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

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

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

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

The interdependency between the components and the networks is critical. There is only flow through a link if the parent nodes in one of the other networks $k \in K$ is operational.

$$x^{k}_{ijtg} \leq u^{k}_{ijg}\left(\alpha^{\bar{k}}_{\bar{\imath}} + \beta^{\bar{k}}_{\bar{\imath}t}\right) \qquad \forall\, (i,j) \in A'^{k}, \forall\, g \in G, \forall\, \bar{\imath} \in N'^{\bar{k}} \mid \left((i,k),(\bar{\imath},\bar{k})\right) \in \Psi \; or \; \left((j,k),(\bar{\imath},\bar{k})\right) \in \Psi, \forall\, k, \bar{k} \in K, \forall \in T, \forall g \in G \tag{3.40}$$

The remaining constraints are regarding the positive or binary nature of the decision variables.

$$m^{k}_{itg} \geq 0 \qquad \forall\, i \in N^{k}_{-}, \forall\, k \in K, \forall\, t \in T \tag{3.41}$$

$$x^{k}_{ijtg} \geq 0 \qquad \forall\, (i,j) \in A^{k}, \forall\, k \in K, \forall\, t \in T \tag{3.42}$$

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

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

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

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

$$f^{k}_{ij} \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \forall\, k \in K \tag{3.47}$$

$$f^{k}_{i} \in \{0,1\} \qquad \forall\, i \in N'^{k}, \forall\, k \in K \tag{3.48}$$

$$\alpha^{k}_{ij} \in \{0,1\} \qquad \forall\, (i,j) \in A'^{k}, \tag{3.49}$$

$$\forall\, k \in K$$

$$\alpha_i^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.50}$$

$$\alpha'^{kr}_{ijt} \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \; \forall\, k \in K, \; \forall\, t \in T, \forall\, r \in R^k \tag{3.51}$$

$$\alpha'^{kr}_{it} \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K, \; \forall\, t \in T, \forall\, r \in R^k \tag{3.52}$$

$$\beta_{ijt}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \; \forall\, k \in K, \; \forall\, t \in T \tag{3.53}$$

$$\beta_{it}^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K, \; \forall\, t \in T \tag{3.54}$$

### 3.5. Decomposition Solution Approach

Decomposition is a common approach to solving multi-level problems [7], [16], [18], [37], [39]. This is an iterative method in which the main problem is decomposed into two smaller problems. For this multi-commodity problem, we will use a set covering decomposition approach for the interdiction level rather than using the dual because the Karush-Kuhn-Tucker sufficient condition is not met [26]. Ghorbani et al. proposed a modified covering decomposition problem that maximized the number of protected and interdicted components (subject to some budget), making the model an optimization one rather than a feasibility problem [26]. This substantially reduces computing time by limiting the number of combinations tested, making this an appropriate solution for a multi-commodity problem in which the additional set of commodities could substantially increase the size of the solution set.

The solution algorithm in this paper decomposes the tri-level model into two smaller problems: a master problem in which the interdicted nodes are fixed, and a subproblem where the protected nodes are fixed. Solving each of these smaller problems produces two objective values, and the algorithm iterates between the two smaller problems until the difference between the master and subproblem reaches a sufficiently small value, producing a final solution.

The master problem fixes the attack decision variables, determining the optimal protection plan *y* as the result of this min-min formulation (minimize unmet demand and minimize recovery time). This relaxed problem produces the smaller value for the model since the attacker's fixed decision seeks to maximize the unmet demand – essentially, how little unmet demand can the defender allow in response to this attack?

$$\xi_{M-1} = \min_{y} \min_{m,x,f,\alpha,\beta} \sum_{t \in T} \zeta_{M-1}(t) \tag{3.55}$$

$$\sum_{k \in K} \sum_{i \in N'^k} CP_i^k y_i^k + \sum_{k \in K} \sum_{(i,j) \in A'^k} CP_{ij}^k y_{ij}^k \leq BP \tag{3.56}$$

$$y_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \tag{3.57}$$

$$y_i^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K \tag{3.38}$$

$$1 + y_{ij}^k - \hat{z}_{ij}^k \geq f_{ij}^k \qquad \forall\, k \in K, \forall\, (i,j) \in A'^k \tag{3.59}$$

$$1 + y_i^k - \hat{z}_i^k \geq f_i^k \qquad \forall\, k \in K, \forall\, i \in N'^k \tag{3.60}$$

Constraints (3.11) – (3.54)

Similarly, the subproblem uses the defender's optimal strategy, *y*, to produce the interdiction plan *z*. This is a max-min relaxed problem that produces the higher objective value for the model. The protector wants to minimize the unmet demand, representing the worst-case scenario for the defender. Essentially, how much unmet demand can the attacker create in response to the existing protection plan?

$$\xi_{M-1} = \max_{z} \min_{m,x,f,\alpha,\beta} \sum_{t \in T} \zeta_{M-1}(t) \quad (3.61)$$

$$\sum_{k \in K} \sum_{(i,j) \in A'^k} CI_{ij}^k z_{ij}^k + \sum_{k \in K} \sum_{i \in N'^k} CI_i^k z_i^k \leq BI \quad (3.62)$$

$$z_{ij}^k \in \{0,1\} \qquad \forall\, (i,j) \in A'^k, \forall\, k \in K \quad (3.63)$$

$$z_i^k \in \{0,1\} \qquad \forall\, i \in N'^k, \forall\, k \in K \quad (3.64)$$

$$1 + \hat{y}_{ij}^k - z_{ij}^k \geq f_{ij}^k \qquad \forall\, k \in K, \forall\, (i,j) \in A'^k \quad (3.65)$$

$$1 + \hat{y}_i^k - z_i^k \geq f_i^k \qquad \forall\, k \in K, \forall\, i \in N'^k \quad (3.66)$$

Constraints (3.11) – (3.54)

Note that both of the smaller problems above have two levels, making them unable to be solved directly with a commercial optimization software. So, they must be turned into single-level optimization models using Benders' decomposition and set covering decomposition. Benders' decomposition is used to address the master problem and set covering decomposition addresses the subproblem. Using set covering for both smaller problems has been identified as a computationally inefficient method [40]. For Benders decomposition, this solution approach uses a set of defined attack plans, indexed by iteration. The new set of decision variables for that attacker plan creates corresponding constraints for the master to use in that iteration [26]. By solving the master problem, we create the inputs for the subproblem to then find the best attacker decision variables. We refer the reader to Zeng and Zhao (2013), Yuan et al., and Ghorbani-Renani (2021) for more information [37], [40], [41]

The subproblem (or interdictor problem) uses set covering decomposition. It is a feasibility-seeking problem in which at least one component must be interdicted, subject to the budget. The inequality is unique from previous inequalities. Eventually, the attacker cannot satisfy all the inequalities and the attacker algorithm terminates with a best-case attack plan in response to the existing protection plan. This is essentially a brute-force method that forces the attacking algorithm to try all possible combinations of attacks that work with the budget, ultimately selecting the most destructive attack, calculated by passing each plan to the restoration function to find the objective value. With the optimal attack plan, we return to the master problem to repeat this iterative process (indexed by $c$). For each $c$, the attacker has a best plan in response to the existing protection scenario; however, the master problem will keep expanding with the new attack scenarios [37]. Iterative algorithms such as this have convergent behavior [41]. Since both the protection and interdiction plans are known, the restoration level can be solved with these two inputs as a simple minimization problem. This is best explained by the following pseudocode (Table 3).

Let $obj_{SP}$ , $obj_{MP}$, and $obj_{RL}$ represent the objective values for the subproblem, master problem, and restoration level, respectively. IL represents the feasibility-seeking interdiction level. $\underline{P}^{c}$ stores the best interdictor solution by comparing $obj_{RL}$. Again, $c$ is the iteration counter. The results is $z^{*}, y^{*}$, or the final protection and interdiction decisions. It is possible that the algorithm may fail to converge quickly enough. The user may choose to add additional constraints on the number of iterations or the minimum cut size if the computational time is significant, as well.

**Table 3. Pseudocode of solution algorithm**

```
Step 1   Input $obj_{MP}$ ← - ∞, $obj_{SP}$ ← +∞, $\hat{Z}^c$ ← 0, $\underline{P}^c$ ← - ∞ in $c$ ← 0
Step 2   **While** $\frac{obj_{SP}-obj_{MP}}{obj_{MP}} > \varepsilon$ **do**
Step 3     Solve Master Problem and return $obj_{MP}$ and protection decision $\hat{y}$
Step 4     $\hat{y}^* \leftarrow \hat{y}, obj_{MP} \leftarrow obj_{MP,}, c \leftarrow c + 1,$
Step 5     **If** attacker budget can attack all vulnerable components $({A'}^k \cup {N'}^k)$ **then**
Step 6       $\hat{z}^c \leftarrow 1$
Step 7       Solve RL for $obj_{MP}$
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 constraint:
             $\sum_{k\in K} \sum_{(i,j)\in {A'}^k | z_{ij}^k=0} z_{ij}^k + \sum_{k\in K} \sum_{i\in {N'}^k | z_i^k=0} z_i^k \geq 1$
Step 11      Solve IL, produce $\hat{z}$
Step 12      Solve RL, produce $obj_{RL}$
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    $obj_{SP} \leftarrow obj_{SP}$
Step 17    **Return** $\hat{z}^c$
Step 18    **Update** MP by creating new decision variables and constraints
Step 19  $z^* \leftarrow \hat{z}^c$
Step 20  **Return** $z^*, y^*$ with objective value $obj_{SP}$
```

We approach the convergence of the master and subproblems in a unique way. While many papers assign an upper bound, or *UB*, as the value of the minimum of the previous upper bound and the subproblem, we instead choose to not to use an upper bound (or lower bound, as well), and instead return the value of the objective value of the subproblem, or the best attack against the current defense *Y*. We use Yao's et al.'s approach in which the values of two bi-level problems converge, not two bounds [16]. Like the method proposed in this paper, Yao's work has a min-min master problem that seeks to minimize the unmet demand (for a power network, as well), and a max-min subproblem that aims to maximize unmet demand. In both cases, the current best attack plan or defense plan in response to the prior iteration's defense or attack (respectively) is returned along with the objective value of the unmet demand. This is the same general structure as the method presented in this paper, in which plans are passed back and forth (the only key difference is that Benders' decomposition is used to solve one of the bi-level problems here). So, for this work the convergence is between $obj_{SP}$ and $obj_{MP}$, without regard to previous iterations. Furthermore, this change avoids a dilemma presented in Israeli and Wood's influential 2002 paper, in which an algorithm terminates due to a "lower bound and quasi-upper bound match," but where the returned solution is incorrect [33]. Additionally, they propose a covering decomposition algorithm in which there is no additional minimization limit on the upper bound: "the master problem is solved for any feasible solution with objective value greater than the current lower bound. The algorithm iterates until no such solution exists; at that point, the best solution found must be optimal" [18]. This suggests that the limits some algorithms place by using bounds is not inherently necessary. Furthermore, Brown, Carlyle, and Salmerón note that it is possible to perform Bender's decomposition with tri-level optimization "whose only constraints consist of super-valid inequalities," and no limits on the values the "bounds" take [2]. Zeng and Zhao assert that iterative algorithms of this nature converge to optimal solutions [41]. Essentially, the objective values for the decomposed bi-level problems converge without artificial limits on what their value is represented as.

The algorithm is highly sensitive to the number of nodes or links that are eligible for protection or interdiction, as this determines the number of potential attack and defense strategy combinations. Computational time should increase significantly as the number of components in this subset increases, and this number is the primary influence on the algorithm runtime.

# Chapter 4: Illustrative Example

## 4.1. Structure of the Systems

In this section, we will illustrate the method provided in the previous chapters with an example from the Swedish power and railway systems. This data set has been studied previously by Johansson and others for a variety of network flow analyses and component criticality problems [17], [25], [42], [43]. The system consists of an electrified railway network and a connected power network. The railway system is made of up 1363 stations connected by 2898 links of varying capacities. Trains carry eleven unique commodities that represent over 64,000 kilotons of freight and represent a significant share (98%) of the Swedish rail economy (Table 6) [25]. Each link has a specific capacity for each commodity. Although it would be interesting to examine the relationship between the national power grid and the entire railway system, the railway data set is simply too large to perform Benders' decomposition in a reasonable time. Ghorbani-Renani notes in her dissertation that "exact solution methods for solving interdiction models typically have limitations from modeling and computational complexity perspectives . . . [and the] computational difficulty of optimizing interdiction models thwarts the decision maker from effectively applying such models to moderate or large-scaled systems" [26]. Therefore, we used *k*-means clustering to produce geographical subsets of the railway network. We selected a cluster with a structure presented in Table 3 with 105 nodes. The data set is a representative sample of the overall network.

The power network provides only a single product (megawatts of electricity) and connects 119 nodes using 374 lines. There are limited physical interdependencies between the power and the railway systems, at only three points. The railway system depends on the power system. For the railway system, a station may be both a supply node and a demand node, depending on the commodities shipped. For the power system, some nodes both generated power and had a load, so their respective supply and demand is simply the difference between the two so that a node is either a supply, demand, or transshipment node. The general structure of the two networks is presented in Table 3 and is represented geographically in Figures 2 and 3. For purposes of the railway network, we count supply nodes as those that produce any amount of any product, demand nodes as those that require any amount of any product, and transshipment nodes as those that have carrying capacity for any product.

**Table 4. Railway subset and power system structures**

| Network | Nodes | Supply Nodes | Demand Nodes | Transshipment Nodes | Edges | Commodities |
|---|---|---|---|---|---|---|
| Railway | 105 | 81 | 79 | 105 | 214 | 11 |
| Power | 119 | 32 | 83 | 4 | 388 | 1 |

The railway system carries eleven commodities, although not every node produces or demands every commodity. There are is also unequal demand for each commodity.

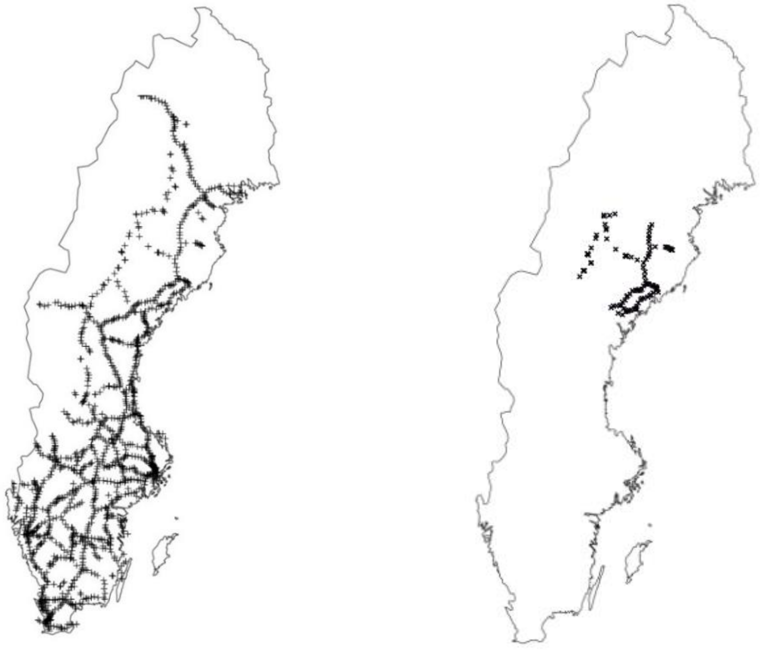

**Figure 2. Locations of all Swedish railway stations (left) and subset (right)**

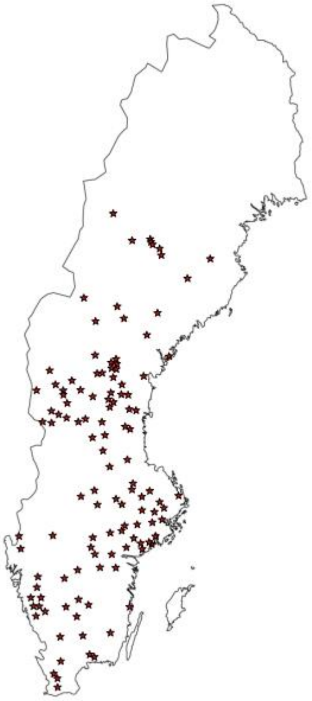

**Figure 3. Location of Swedish power stations**

## 4.2. Model Parameters

For this example, we assume that only nodes (and not links) are eligible for protection and interdiction (i.e. $A'^{k} = \emptyset$). We make this assumption for several reasons. First, it reduces the computation time for this multi-commodity example. For networks of this size, the problem requires substantial computing time and limiting the eligible components to nodes reduces the computational time while still maintaining much of the problem complexity through the included interdependencies and link capacities. Additionally, for a real-life example the point on a link at which an attack occurs can have substantial effects on the disruption and recovery. For a problem like this in which links represent physical structures that span hundreds of kilometers – so relative distance from recovery work crews matters. Essentially, an attack that occurs in the middle of a long link can be more disruptive than one that occurs close to a node, even though mathematically they represent the same attack. For this problem, to determine the subset of nodes that are eligible for attack we use the degree of each node, assuming that these nodes are somewhat important and accessible. To calculate the degree we only account for the number of connections between nodes in the same network, not between networks. This is a topological approach that is well-represented in the literature as a measure of node criticality [26], [44], [45]. We will only consider nodes with a degree greater than four for the railway system and greater than ten for the power system (Table 5). This produced twenty nodes. However, as the computational time grows exponentially with the number of components in the subset, the time was simply too long, so the subset had to be narrowed further. For the railway data set, the within those thirteen nodes, the top half with the greatest flow (absolute value of supply and demand) were kept, selecting six. This keeps the problem at a small enough size – 13 – to compute and ensures that only critical nodes are interdicted.

**Table 5. Nodes in railway subset and power systems**

| Network | Nodes | Avg. Degree | Nodes with Degree > 6 | Nodes with Degree > 8 | Nodes with Degree >10 |
|---|---|---|---|---|---|
| Railway | 105 | 4.07 | **13** | 0 | 0 |
| Power | 119 | 6.29 | 45 | 28 | **7** |

While this data set has been used extensively by other authors, protection and interdiction costs for either network have not been created and will be generated specifically for this thesis. For the railway system, protection and interdiction costs for nodes were generated using a tiered random number generation system with a uniform distribution  based on the degree of the node. The bounds for the costs are presented in Table 6. Acceptability rates (or epsilon) for nodes are generated using a uniform distribution on [0.1, 0.2] ; and performance rates are equal to 0.5 for nodes, meaning that all components will take two time periods to recover.

**Table 6. Protection and interdiction cost generation parameters**

| Degree | Range for Protection Costs | Range for Interdiction Costs |
|---|---|---|
| [6,10) | U[20, 30] $\in \mathbb{Z}$ | U[40, 50] $\in \mathbb{Z}$ |
| [10,14) | U[30, 40] $\in \mathbb{Z}$ | U[50, 60] $\in \mathbb{Z}$ |
| [14,18) | U[40, 50] $\in \mathbb{Z}$ | U[60, 70] $\in \mathbb{Z}$ |

We also needed to generate relative weights for the importance of each commodity, at each node, at each time. We assume that the weights are held constant over time, again to emulate a real-life scenario and to improve computational speed. We will use a weighting schema by commodity. For the power network, with its single commodity, all node-commodity-time combinations have a weight of 0.5. For the railway system, commodities are weighted by the percentage of the Swedish rail economy (in tens of megatons) that they occupy and held constant across all nodes for that commodity. If the demand for that commodity is zero, the weight is zero. The values are adapted from work by Whitman et al. but scaled down by a factor of $10^5$ to make the magnitude of values across the networks similar [25]. We choose not to further vary the weight by the demand at each node, because demand does not always correlate with criticality. See Table 7 for the weighting in the railway system.

**Table 7. Railway commodity weights**

| Commodity *(g)* Index | Commodity Name | Weight |
|---|---|---|
| 1 | Agriculture, forest, fishing | 0.1388 |
| 2 | Ore | 0.4361 |
| 3 | Food, beverages, tobacco | 0.0133 |
| 4 | Wood, cork, pulp, paper | 0.0953 |
| 5 | Petroleum products | 0.0225 |
| 6 | Chemicals, rubber, plastics | 0.0202 |
| 7 | Fabricated metal products | 0.0747 |
| 8 | Transport equipment | 0.0145 |
| 9 | Return materials and recycling | 0.0244 |
| 10 | Equipment for transportation | 0.0157 |
| 11 | Unidentifiable goods | 0.1445 |

The final parameters are fairly straightforward. There is one work crew for each network, so two work crews total. We set our maximum recovery time at 10 units – all nodes must be back to operational status by this time. The convergence ratio is set at 0.025 (i.e. ε = 0.025), meaning the algorithm will terminate when the master problem and subproblem produce objective values with a difference divided by the master problem that is less than this value.  Let M have a value of 12.

To solve each instance, we used Python 3.8.5 with Gurobi 9.1.1. on a 64-bit Intel ® Core™ i7-8565U CPU @ 1.80GHz laptop.

### 4.3. Results

Now, we provide the optimal protection-interdiction-restoration scenarios for the Swedish power and railway systems. In this section, we will discuss the gameplay behavior, the computational time and complexity of this problem, the results for many budget combinations, the convergence behavior of the Benders' algorithm, and the recovery with a focus on commodity-specific recovery.

#### 4.3.1. Protector-Interdictor Gameplay

We begin with the protector-interdictor interactions from a scenario in which the players have similar budgets. This will demonstrate the behavior of the Benders' cuts and the Stackelberg nature of the interaction between the attacker and the defender. Table 8 provides the component selections for the defender, the attacker, and the difference between the master problem and the subproblem (which decreases gradually until it is smaller than the terminating condition). In this table, the notation *(k,i)* refers to node *i* in network *k*, where $i \in N'^k$ and $k \in K$. Recall that *k* = 1 for the railway network and *k* = 2 for the power network.

In each iteration, the defender responds to the most disruptive attack plan found in the prior iteration. In response, the defender then develops a new attack plan while still subject to its budget. As the algorithm iterates, the difference between the subproblem and master problem decreases. After iteration six, the algorithm takes one more iteration to simply output the optimal protection and attack plans. We can also see that node (1,149) is always protected as soon as possible, indicating that this is a critical node. The subproblem objective value decreases significantly once that node is hardened.

**Table 8. Protector-interdictor gameplay for BP = 60, BI = 150**

| Step | Protected Components | Interdicted Components | $obj_{MP}$ | $obj_{SP}$ |
|---|---|---|---|---|
| 1 | N/A | (1,99), (1,130), (1,149) | 0.077 | 0.785 |
| 2 | (1,99), (1,149) | (1,78), (1,115), (1,130) | 0.143 | 0.481 |
| 3 | (1,130), (1,149)) | (1,78), (1,99), (1,113) | 0.172 | 0.328 |
| 4 | (1,78), (1,149) | (1,99), (1,115), (1,130) | 0.266 | 0.490 |
| 5 | (1,130), (1,149) | (1,78), (1,99), (1,113) | 0.231 | 0.327 |
| 6 | (1,130), (1,149) | (1,78), (1,99), (1,113) | 0.326 | 0.327 |

### 4.3.2. Component Selections by Budget Scenario

The number and selection of components is dependent on the budgets available to the players, as well as the difference between the budgets. By varying the budgets available to the defender and the attacker, we can assess the relative importance of each eligible node to the network as well as examine some factors that may lead to the selection of each node, while considering that some nodes may be critical to one commodity and unimportant to another. Budget is one way to perform a sensitivity analysis. Table 9 provides the component selections *(k,i)* for twelve combinations of protector budget (BP) and interdictor budget (BI). Y* represents the defender's selections and *Z** represents the attacker's selections. Recall that the maximum budget range required to protect a component is 50 and 70 to interdict a component.

**Table 9. Component selections by budget scenario**

| BP | BI = 50 | BI=100 | BI = 150 | BI = 200 |
|---|---|---|---|---|
| 0 | Y*: None<br>Z*: (1,149) | Y*: None<br>Z*: (1,99), (1,149) | Y*: None<br>Z*: (1,99), (1,130), (1,149) | Y*: None<br>Z*: (1,78), (1,115), (1,130), (1,149) |
| 30 | Y*: (1,149)<br>Z*: (1,99) | Y*: (1,149)<br>Z*: (1,99), (1,130) | Y*: (1,149)<br>Z*: (1,99), (1,115), (1,130) | Y*: (1,149)<br>Z*: (1,78), (1,99), (1,115), (1,130) |
| 60 | Y*: (1,99), (1,149)<br>Z*: (1,130) | Y*: (1,99), (1,149)<br>Z*: (1,115), (1,130) | Y*: (1,130), (1,149)<br>Z*: (1,78), (1,99), (1,113) | Y*: (1,130), (1,149),<br>Z*: (1,78), (1,99), (1,113), (2,19) |
| 90 | Y*: (1,99), (1,130), (1,149)<br>Z*: (1,78) | Y*: (1,99), (1,130), (1,149)<br>Z*: (1,78), (1,113) | Y*: (1,99), (1,130), (1,149)<br>Z*: (2,45), (2,110) | Y*: (1,78), (1,99), (1,149)<br>Z*: (2,19), (2,45), (2,70), |

The first row of the table, in which the defender does not have a protection budget, indicates what nodes are the highest priority for attack, since the attacker may choose whatever components they wish subject to the budget. Note that node (1,149) appears in every selection combination in this table, but this row is the only one in which the attacker may interdict it. This indicates that (1,149) is a very high-value component for the defender. This node has the largest total flow across commodities (absolute value of supply plus demand) and largest average flow of any of the eligible nodes; and has the greatest flow of commodity *(1,2)* – the ore that received the heaviest weighting. This node is a demand node for seven commodities and only a supply node for one commodity, making it a significant contributor to unmet demand if interdicted. The other three nodes that appear most frequently, (1,78), (1,99), and (1,130) are the top three eligible nodes for both overall expected flow and flow of ore. In an example in which the weighting was more evenly distributed, there may be more variation in the selection of components. This provides a possible extension for this research. Additionally, because all of the repair times for the components were constant, this factor would not influence component selection. If restoration times were not equal, we may see a preference for different components.

Also note that the majority of selected components come from the railway network, and power nodes are only attacked when the defender has a high budget. There is likely several reasons for this. First, the railway network has lower protection and interdiction costs, due to the smaller degree of these nodes. The railway network has an average protection cost of 23.33 and interdiction cost of 43.33. The power network has an average protection cost of 40.14 and an average interdiction cost of 61.86. While the average expected flow of the eligible power network nodes are greater than that of the eligible railway network nodes (234.83 and 196.47, respectively), this is skewed by one node in the power network subset with a substantially larger flow. When we compare the median expected flow across commodities of the railway network (157.36) and the power network (24.28), railway nodes are generally selected because they provide a greater "bang for one's buck" due to the greater flow and larger cost. Additionally, the power network is more interconnected, whereas the railway system is connected in more of a linear fashion, where a disruption to a node in the middle could have severe impacts. This agrees with prior work by Svegrup and Johansson with this data set that stated that the national railway system is more vulnerable to disruption than the power system [42].

### 4.3.3. Budget and Objective Value

The budget affects the objective value, which recall is a measure of the weighted unmet demand over time. As the defender's budget grows, the final objective value decreases, indicating that the system will suffer less from the optimal attack – the system is more resilient to disruption. But as the attacker budget increases, for a given defender budget, the objective value increases, as the attacker may interdict more components and cause more disruption. But as the protector budget is greater (or the difference between the attacker and defender budget is smaller), this effect is smaller. This is shown in both Table 10 and in the decreasing vertical distance between lines as BP increases in Figure 4. This suggests that even small improvements to the protector budget may have significant effects on the system resilience, but increased budget may provide diminishing returns. Note that because this is an unbalanced system with some initial unmet demand, the objective value shown is relative to the objective value in a steady-state case with no protection or interdiction. This value is approximately 0.077 (rather than 0.0 for a balanced case) and thus all objective values were divided by 0.077 for these figures.  This normalizes the results for scenarios that recover earlier or later.

**Table 10. Relative objective value for given budget combination**

| BP | BI = 50 | BI = 100 | BI = 150 | BI = 200 |
|---|---|---|---|---|
| 0 | 4.61 | 7.29 | 10.16 | 12.89 |
| 30 | 2.29 | 4.16 | 6.35 | 8.80 |
| 60 | 1.86 | 3.37 | 4.24 | 5.18 |
| 90 | 1.77 | 2.14 | 2.91 | 5.14 |

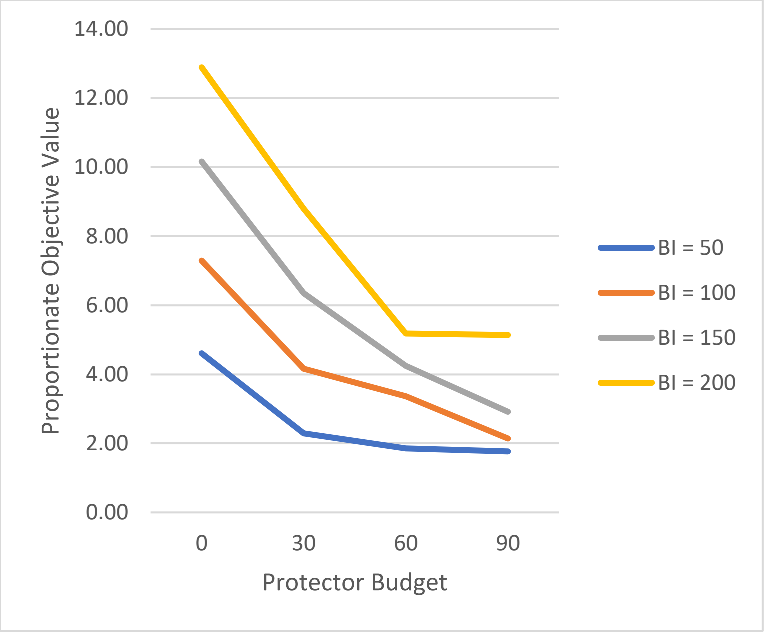

**Figure 4. Graph of objective value for given budget combination**

### 4.3.4. Budget and Computational Time

There are two keys factors that affect the computational time of this algorithm. The first, which will not be examined in this paper, is the size of the eligible subset of nodes and links that may be protected or interdicted. As the algorithm tests all feasible attack combinations and then all feasible protection combinations, this is essentially a knapsack problem, in which combinations that fall under the "weight" (budget) take on binary values. If there are more eligible nodes or links in the subset, the number of combinations increases exponentially. This has been identified in the literature as one of the key factors that limits the use of these techniques [8], [36], [46]. As the budget increases, the number of potential combinations of protected or interdicted components increases exponentially. So, if there are more eligible components, this effect on computational time will be even greater. As the budget increases, the computational time increases exponentially.

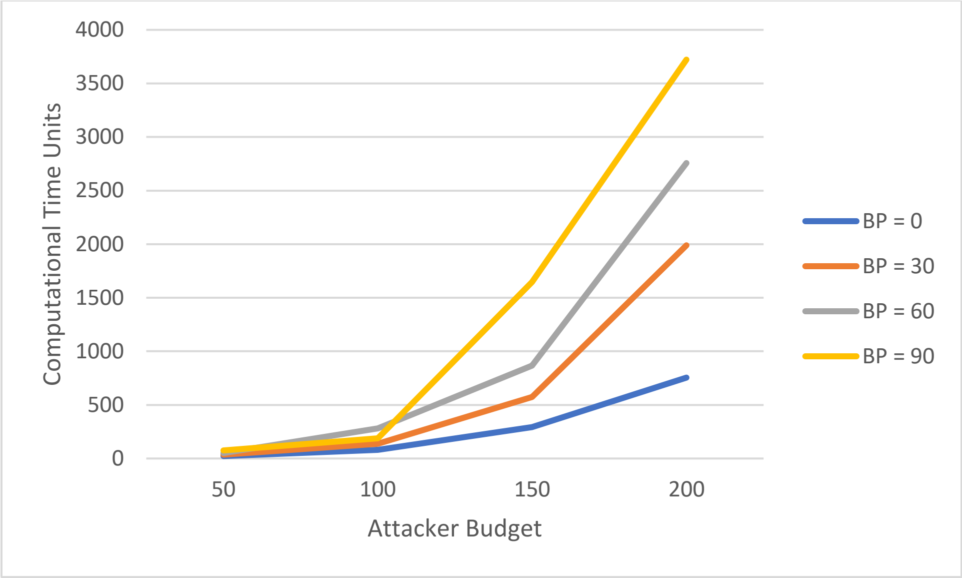

**Figure 5. Computational time units under different budget combinations**

To scale up this methodology for a larger data set ore one in which the eligible subset and the budget allow for the protection or interdiction of many nodes, a metaheuristic would likely have to be used within the subproblem to find an optimal attack plan faster or make larger cuts. Another possible alternative to improve the computational time comes from experimental validation. If early tests for small budgets reveal that a specific component is always protected (such as (1,149) in this instance), a constraint requiring that the attacker cannot interdict that component could speed up the set covering.

### 4.3.5. Convergence Behavior

In this section we will examine the convergence of the bilevel problems for all budget scenarios (Figure 6), as well as the convergence of the objective value by commodity (Figures 7 - 9). In the following (Figure 6), we can see that as the interdictor's budget increases, the initial subproblem objective value increases as well. The second iteration typically provides the greatest decrease in that value, as after that the attacker typically responds to a protection plan that protects the same node, (1,149). As the total budget increases, the number of iterations increased as well. The scenarios with the greatest number of iterations are the ones in which the respective budgets allow the protector and the interdictor to select the same number of components. The increased “gameplay” of these cases is shown by the non-uniform increases and decreases of the master and subproblems. The key rule for the convergence is that the final objective value is in between or equal to the initial objective values of the master problem and subproblem.

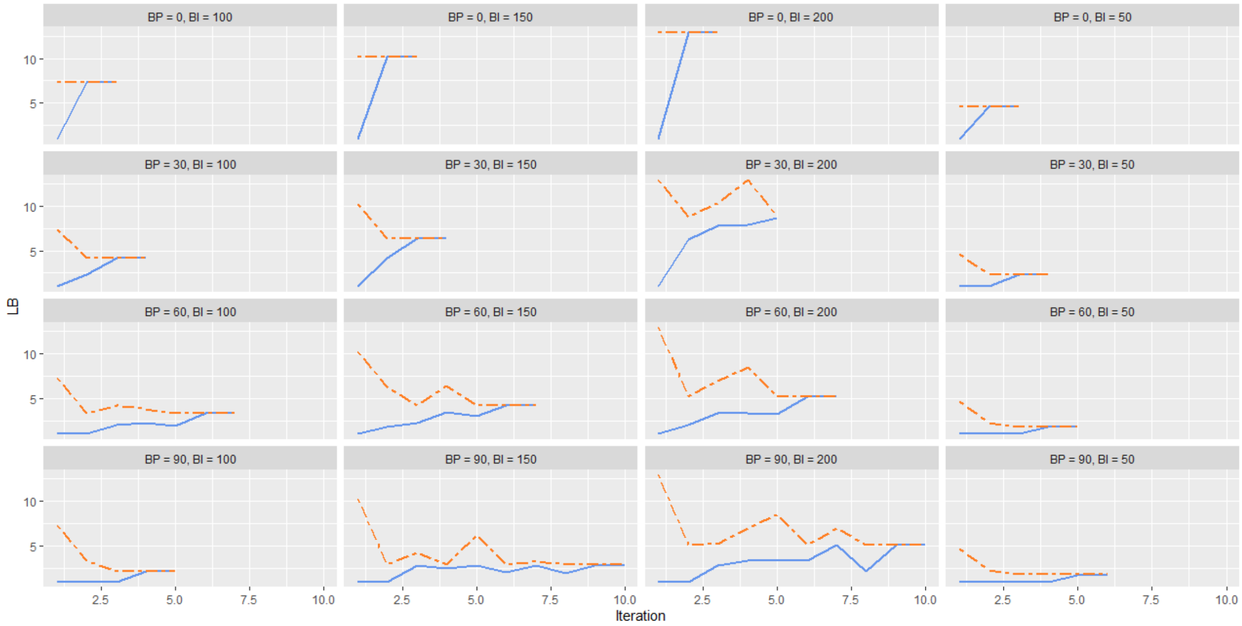

**Figure 6. Scaled convergence behavior for all budget scenarios**

We may also examine the convergent behavior by commodity. Unlike the overall objective value, the objective value by commodity does not have to constantly increase or decrease. The only rule is that the final objective value by commodity must be greater than or equal to the initial lower objective value of the master problem. The contribution to $obj_{SP}$ may increase even greater than its value in the first iteration, as the attacker prioritizes new commodities once the more heavily weighted commodities are hardened. This occurs with commodity *(2,1)* in Figure 9, as the objective value for the railway commodities decreases in both iterations but at the expense of the power network. The objective values may even cross before terminating. Given that each component has a different relationship to each commodity, and a different relationship between components by commodity, this is not surprising. The convergence and attack and defense plans are based on the aggregate objective values, not by commodity. An attacker or defender may scarifice one commodity to better protect or attak another that is either more heavily weighted or with greater flow.

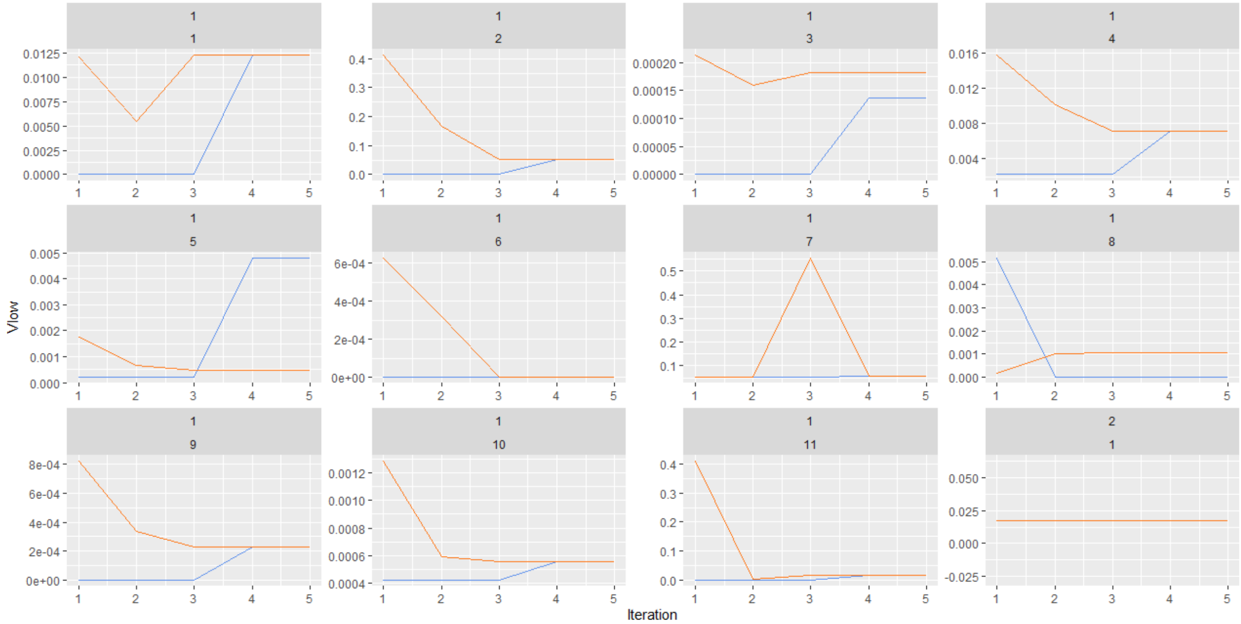

**Figure 7. Convergence behavior by commodity for BP = 90, BI = 100**

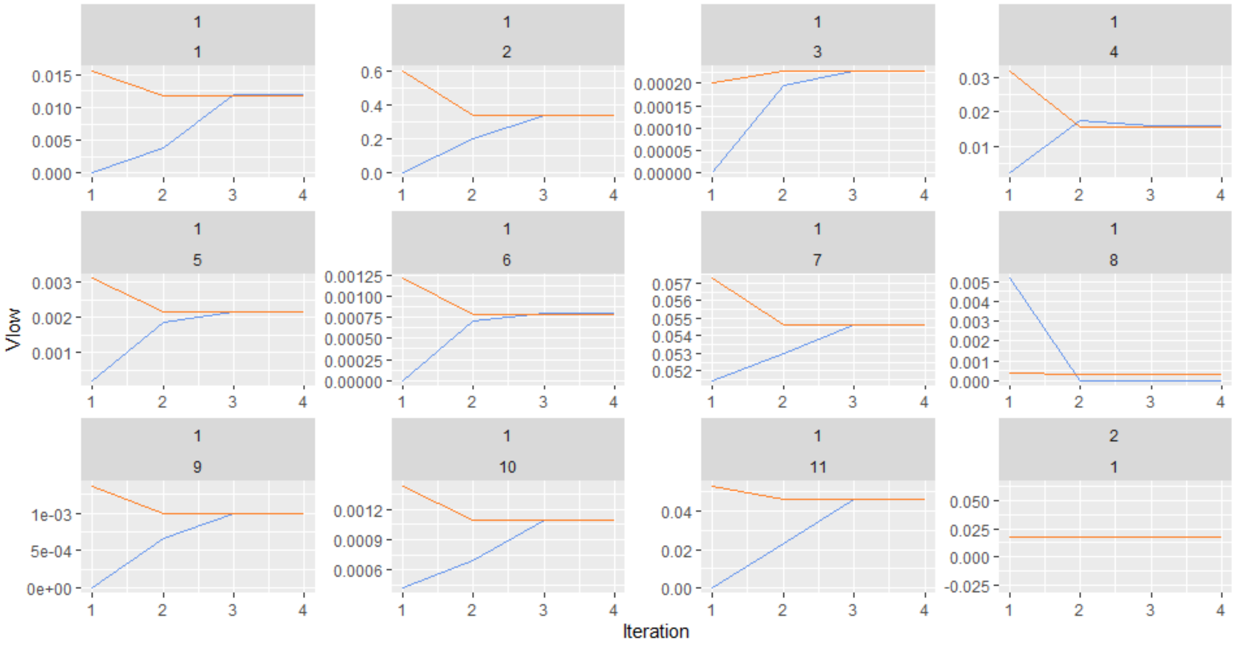

**Figure 8. Convergence behavior by commodity for BP = 30, BI = 150**

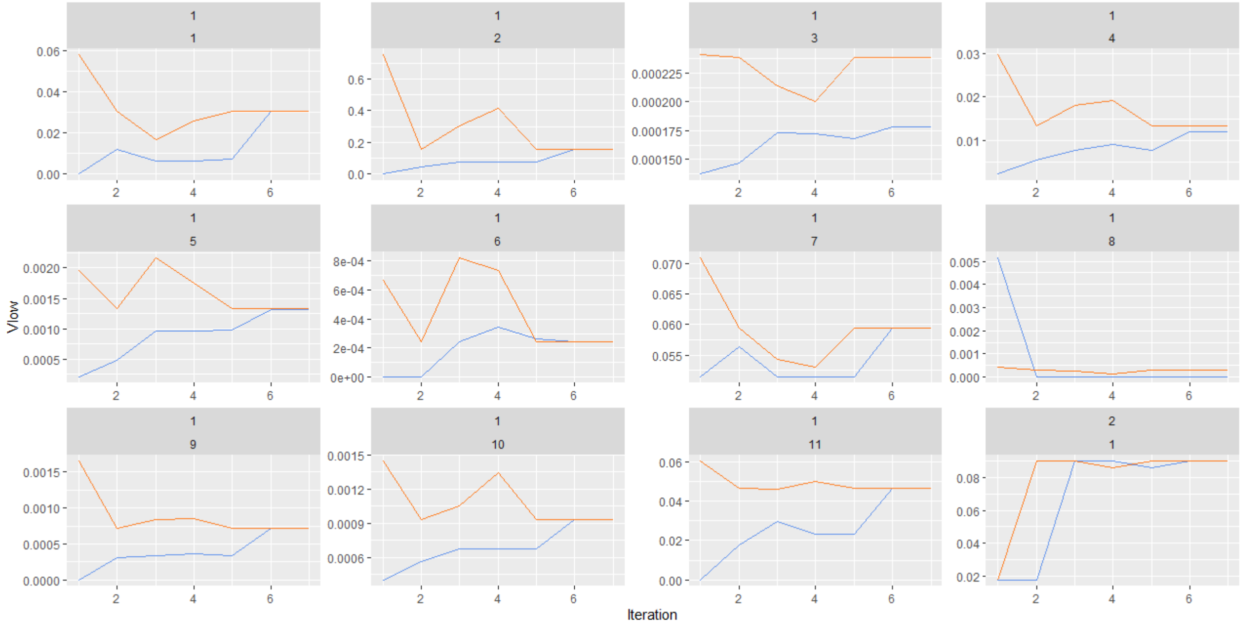

**Figure 9. Convergence behavior by commodity for BP = 60, BI = 200**

### 4.3.6. Network Recovery Trajectory

Finally, we will examine the network performance recovery trajectory, with a focus on the recovery by commodity. Again, system performance is relative to the performance at time *t* =

0, which does have unmet demand. Recovery trajectories are provided for three cases with higher attacker budgets. Not all commodities recover at an equal rate, because not all are impacted equally by the optimal attack plan. Recall that the recovery rate for all nodes is 0.5, meaning that each impacted node on a given network will take 2 time units to recover. Figures 10 - 12 show the unweighted network performance by commodity. Note the immediate drop in performance after the attack is carried out at time *t* = 1. he unweighted network performance by commodity. Note the immediate drop in performance after the attack is carried out at time *t* = 1.

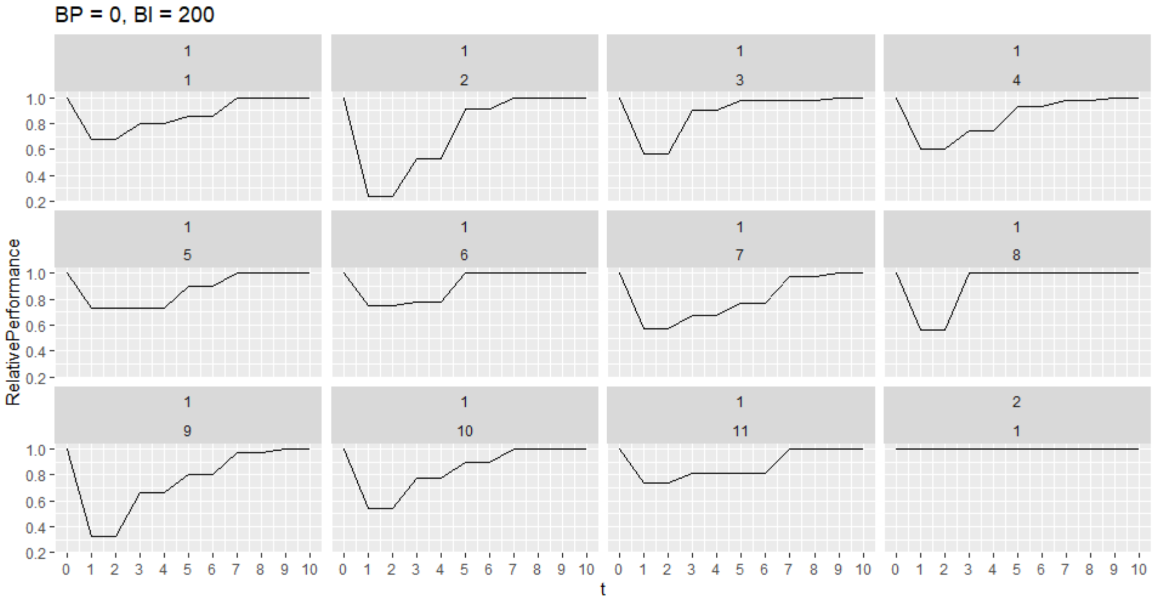

**Figure 10. Network performance trajectory by commodity for BP = 0, BI = 200**

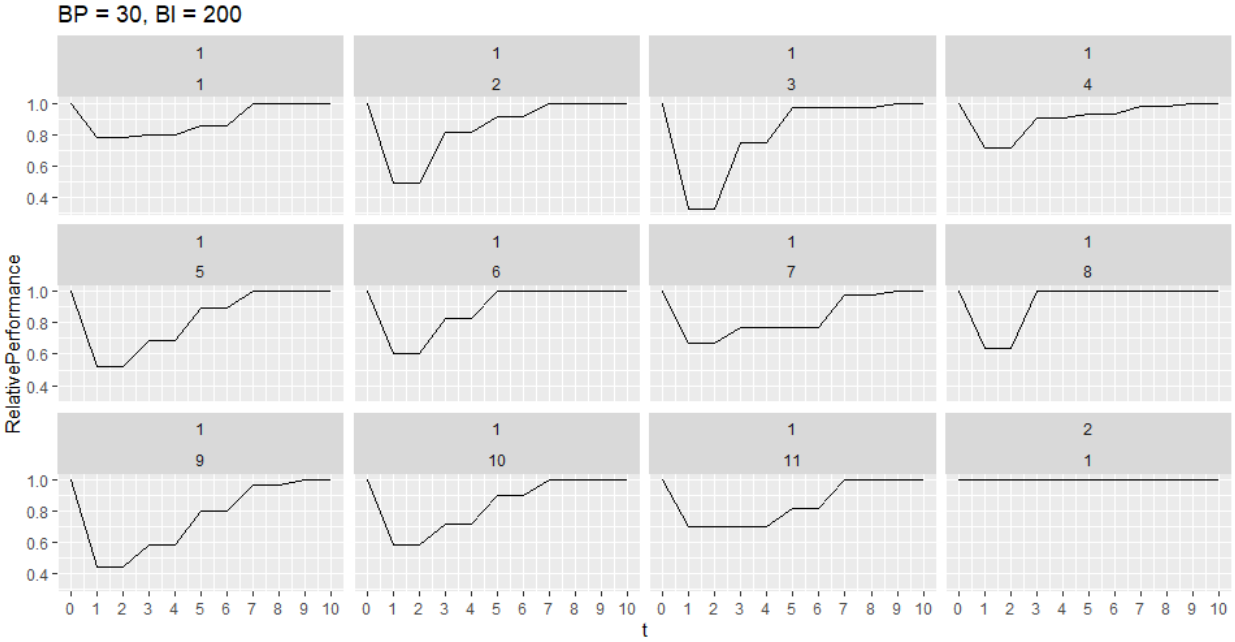

**Figure 11. Network performance trajectory by commodity for BP = 30, BI = 200**

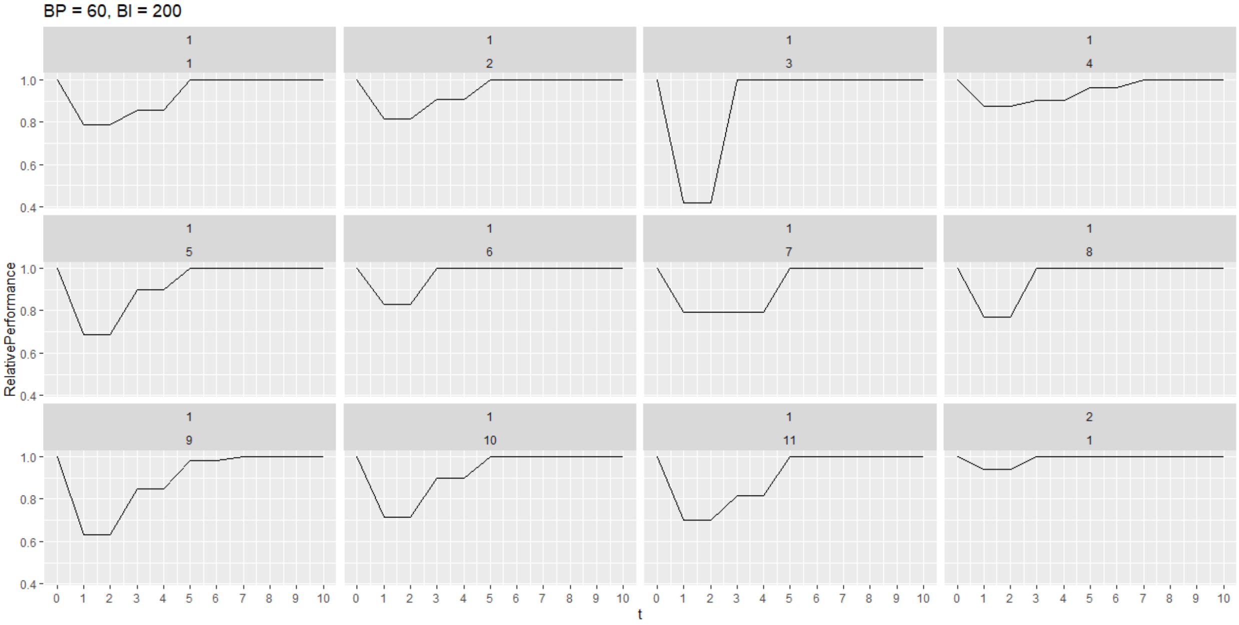

**Figure 12. Network performance trajectory by commodity for BP = 60, BI = 200**

The system recovery does not improve uniformly across commodities, as interdicted nodes have different importance levels across commodities. The relationship between the nodes (parent and child) also is commodity-dependent. Therefore, some commodities will recover faster than others. Commodities (1,4), (1,5), and (1,7) consistently took longer to recover than others. There are several potential reasons for this. First, these commodities are weighted less heavily than others. So, when the recovery is sequenced, nodes that represent heavier unmet demand for other products (such as node (1,149)) will be repaired first, even if they do not improve the system performance for Commodities (1,4), (1,5), and (1,7). Note that Commodity (1,2) generally recovers quickest, because nodes that carry more of this product (such as (1,149)) are repaired first. Second, it is possible that the supply and demand nodes for these unimportant commodities are poorly connected with few supply and demand nodes, and the loss of even a few nodes greatly limits the connection between them.

As the protector's budget increase, the initial drop in the network performance decreases, since they are able to protect either more or more critical nodes. This is particularly noticeable for Commodity (1,2), which was weighted most heavily and is the focus of both attack and defense strategies. As stated previously, increasing the protection budget decreases the vulnerability of the system. The scenario with the greatest protection budget (Figure 11) also recovers the fastest, as in this scenario the attacker chose to attack the power network. This means that the railway network faced comparatively less damage and could recover faster, since the power network has its own work crew that may work simultaneously with the crew on the railway network. For the interdictor, the selection of attack targets must balance an increase in recovery time (by targeting one network *k* at the cost of others) with an increase in initial unmet demand (perhaps by targeting key nodes across all networks).

## Chapter 5: Conclusion

Protecting critical infrastructure systems from potentially devastating attacks is a core motivation for developing better tri-level optimization models. The introduction of multi-commodity models such as this one greatly expands the scope of the sorts of networks that may be modeled with tri-level optimization. While more work has been done on bi-level models, tri-level models like the one proposed here better captures the full scale of a system's resilience, as they include recoverability – which in many cases is very limited by finances or worker availability. This work is innovative for considering multiple commodities in the protection, interdiction, and restoration phases of the model, as well as using both Benders' decomposition and set covering decomposition with multiple commodities to solve the proposed model.

This study focuses on tri-level optimization for multi-commodity systems and uses Benders' decomposition with a set covering algorithm to model the gameplay between the attacker and the defender. This proposed model considers the relative supply and demand for each commodity across networks, the weighted importance of each commodity, the link capacity by commodity, and the recovery rate in order to minimize the unmet demand after interdiction over a specified time horizon. Protection and interdiction decisions are made in an iterative manner from a designated subset of components in the system.

The model was tested on a Swedish system. The dataset included a geographically clustered subset of railway stations with eleven commodities and the Swedish power system with a single commodity. The illustrative example demonstrated the importance of the weighting metric to protection and interdiction decisions. The objective value increases as the attacker's budget increases, but the increase can be limited by small additions to the protector budget. The computational time of this algorithm is primarily a function of the number of eligible components and the budget. While the values of the master and subproblem converge across components, by component the objective values do not have the same behavior and do not constantly increase or decrease. Furthermore, the recovery is not uniform across commodities.

There are several directions that future work could take. First, while this paper only examined one weighting scheme, future work may include more sophisticated commodity weighting schema that measure the relative importance of a commodity to a particular node, perhaps using an economic or production metric. Additionally, this work was limited by the computational time. The size of the subset of eligible nodes as well as the size of the entire system could be increased through the use of a metaheuristic in the max-min subproblem. A metaheuristic could provide high-quality solutions while substantially reducing the computing time. One final extension of this work could be the implementation of partial protection. In the existing model, protection and interdiction decisions are binary. Future work could allow partial protection decisions, making the decision not only which components to protect, but also how much. These extensions could enhance the usefulness and applicability of the proposed multi-commodity model.

## References

[1] The White House, “Critical Infrastructure Security and Resilience,” *Pres. Policy Dir.*, pp. 1–12, 2013, doi: 10.1177/0360491801031002007.

[2] G. Brown, W. M. Carlyle, J. Salmerón, and K. Wood, “Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses,” *INFORMS TutORials Oper. Res.*, pp. 102–123, 2014, doi: 10.1287/educ.1053.0018.

[3] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 43–60, 2014, doi: 10.1016/j.ress.2013.06.040.

[4] M. G. Whitman, H. Baroud, and K. Barker, “Multi-Criteria Risk Analysis of Commodity-Specific Dock Investments at an Inland Waterway Port,” *Eng. Econ.*, vol. 64, no. 4, pp. 346–367, 2019.

[5] X. Gao, “A bi-level stochastic optimization model for multi-commodity rebalancing under uncertainty in disaster response,” Springer US, 2019.

[6] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, “A review of definitions and measures of system resilience,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016, doi: 10.1016/j.ress.2015.08.006.

[7] M. Ouyang, “A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks,” *Eur. J. Oper. Res.*, vol. 262, no. 3, pp. 1072–1084, 2017, doi: 10.1016/j.ejor.2017.04.022.

[8] N. Bešinović, “Resilience in railway transport systems: a literature review and research agenda,” *Transp. Rev.*, vol. 40, no. 4, pp. 457–478, 2020, doi: 10.1080/01441647.2020.1728419.

[9] L. T. T. Dinh, H. Pasman, X. Gao, and M. S. Mannan, “Resilience engineering of industrial processes: Principles and contributing factors,” *J. Loss Prev. Process Ind.*, vol. 25, no. 2, pp. 233–241, 2012, doi: 10.1016/j.jlp.2011.09.003.

[10] E. D. Vugrin, D. E. Warren, and M. A. Ehlen, “Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane,” *Process Saf. Prog.*, vol. 30, no. 3, pp. 280–290, 2011, doi: 10.1002/prs.

[11] Y. Y. Haimes, “On the definition of resilience in systems,” *Risk Anal.*, vol. 29, no. 4, pp. 498–501, 2009, doi: 10.1111/j.1539-6924.2009.01216.x.

[12] N. Ghorbani-Renani, A. D. González, K. Barker, and N. Morshedlou, “Protection-interdiction-restoration: Tri-level optimization for enhancing interdependent network resilience,” *Reliab. Eng. Syst. Saf.*, vol. 199, no. June 2019, 2020, doi: 10.1016/j.ress.2020.106907.

[13] J. E. Ramirez-Marquez, C. M. Rocco, and K. Barker, “Bi-Objective Vulnerability-Reduction Formulation for a Network under Diverse Attacks,” *ASCE-ASME J. Risk Uncertain. Eng. Syst. Part A Civ. Eng.*, vol. 3, no. 4, p. 04017025, 2017, doi: 10.1061/ajrua6.0000929.

[14] K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, “Resilience-based network component importance measures,” *Reliab. Eng. Syst. Saf.*, vol. 117, pp. 89–97, Sep. 2013, doi: 10.1016/j.ress.2013.03.012.

[15] J. P. Babick, “Tri-Level Optimization of Critical Infrastructure Resilience,” 2009.

[16] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, “Trilevel optimization in power network defense,” *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 37, no. 4, pp.

712–718, 2007, doi: 10.1109/TSMCC.2007.897487.

[17] M. J. McCarter, K. Barker, J. Johansson, and J. E. Ramirez-Marquez, “A Bi-Objective Formulation for Robust Defense Strategies in Multi-Commodity Networks,” *Reliab. Eng. Syst. Saf.*, vol. 176, pp. 154–161, 2018.

[18] E. Israeli, “System Interdiction and Defense,” Naval Postgraduate School, 1999.

[19] K. Hausken and G. Levitin, “Review of systems defense and attack models,” *Int. J. Performability Eng.*, vol. 8, no. 4, pp. 355–366, 2012.

[20] J. E. Ramirez-Marquez, C. M. Rocco, and G. Levitin, “Optimal network protection against diverse interdictor strategies,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 3, pp. 374–382, 2011, doi: 10.1016/j.ress.2010.10.003.

[21] M. G. H. Bell, U. Kanturska, J. D. Schmöcker, and A. Fonzone, “Attacker-defender models and road network vulnerability,” *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, vol. 366, no. 1872, pp. 1893–1906, 2008, doi: 10.1098/rsta.2008.0019.

[22] J. G. Jin, L. Lu, L. Sun, and J. Yin, “Optimal allocation of protective resources in urban rail transit networks against intentional attacks,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 84, pp. 73–87, 2015, doi: 10.1016/j.tre.2015.10.008.

[23] J. Salmerón, K. Wood, and R. Baldick, “Optimizing Electric Grid Design Under Asymmetric Threat (II),” 2004.

[24] E. Kuttler, K. Barker, and J. Johansson, “Network Importance Measures for Multi-Component Disruptions,” in *2020 Systems and Information Engineering Design Symposium (SIEDS)*, 2020, pp. 1–6, doi: 10.1109/SIEDS49339.2020.9106662.

[25] M. G. Whitman, K. Barker, J. Johansson, and M. Darayi, “Component importance for multi-commodity networks: Application in the Swedish railway,” *Comput. Ind. Eng.*, vol.

112, pp. 274–288, Oct. 2017, doi: 10.1016/j.cie.2017.08.004.

[26] N. Ghorbani-Renani, “Tri-Level Interdiction Model for Enhancing Interdependent Network Resilience,” University of Oklahoma, 2021.

[27] I. Ahmad, A. Clark, A. Sabol, D. Ferris, and A. Aved, “Maximizing resilience under defender attacker model in heterogeneous multi-networks,” in *Proceedings - 2020 3rd International Conference on Data Intelligence and Security, ICDIS 2020*, 2020, pp. 117–126, doi: 10.1109/ICDIS50059.2020.00022.

[28] J. Qiao, D. Jeong, M. Lawley, J. P. P. Richard, D. M. Abraham, and Y. Yih, “Allocating security resources to a water supply network,” *IIE Trans. (Institute Ind. Eng.*, vol. 39, no. 1, pp. 95–109, 2007, doi: 10.1080/07408170600865400.

[29] L. R. Ford, D. R. Fulkerson, and J. Kennington, “A suggested computation for maximal multi-commodity network flows,” *Manage. Sci.*, vol. 5, no. 1, pp. 97–101, 1958, doi: 10.1287/mnsc.1040.0269.

[30] A. T. Murray, T. C. Matisziw, and T. H. Grubesic, “Critical network infrastructure analysis: interdiction and system flow,” *J. Geogr. Syst.*, vol. 9, no. 2, pp. 103–117, Jun. 2007, doi: 10.1007/s10109-006-0039-4.

[31] A. D. González, L. Dueñas-Osorio, M. Sánchez-Silva, and A. L. Medaglia, “The Interdependent Network Design Problem for Optimal Infrastructure System Restoration,” *Comput. Civ. Infrastruct. Eng.*, vol. 31, no. 5, pp. 334–350, 2016, doi: 10.1111/mice.12171.

[32] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, “Defending critical infrastructure,” *Interfaces (Providence).*, vol. 36, no. 6, pp. 530–544, 2006, doi: 10.1287/inte.1060.0252.

[33] E. Israeli and R. K. Wood, “Shortest-Path Network Interdiction,” *Networks*, vol. 40, no. 2,

pp. 97–111, 2002, doi: 10.1002/net.10039.

[34] A. Haghani and S. C. Oh, “Formulation and solution of a multi-commodity, multi-modal network flow model for disaster relief operations,” *Transp. Res. Part A Policy Pract.*, vol. 30, no. 3, pp. 231–250, 1996, doi: 10.1016/0965-8564(95)00020-8.

[35] J. F. Benders, “Partitioning procedures for solving mixed-variables programming problems,” *Numer. Math.*, vol. 4, no. 1, pp. 238–252, 1962, doi: 10.1007/BF01386316.

[36] N. Ghorbani-Renani, K. Barker, and A. D. González, “Hybrid Algorithms for Enhanced Efficiency and Scalability of Tri-Level Protection-Interdiction-Restoration Models,” 2021.

[37] N. Ghorbani-Renani, A. D. González, and K. Barker, “A decomposition approach for solving tri-level defender-attacker-defender problems,” *Comput. Ind. Eng.*, vol. 153, no. November 2020, 2021, doi: 10.1016/j.cie.2020.107085.

[38] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Modeling and simulating critical infrastructures and their interdependencies,” *Proceedings of the Hawaii International Conference on System Sciences,* vol. 37, pp. 873–880, 2004.

[39] D. Henry and J. Emmanuel Ramirez-Marquez, “Generic metrics and quantitative approaches for system resilience as a function of time,” *Reliab. Eng. Syst. Saf.*, vol. 99, pp. 114–122, 2012, doi: 10.1016/j.ress.2011.09.002.

[40] W. Yuan, L. Zhao, and B. Zeng, “Optimal power grid protection through a defender – attacker – defender model,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 83–89, 2014, doi: 10.1016/j.ress.2013.08.003.

[41] B. Zeng and L. Zhao, “Solving two-stage robust optimization problems using a column-and-constraint generation method,” *Oper. Res. Lett.*, vol. 41, pp. 457–461, 2013, doi: 10.1016/j.orl.2013.05.003.

[42] L. Svegrup and J. Johansson, “Vulnerability analyses of interdependent critical infrastructures: Case study of the Swedish national power transmission and railway system,” in *Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015*, 2015, pp. 4499–4507, doi: 10.1201/b19094-590.

[43] T. Sonesson and J. Johansson, “Modeling National Interdependent Critical Infrastructures: Application and Discussion for the Swedish Power and Internet Backbone,” in *29th European Safety and Reliability Conference*, 2019, pp. 1–8, doi: 10.3850/981-973-0000-00-0.

[44] Y. Du, C. Gao, S. Mahadevan, and Y. Deng, “A new method of identifying influential nodes in complex networks based on TOPSIS,” *Phys. A Stat. Mech. its Appl.*, vol. 399, pp. 57–69, 2014.

[45] Y. P. Fang, N. Pedroni, and E. Zio, “Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems,” *IEEE Trans. Reliab.*, vol. 65, no. 2, pp. 502–512, 2016, doi: 10.1109/TR.2016.2521761.

[46] P. Alvarez San Martin, “Tri-Level Optimization Models to Defend Critical Infrastucture,” Naval Postgraduate School, 2007.