ANALYTICAL APPROACHES TO PROTECTION PLANNING IN RAIL-TRUCK INTERMODAL TRANSPORTATION

by

© Hassan Sarhadi

A Dissertation Submitted to the

School of Graduate Studies

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Faculty of Business Administration

Memorial University of Newfoundland

May 2015

St. John's Newfoundland and Labrador

ABSTRACT

A significant volume of traffic uses a rail-truck intermodal transportation network, making it the preferred transportation medium for customers. Thus, the associated infrastructure of rail-truck intermodal transportation should be considered critical, i.e., systems and assets whose destruction (or disruption) would have a crippling effect on security, economy, public health, and safety. Disruptions could be induced by nature such as hurricane Katrina in 2005, or man-made disturbances such as the 9/11 terrorist attacks in the United States. This thesis proposes an analytical approach to preserve, as much as possible, the functionality of a rail-truck intermodal transportation system in the wake of worst-case attacks. As such, it will serves as an aid to the top managers to compare the cost of implementing protective measures with the benefits that such measures could bring. A tri-level Defender-Attacker-Defender (DAD) approach is proposed to model this situation, where the outermost problem belongs to the network operator with a limited budget to protect some of the terminals, the middle level problem belongs to the attacker with enough resources to interdict some of the un-protected terminals, and the innermost problem belongs to the intermodal operator who attempts to meet the demand on a reduced network with the minimum cost. Since the resulting model is very difficult to solve by any optimization package, efficient solution techniques have been developed for solving this model. Finally, the proposed framework is applied to the rail-truck intermodal transportation network of a Class I railroad operator in North America to discover the optimal way to protect the system.

ACKNOWLEDGEMENTS

I would like to express my utmost gratitude to Dr. Manish Verma and Dr. David Tulett, my thesis supervisors, for their unwavering support. I should also mention Dr. Kara Arnold (Director, PhD program), Dr. Dale Foster, Dr. Jeffery Parsons, and Donna Fitzgerald for their persistent and kind help during my study.

Lastly, I'm thankful to my family members, my mother, father, my wife and my sisters, for their kind support and motivation without which it would have been impossible to overcome difficulties.

DEDICATION

This thesis is dedicated to my family members for their true love and their significant roles in my life.

Table of Contents

Chapter 1: Introduction **1**

1.1 Background and Motivation *1*

1.2 Literature Review *2*

1.2.1 The Disaster Operations Life Cycle *3*

1.2.3 Vulnerability Assessment 7

1.2.4 Fortification Planning 13

1.2.5 Rail-Truck Intermodal Transportation 19

1.3 Conclusion *23*

1.4 Motivation and Objectives *24*

1.5 Co-authorship Statement *25*

Chapter 2: A Defender-Attacker-Defender Framework to the Optimal Fortification of a Rail-Truck Intermodal Terminal Network **27**

2.1 Introduction *27*

2.2 Problem Description *27*

2.3 Defender-Attacker-Defender Framework *30*

2.4 Mathematical Model *31*

2.4.1 Assumptions 31

2.4.2 Sets 32

2.4.3 Parameters 34

2.4.4. Intermodal Operator's Decision Variables 35

2.4.5 Network Operator's Decision Variable 35

2.4.6 Interdictor's Decision Variable 35

2.4.7 Mathematical Formulation 35

2.4.8 Explanation of the Constraints 37

2.5 Introducing a Realistic Case Study *40*

2.5.1 Estimation of Parameters 42

2.6 Numerical Analysis *42*

2.6.1 Part One: the Network Operator and the Interdictor Can Protect/Disrupt One Terminal 43

2.6.2 Part Two: the Network Operator and the Interdictor Can Protect/Disrupt Two Terminals 44

2.7 Conclusion *45*

Chapter 3: Protection Planning of a Rail-Truck intermodal Terminal Network: Extensions and Traffic-based Solution Technique **48**

3.1 Introduction *48*

3.2 Problem Description *48*

3.3 Assumptions *49*

3.4 Path-based Defender-Attacker-Defender Framework *50*

3.4.1 Mathematical Model 50

3.5 Numerical Analysis *54*

3.5.1 Parameter Estimation: 54

3.6 Solution Algorithms *55*

3.6.1 Complete Enumeration 56

3.6.2 Implicit Enumeration 57

3.6.3 Proposed traffic-based heuristic 60

3.6.3.1 Numerical Analysis 61

3.6.3.2 Analysis of Results 62

3.6.3.3 Capacity and Network Connectivity 63

3.7 Conclusion *66*

Chapter 4: A Decomposition-based Solution Technique for Protection Planning of a Rail-Truck Intermodal Terminal Network 68

4.1 Introduction *68*

4.2 Decomposition based Heuristic *68*

4.2.1 The First Stage 69

4.2.2 The Second Stage 69

4.2.3 Linearization Scheme 73

4.3 Numerical Analysis *75*

4.3.1 Problem setting 75

4.3.2 Solution 76

4.3.3 Computational Performance 81

4.3.4 Insights 82

4.4 Conclusion *84*

Chapter 5: Tabu Search Metaheuristic for Solving Protection Planning in Rail-Truck Intermodal Transportation 87

5.1 Introduction *87*

5.2 Literature Review *88*

5.2.1 Metaheuristics 88

5.2.2 Tabu Search 91

5.3 A Simple Outline of Tabu Search Algorithm *94*

5.4 Tabu search Implementation for solving the DAD problem *95*

5.5 Numerical Analysis *99*

5.6 Insights *103*

5.7 Conclusion *104*

Chapter 6: Conclusion and Future Research **105**

6.1 Conclusion *105*

6.2 Future Directions *106*

6.2.1 Network Design Considerations 106

6.2.2 Uncertainty and Asymmetric Information 108

6.2.3 Random Attacks 108

6.2.4 Efficient Solution Methods for the Intermodal Operator's Problem 109

References **110**

Appendix A: Defined Train Services on the Network **117**

Appendix B **118**

Appendix C **119**

List of Figures

FIGURE 1-1. THE PROPOSED TAXONOMY OF PLANNING EFFORTS IN DISRUPTION MANAGEMENT STUDIES 5

FIGURE 1-2: STRUCTURE OF THE THESIS 24

FIGURE 2-1: HIERARCHICAL STRUCTURE OF THE FORTIFICATION PLANNING 29

FIGURE 2-2: A DEPICTION OF RAIL-TRUCK INTERMODAL TRANSPORTATION 30

FIGURE 2-3. TRAIN SERVICE V DEFINED ON THE NETWORK 33

FIGURE 2-4: LOCATION OF 18 TERMINALS (ADAPTED FROM: VERMA & VERTER, 2010) 41

FIGURE 2-5: LOCATION OF 37 CUSTOMERS (ADAPTED FROM: VERMA & VERTER, 2010) 41

FIGURE 3-1: TREE SEARCH 58

FIGURE 4-1: PSEUDO CODE FOR THE DECOMPOSITION ALGORITHM 75

FIGURE 4-2: INTERACTION BETWEEN THE MASTER PROBLEM AND THE SUB-PROBLEM 75

FIGURE 4-3: COST IMPOSED TO THE SYSTEM FOLLOWING EACH DEFENSE SCENARIO 79

FIGURE 5-1: 1-SWAP MOVEMENT 96

FIGURE 5-2: 2-SWAP MOVEMENT 96

FIGURE 5-3: FLOWCHART OF THE PROPOSED TABU SEARCH ALGORITHM 98

List of Tables

TABLE 2-1: TERMINAL LEGENDS 40

TABLE 2-2: RESULTS OF DEFENDING/ATTACKING 1 TERMINAL 43

TABLE 2-3: RESULTS OF DEFENDING/ATTACKING 2 TERMINALS 44

TABLE 3-1 SUMMARY OF COMPUTATION TIME 61

TABLE 3-2: SNAPSHOT OF THE NINE SCENARIOS 63

TABLE 3-3: CAPACITY UTILIZATION AND CONNECTIVITY 65

TABLE 4-1: OBJECTIVE FUNCTION VALUES FOR THE FOUR SCENARIOS 77

TABLE 4-2: TRAFFIC SPLIT BETWEEN TRUCK-ONLY (T) AND RAIL-TRUCK INTERMODAL (RT) 80

TABLE 4-3: NUMBER OF INTERMODAL TRAIN SERVICES 80

TABLE 4-4: CPU TIME (SECONDS) FOR THE THREE FORTIFICATION TECHNIQUES 82

TABLE 4-5: CAPACITY UTILIZATION OF THE TERMINALS 83

TABLE 5-1: RAPID GROWTH OF SIZE OF THE TREE SEARCH 87

TABLE 5-2: OBJECTIVE FUNCTION VALUES OF SOLUTIONS FOUND BY FOUR VARIANTS OF TABU SEARCH 101

TABLE 5-3: COMPUTATIONAL PERFORMANCE OF FOUR VARIANTS OF TABU SEARCH 102

Chapter 1: Introduction

1.1 Background and Motivation

Critical infrastructure, as defined by the U.S. Government, consists of systems and assets, physical or virtual, which have a vital role to the society such that destruction of them would have a crippling effect on security, economy, public health, safety or any combination of these.

The infrastructures of supply chains, like other kinds of critical infrastructures, are susceptible to risk of failures. Recent high-profile events, like the attacks of 11 September 2001, hurricane Katrina, and earthquakes in Japan, especially the ones that hit nuclear power stations in March 2011, clearly show how disruptions can plague supply chains and impose direct and indirect costs to society. In response to these events, the United States and other countries have started initiatives to assess threats to critical infrastructures and to develop defense plans that help prevent attacks and mitigate their effects. This is especially important during strategic planning because long term decisions, like network design and facility location, cannot be easily modified.

In an effort to increase common understanding about the risks that supply chains are facing, Chopra and Sodhi (2012) have categorized a variety of risks, including the risk of disruption, for supply chains together with their drivers. They defined disruption as a risk that negatively influences the flow of material anywhere in the supply chain which can happen due to war or terrorism, natural disasters, and labour strikes.

It should be noted that in addition to the surge in the number and magnitude of risks in recent decades, tightly optimized and lean supply chain practices are contributing to the vulnerability of these systems. Thus, in contradiction to conventional wisdom, it can be argued that supply chains should have more redundancy to provide a buffer against uncertainties and risks. Nevertheless, companies have historically been reluctant to invest in additional supply chain infrastructure or inventories despite large payoffs that such investments can have if a disruption happens. Yet, some companies, like WalMart, have launched programs like business continuity planning (BCP) to smooth their operations during various disruptions (Buffy, 2006).

In recent years, growing freight volumes, increasingly congested roads, and environmental concerns have contributed to the prominence of rail-truck intermodal transportation such that the volume of such traffic has increased more than three times in the last three decades (AAR, 2015). Despite such importance, the issue of vulnerability assessment of rail-truck intermodal transportation to disruptions and taking preventive fortification plans has not been investigated so far.

1.2 Literature Review

This literature review discusses the planning efforts to address disruptions in supply chains in general and rail-truck intermodal transportation in particular. In the first part of this literature review, the research efforts regarding the disruption management will be categorized and presented. In order to better understand how to manage disruptions, it is

necessary to know all the activities around managing disruptions. In the first part of this literature review, these key activities will be presented.

The context of rail-truck intermodal transportation will be elaborated in the second part of the literature review.

1.2.1 The Disaster Operations Life Cycle

There is a need to organize activities that can be done before and after the occurrence of the disaster. The efforts to organize such operations began with Tufekci and Wallace (1998) who organized activities into two categories, pre-event and post-event activities. Pre-event activities include predicting and analyzing potential threats and preparing plans to lessen their effects while the post-event activities contain locating, allocating and managing available resources for an effective response. Therefore, a successful disaster relief plan should integrate activities of both categories.

In an extensive review, Altay and Green (2006), in line with United States emergency management practice (NEHRP, 2009) further categorized a disaster operations life cycle as having four phases: mitigation, preparedness, response, and recovery. *Mitigation* is the combination of measures to either prevent the disaster or to reduce its effects. *Preparedness* includes activities to prepare the community to respond when the disaster hits. *Response* is the actual employment of resources and emergency procedures to preserve lives and properties. Finally, *recovery* involves the actions taken after the occurrence of a disaster to stabilize the situation and to restore it to normalcy. In a similar

way, Wright, Liberatore, and Nydick (2006) identified four phases for a disaster relief life cycle as: planning, prevention, response, and recovery. While the response and recovery are exactly the same as defined by Atlay and Green (2006), they have defined the planning as the set of long term and strategic activities including policy and risk analysis, system design, and resource allocation. Prevention, on the other hand, embraces short-term activities, like patrolling borders and screening airline passengers, to identify and eliminate threats.

Among pre-disruption activities, the planning is deemed to play the major role because it has a significant impact on post-disruption activities like response and recovery. In order to better understand this important phase of disruption management, in the remainder of this review, the major planning efforts regarding disruptions in supply chains will be categorized in three major classes as shown in Figure 1-1:

- Network design and facility location models: in these models the question is how to design networks or to locate facilities at the beginning to satisfy all the demands and to hedge against future interruptions in the best way;
- Vulnerability assessment: in these models, the emphasis is on preparing for the worst-case by finding the set of system components that, if lost, would dramatically deteriorate the system performance;
- Fortification planning: these models extend the interdiction and design models. For networks that have been formed and their complete redesign would be too

costly, fortification models show how to allocate limited resources to improve their performance against possible disruptions;

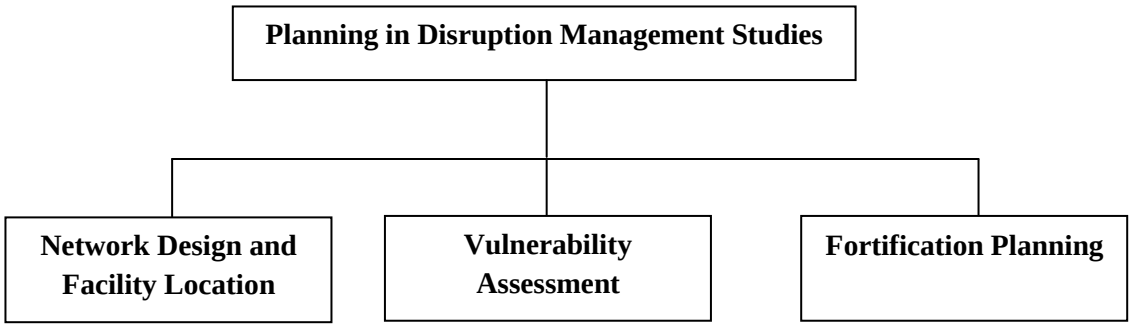

Figure 1-1. The proposed taxonomy of planning efforts in disruption management studies

1.2.2 Network Design and Facility Location Models

In network design models the assumption is that no network currently exists and therefore these models start from scratch to form a network that can satisfy the demands as well as withstand against disruptions. More specifically, the main premise of these models is that the impact of disruptions can be mitigated by the initial design of a system.

Thus, in the network design models, a network of arcs and nodes needs to be created where each node serves as either a source, a sink or a transshipment node and the whole network is responsible for delivering the commodities from the source node to the sink node using arcs and transshipment nodes.

A rather similar design problem against disruption, with important practical applications in the design of telecommunication networks, is the survivable network design (SND)

problem which seeks a minimum cost robust network configuration that provides a number of alternative paths between nodes of the network (Grotschel, Monma & Stoer, 1995). SND problems consist of selecting links so that the sum of their costs is minimized while some given requirements (like minimum number of paths between every pair of nodes that have to exist in any situation) are satisfied. Implementing the SND principle ensures that, after the occurrence of the disruption, the service could be restored around the damaged components. This is because alternative paths will be used in this situation to reroute traffic and bypass the damaged components. In most SND studies the random failure of a single network component has been considered which may not guarantee network robustness against intentional disruptions (Kerivin & Mahjoub, 2005).

In facility location models, each facility provides services to its neighboring customers and the problem is where to locate these facilities to minimize the total cost of accessing them from customers' locations.

Snyder and Daskin (2005) extended the classical p-median and uncapacitated fixed charge location problems to account for failures of facilities. Also, Peng, Snyder, Lim, and Liu (2011) proposed a mathematical model for designing a logistics network that can perform well in pre- and post-disruption conditions.

Resilient design of coverage-based service systems has been accomplished by O'Hanley and Church (2011). The authors proposed a model that aims to locate a set of facilities

such that the combination of initial demand coverage and the minimum coverage following a loss is maximized.

However, for the networks or facilities that have been formed, redesigning the entire system is not always a reasonable solution given the high costs involved with relocating facilities and building new networks, and so this is why other strategies should be pursued.

First, in order to assess the significance of disruptions on a given system, the worst-case vulnerability analysis needs to be done with the aid of interdiction models. Then, after getting a sense of the magnitude of disruptions, in order to optimize the fortification of the system, fortification models can be used to decide which parts of the existing network should be fortified. In other words, as a less costly alternative, the resistance of existing infrastructures can be enhanced through efficient investments in protection and security measures. Planning for network protection is an enormous challenge given the complexity of today's logistics systems, the interdependencies among them, and the diversity of hazards and threats.

1.2.3 Vulnerability Assessment

Most infrastructure systems are designed to handle disruptions that result from accidents and random acts of nature. The system reliability techniques have been proposed for estimating vulnerability through finding cut-sets, which are the sets of events that are most likely to disrupt a system. The system is robust if the combined probability of such

events is sufficiently low. The downside of this kind of analysis is that the infrastructure that resists against random failure or whose cut-sets have a low probability of occurrence, may not resist against low probability but high consequence disruptions, like an intelligent malicious attack, and this is why reliability analysis is not enough to prevent against high consequence low probability events (Garcia, 2008).

Interdiction models have been used extensively over the past few years as a tool for assessing network vulnerabilities against worst-case disruptions. As the first step into modeling deliberate attacks, interdiction models have a long history in military and homeland security operations. Interdiction problems are inherently bi-level since they involve conflicting decisions of an interdictor, who tries to degrade the system performance, and decisions of system users who try to operate the system in an optimal way after interdictions.

The interdiction studies can be categorized in two classes: network interdiction and facility interdiction. In network interdiction, which forms the majority of interdiction studies, the effect of losing network components, like arcs and nodes, on some network models has been studied. These network models are mainly the minimum cost flow, the shortest path, and the maximum flow models. Besides modeling the interruption of flow and paths, there has been some research on modeling the effects of interdiction on the overall connectivity of the network. In this regard, Grubesic, O'Kelly, and Murray (2003) studied the loss of internet services and communication connectivity when certain internet backbone links are disrupted.

The maximum flow interdiction problem takes place on a network with designated source and sinks nodes with capacitated arcs. The objective is to find a set of flows from source to sink that obey flow balance and capacity constraints, and moves as much total flow from the source to the sink as possible. Since the user's goal is to maximize the flow, the interdictor has the goal of minimizing the user's maximum flow. The effect of interdiction on the maximum flow problem was studied in Wollmer (1964), and Wood (1993).

Wollmer (1964) represents the earliest mathematical study of an instance of network interdiction. Wollmer explores the problem of finding the most critical link, or the arc whose removal minimizes the maximum flow from the source node to the sink node, in a capacitated flow network. In this study, the interdictor can destroy exactly one arc and the user aims to maximize the flow on the remaining network.

Ratliff, Sicilia, and Lubore (1975) broadens Wollmer's (1964) basic model to the problem of finding a set of arcs in a capacitated network whose removal minimizes the maximum flow from the source node to the sink node. While investigating problems of drug interdiction, Wood (1993) generalized these models to allow for an interdiction using general resource constraints instead of cardinality constraints.

Related to Wood (1993), the network interdiction model of Washburn and Wood (1995) establishes the game between an evader, who wants to traverse paths without being detected, and an interdictor, who aims to detect the evader by placing inspection points on

some network arcs. The interaction between these two players is modeled as a two-person, zero-sum, simultaneous game (Cournot) and thus is quite different from traditional bi-level interdiction models.

More specifically, an interdictor places inspectors strategically on some arcs of a transportation network to maximize the chance of detecting the evader, who could be a drug smuggler, moving secretly on that network. If the evader traverses arc k when an inspector is present, he will be detected with the probability p_k; otherwise the evader won't be detected.

In a simultaneous game, none of the players can observe the other's actions before acting himself. Therefore, the solution for this model portrays probabilistic mixed strategies for both players. In this case, the interdictor's strategy defines a probability distribution over the inspections' locations, and the evader's strategy defines a probability distribution over different paths in the network. This is in a sharp contrast with solutions of bi-level sequential network interdiction models where deterministic pure strategies for both players will be found.

In the shortest path network interdiction, the user of the network seeks the shortest path from the source node to the sink node while the interdictor wishes to take some actions to maximize the user's shortest path cost. Interdiction in this case usually refers to eliminating arcs or increasing lengths of arcs.

In this regard, Fulkerson and Harding (1977) and Golden (1978) investigate the problem of maximizing the length of the shortest path in a network to slow enemy advancements using models in which the length of each network arc can be increased linearly within limits based on the amount of interdiction resources applied to it. In a closely related problem, Malik, Mittal, and Gupta (1989) seeks the k-most-vital-arcs in the network in which k arcs will be interdicted and interdiction decisions are binary. If an arc is attacked and it becomes destroyed its length becomes infinite, or if it is left unaffected it keeps its original length. Israeli and Wood (2002) developed the general resource constraint version of this problem.

In the minimum cost flow interdiction problem, arc costs and capacities are given together with supplies and demands at every node. The network user tries to meet all the demands while considering the capacity constraints on each arc and minimizing total costs. As long as the material is homogenous, the minimum cost flow problem will be the best way of satisfying all the demands and minimizing the total costs, whereas when materials are heterogeneous, the multi-commodity network flow problem, which considers pairs of demands of different types, is the suitable modeling framework. In either case, the interdictor attempts to disrupt the network by removing a set of arcs to maximize the minimum cost of satisfying demands. As a clear example of this type of interdiction, Lim and Smith (2007) studied the revenue maximization variant of multi-commodity network interdiction which, in the lower level, the network user maximizes the revenue by shipping commodities on the network and on the higher level the

interdictor destroys arcs to minimize the maximum revenue that the network user can make.

More recently, interdiction models have been developed for service networks composed of facilities. The first published work in the facility interdiction of service networks was that of Church, Scaparra, and Middleton (2004). They devised two basic interdiction models known as *r*-interdiction median problem (RIM) and *r*-interdiction covering problem (RIC). The objective of both of these models is to find among p existing facilities a subset of r facilities whose loss would cause the worst-case service delivery to customers.

The RIM is the direct opposite of the well known *p*-median problem. The objective of the *p*-median problem is to determine the best places of p facilities among a given number of potential places to satisfy customer demands and to minimize the demand-weighted total distance. The RIM on the other hand, seeks to maximize the demand-weighted total distance by disrupting r facilities out of p facilities when the customers of these r facilities must be reassigned to other unaffected facilities.

It should be noted that using deterministic strategies in the bi-level network interdiction may bring uncertainty elements into consideration. Cormican, Morton, and Wood (1998) developed a stochastic programming version of the maximum flow interdiction problem to examine how the interdictor can minimize the expected maximum flow when interdiction successes are not guaranteed. They also studied the situation in which arc

capacities are uncertain. Whiteman (1999) also considered uncertainty using Monte Carlo simulation of maximum flow interdiction models.

It is worth mentioning that the use of an interdiction framework does not always presume the existence of an intelligent attacker. The interdictor sub-problem is merely used as a way to estimate the worst-case situation. Therefore, this framework is also applicable to problems involving natural disasters when the impact of disruptions are severe enough to warrant a highly risk-averse decision making strategy based on minimizing the effects of the maximum possible damage.

1.2.4 Fortification Planning

A crucial issue in today's distribution and supply systems is to guarantee continuity and efficiency in service provision in the face of natural and man-made threats. If limited protective resources are available to increase system robustness, a key question is how to allocate these resources in order to preserve the functionality of the whole system as much as possible in the case of disruptions.

At first glance, it seems that the only way to prevent, or even mitigate, the negative impacts of disruptions is through the use of design models to dramatically change the initial configuration of the system. However, redesigning the entire system is not always possible due to its large expenses. Instead, methods for protecting existing systems may not only be preferable over the short term, but may also lead to more benefits over the passive design strategies in the long term. In addition, many design models are suitable

for situations when natural or accidental attacks are major concerns. Therefore, it is obvious that modeling protection strategies against intentional attacks, which are worst-case situations, is completely different since intelligent agents will try to inflict the maximum harm and may adjust their offensive strategies to circumvent initial design measures.

One of the popular techniques for infrastructure protection planning against deliberate attacks is probabilistic risk assessment (PRA) (Kumamoto & Henley, 1996) which extends the traditional risk assessment for non-deliberate attacks (like natural disasters, technological failure, and accidents) to deliberate and intentional attacks. The PRA, which is quite common among many organizations including the U.S. Department of Homeland Security, in its simplest case scores the risk associated with individual attack scenarios as *Risk=Threat*Vulnerability*Consequence*. The threat is the probability of a particular attack, vulnerability is the probability that such an attack would be successful and the consequence points to the damage incurred by a successful attack in terms of economic losses or lives lost. In order to assess these quantities, subject-matter experts must be involved. Then, a prioritized investment plan based on the risk scores will be created. The PRA, as just described, has some shortcomings.

First, it requires that event probabilities be defined as static inputs. But, the static probabilities are inappropriate for modeling behaviour of an intelligent adversary since intelligent adversaries can collect information (Mosleh, Bier & Apostolakis, 1988). Furthermore, even if PRA could measure risks correctly by static inputs, it offers no

optimized method for allocating a limited budget to minimize the risk. The method of spending down the prioritized list until a budget limit is reached is unlikely to be optimal.

Another tool for optimizing the protection planning is game theory. Game theory provides a suitable framework for modeling interaction of different players in this environment. The players can be categorized as:

- Those who want to protect their infrastructure against attacks (the network owners);
- An adversary who is likely to see the protection efforts and wants to maximize the damage (the interdictor);
- People who will see the result of interdictor's attacks and will try to use the attacked infrastructure in the best possible way (the users).

In Brown, Carlyle, Salmerón, and Wood (2005, 2006), two sorts of models to help safeguard systems were introduced: Attacker-Defender (AD), and Defender-Attacker-Defender (DAD). Attacker-Defender, as a bi-level model, reveals the critical components in the network that would be attacked. On the other hand, Defender-Attacker-Defender, as a tri-level model, portrays the best set of decisions for the Defender to hedge the network against the worst-case attacks of the interdictor. Also, they argued that when the effect of attacking a system component can be easily computed, the simpler bi-level Defender-Attacker model is capable of finding the best fortification decisions. Finally, the

authors provided examples of applying these methods in protecting the strategic petroleum reserve, patrolling the border, and the electric power grid.

Church and Scaparra (2007) add protection of critical facilities to the basic RIM model. The new model, which is called interdiction median problem with fortification (IMF), seeks to identify q facilities to be protected in a network of service facilities consisting of p facilities while r facilities are going to be interdicted. The objective of this model is to minimize the total demand-weighted shortest distance between $p-r$ non-interdicted facilities and customers. The disruptions which render r facilities inoperable try to maximize the demand satisfaction cost, thus the network planner and the interdictor have conflicting objectives. It is also assumed that the interdictor has knowledge of which facilities have been protected. Since the formulation of IMF is based on enumerating all possible combinations of attacking r facilities out of p facilities, the number of feasible solutions grows exponentially with the increase in p and r and this results in a long computational time when solving it by the CPLEX solver. Scaparra and Church (2008a) develop a new formulation, called the maximal covering problem with precedence constraints (MCPC), to solve larger instances of the IMF. The new formulation has the advantage of reducing the size of the problem and thus larger problems can be solved to optimality by the CPLEX solver.

In another paper by the same authors, a bi-level expansion of the RIM referred to as R-Interdiction Median Problem with Fortification (RIMF) is proposed. The lower level of the RIMF corresponds to the RIM described earlier in which the interdictor, as the

follower, has to solve an interdiction problem. The upper-level of the RIMF is the fortification problem of the defender, as the leader. The proposed solution technique of the RIMF performs an implicit enumeration on a search tree. The main principle of this technique is based on the observation that at least one of the facilities that would be interdicted in the worst-case interdiction, or in the solution of the lower-level RIM, must be protected. This intuitive observation is repeatedly used in order to reduce the size of the search space. Thus, larger instances of RIMF can be solved to optimality by using this search tree.

Aksen, Piyade, and Aras (2010) introduce two new aspects into the original RIMF model: general budget constraints for interdictions, as opposed to cardinality constraints, and limited but flexible capacity of facilities. Each facility has a flexible service capacity which has been determined at the outset according to the pre-attack assignment of customers. When a facility is interdicted, its customers pursue the nearest intact facility and this necessitates a capacity expansion in that facility proportional to the new demand reassigned to it. This new version is solved to optimality using an adaptation of the implicit enumeration algorithm described earlier on a binary tree.

In a later paper, Aksen, Aras, and Piyade (2013) augment their 2010 paper by adding facility location concerns. More specifically, the defender needs to simultaneously decide where to locate facilities and which facilities to protect. This paper represents the first effort in integrating location, protection, and interdiction decisions on a median-type

facility service network as a static Stackelberg (Stackelberg, 1952) game between a defender and an attacker.

In an effort to supplement the traditional network design models with the subsequent decisions of the interdictor, Smith and Lim (2007) introduced a three-level network design model. In the first level, the network designer constructs the network, while in the second level the enemy inflicts the damage to the network by reducing the capacity of some arcs. Finally, in the third level, the designer maximizes the post interdiction profit by solving a multi-commodity flow problem on the remaining network.

While the need for an all-hazard approach to incorporate the possibility of worst-case and random attacks simultaneously is raised in Zhuang and Bier (2007), more recently, the idea of inserting probability and uncertainty into traditional fortification models has become more appealing.

Liberatore, Scaparra, and Daskin (2011) studied a variant of RIMF model in which the number of attacks is unknown to the defender, and instead, the defender has access to the probability distribution of the number of facilities that could be attacked. In this case, the defender must safeguard the system against the expected number of attacks. The extension of fortification models by Zhu, Zheng, Zhang, and Cai (2013) embraces the vulnerability of protected facilities by attaching a probability of success to each protection decision of the defender. Subsequently, the impact of random attacks, the attacks when the target cannot be predicted, in the median type system of facilities, is discussed in

Zhang, Zheng, Zhu, and Cai (2014). In this case, the defender needs to preserve the system in a way that minimizes the expected cost of operating the system. Furthermore, in the same paper, the authors introduce a unified model that integrates worst-case and random attacks. Random attacks happen due to 1) misplacement or observation errors in the attacker's side in imposing intentional attacks or 2) natural disasters. In both cases of random attacks, the defender is unable to predict where the attack is going to happen. Therefore, the defender has to protect the system against both types of random and worst-case attacks.

1.2.5 Rail-Truck Intermodal Transportation

Rail-truck intermodal transportation is one of the most important parts of modern supply chains. In 2014, according to the Association of American Railroads (AAR), intermodal transportation was responsible for almost 22 percent of total revenue for major U.S. railroads surpassing the transportation of coal, which traditionally was the largest source of revenue for railroads. Also, the volume of intermodal traffic has increased dramatically from 3.1 million containers and trailers in 1980 to 13.5 million containers and trailers in 2014 (AAR, 2015).

Broadly speaking, rail-truck intermodal transportation refers to the transportation of freight from origins to destinations by a sequence of rail and truck transportations. Transfers from one mode to the other are performed at intermodal terminals.

The fundamental idea of intermodal transportation is to consolidate small loads for efficient long-haul transportation (by ocean vessels or rail), while using convenient local pick-up and delivery operations of trucks. In many cases, intermodal transportation is container-based transportation. The focus here is on rail-truck transportation of containers which has four main decision makers: drayage operator, terminal operator, network operator and intermodal operator. The drayage operator is responsible for the planning and scheduling of trucks between the terminals and shipper/receiver locations. The terminal operators take care of the terminal operations like loading, unloading and storage of containers. The network operator takes care of the infrastructure planning and formation of train services. Finally, the intermodal operator organizes the transportation of shipments on behalf of shippers by selecting the best available routes and services for each shipment (Macharis & Bentekoing, 2004).

This model of transportation is quite different from the traditional rail carload service which has been in the spotlight of the academic community in previous decades (Assad, 1980; Haghani, 1989). A fundamental aspect of carload service is that individual cars are grouped into blocks and that all the cars within the same block travel together over long distances. Such blocks are being formed in classification yards where cars are transferred from one block to another and blocks are placed on or dropped from trains.

Intermodal traffic is now carried by exclusive intermodal trains operating between intermodal terminals and bypassing classification yards entirely. The intermodal network

of major U.S. railroads is also completely distinct from their regular freight traffic network and they only share main line tracks and other related infrastructure.

Another distinction between intermodal trains and regular freight trains is emanating from the fact that in the intermodal trains, the travel of railcars, or containers, from the shipper's location to the intermodal terminal happens over the road. This is completely different from the established tradition in regular freight trains in which railcars typically travel by a local freight train on a private rail line to the origin classification yard. The reverse of this process happens at the destination yard, and thus the entire travel of railcars is by rail.

Yet another major difference between intermodal trains and traditional freight trains is that the former ones operate on a fixed schedule and are quite punctual, as opposed to the non-schedule based services of traditional freight trains.

Considering the extreme prominence of rail-truck intermodal transportation, any effort to improve efficiency, competitiveness and reliability is highly valuable. Morlok and Spasovic (1995) is one of the first papers that dealt with this issue and identified cost reduction in the highway portion of this service as an approach to increase the competitiveness of intermodal transportation. In fact, for a long time, rail-truck intermodal transportation suffered from a high cost which is mainly due to the drayage operations, thereby precluding it from capturing high volumes of freight.

A number of studies based on surveys have tried to determine the important characteristics of intermodal service from the shipper's perspective.

In this regard, Murphy and Hall (1995) have observed that reliability is the most important factor for U.S. shippers rather than the cost. More importantly, the shipper's perception of intermodal transportation is believed to have a higher impact on their decisions. In Evers, Harper, and Needham (1996), shippers decide on the mode of transportation and the specific carrier after they have formed a perception of available services. Based on this study, the main determinants of the shipper's perception are: timeliness, availability, firm contract, suitability, restitution, and cost where the first two factors are the most important ingredients of the perception.

In another study, Harper and Evers (1993) have found acceptability of rail-truck intermodal transportation as the most important determinant of the extent to which it can be regarded as a viable alternative to the traditional truck-based transportation. Based on this study, acceptability itself depends on the availability, quality and price of this service.

The ability of rail-truck transportation to resist against the loss of its infrastructures, which can decrease the need for drayage operations and can increase availability and quality of this service, is clearly absent in these studies. More specifically, the idea of identifying critical components (like terminals and links) and then preparing appropriate plans to protect them against disruptions has not been addressed so far. Obviously, one of the most important decisions for network owners is to invest in fortification of their assets

and this kind of decision also deeply influences the downstream decisions of the intermodal operator who tries to select the best combination of rail/truck services to meet the demands with the minimum cost. Therefore, integrating decisions of the network operator and the intermodal operator will fill this gap.

1.3 Conclusion

In this literature review, the body of research regarding disruption planning in supply chains has been reviewed. Important planning efforts, like network design and interdiction models, have been examined. Based on this review, the issue of disruption planning in rail-truck intermodal transportation lacks proper attention and therefore needs to be investigated in future research studies. Regarding the high importance of rail-truck intermodal transportation, operations research specialists have to take initiatives to analytically address these issues and fill the research gap.

The body of research in the rest of the thesis is classified into four chapters, which study four different developments of the original research question presented in Chapter One. In this regard, Chapter Two, Chapter Three, Chapter Four, and Chapter Five gradually develop and generate my research contributions where each chapter uses the results and improvements of earlier chapters. Lastly, Chapter Six reiterates research findings of the thesis and outlines a number of suggestions for the future research. Figure 1-2 outlines the organization of this thesis and the content of each chapter.

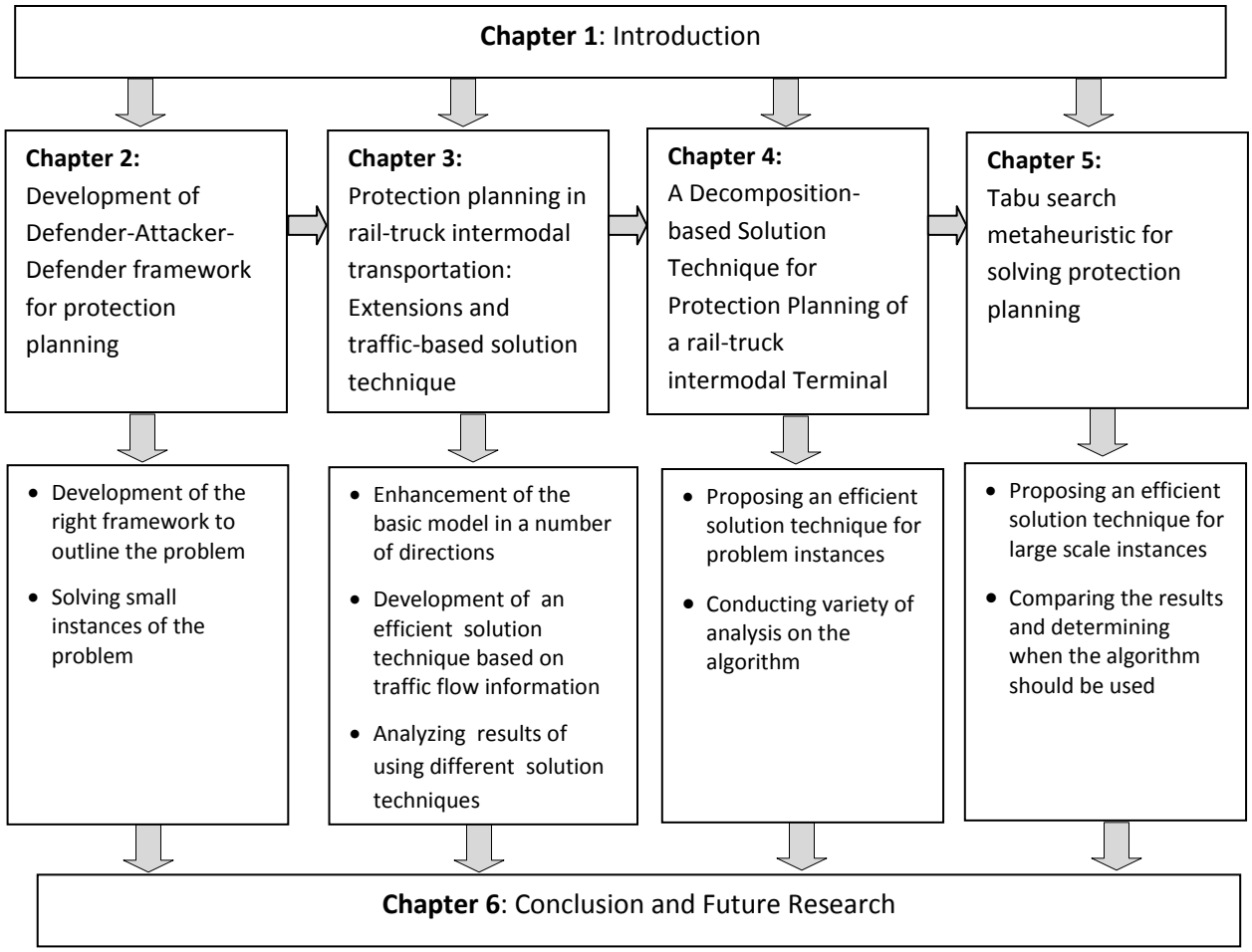

Figure 1-2: Structure of the thesis

1.4 Motivation and Objectives

Considering the utmost importance of rail-truck intermodal transportation, it is necessary to evaluate the vulnerability of this type of transportation against worst-case disruptions carefully. Also, proper plans should be provided to reduced such a vulnerability and improve the overall performance of the system in the wake of disruptions. Therefore, within this research, I endeavor to provide a proper analytical framework and efficient

solution techniques to address vulnerability assessment and fortification planning in the rail-truck intermodal transportation domain.

1.5 Co-authorship Statement

I, Hassan Sarhadi, hold a principal author status for all the manuscript chapters (Chapters Two, Three, Four, Five, and Six) in my thesis. However, each of the manuscripts is co-authored by my supervisors, Dr. Manish Verma and Dr. David Tulett, whose contributions have expedited the progress of developing the ideas, conducting computational experiments, and the manuscript writing.

Summary of Contributions of Chapter Two

Presentations and Publications:

- Presented at TRANSLOG 2014, Burlington, Canada.

Output:

- Formulation of a mathematical model for Defender-Attacker-Defender problem in the rail-truck intermodal transportation.
- Solving small-scale instances of the DAD problem using the CPLEX solver.

Chapter 2: A Defender-Attacker-Defender Framework to the Optimal Fortification of a Rail-Truck Intermodal Terminal Network

2.1 Introduction

Critical infrastructure plays a pivotal role in the wellbeing of each economy. Regarding their unique importance, a crucial issue in modern supply chains is to guarantee continuity and efficiency in the event of natural and man-made threats. Such a task is challenging, especially given the finite resources and the complexity of the transportation infrastructure.

In this chapter, we make use of the Defender-Attacker-Defender framework to uncover the optimal strategy for fortifying a given number of rail-truck intermodal terminals, such that the losses resulting from worst-case attacks are kept at their minimum level.

The proposed tri-level optimization model then is applied to a realistic-size case study and is solved using CPLEX. Finally, the results reveal some managerial insights and directions for future research.

2.2 Problem Description

In this section, we provide a formal statement of the problem, emphasize its complexity, and then state the modeling assumptions.

The rail-truck intermodal transportation fortification problem entails hierarchical and sequential decisions amongst three players, i.e., the network operator, the interdictor, and

the intermodal operator (Figure 2-1). Based on the classification presented in Macharis and Bontekoning (2004), the network operator is the owner of the railway infrastructure of the intermodal infrastructure such as terminals, tracks, and locomotives. At the highest level, the network operator attempts to minimize the cost of the worst-case disruption by fortifying a limited number of intermodal terminals. Note that this is possible only if the owner knows the cost of the worst-case attack by the interdictor, and hence the latter's problem is a part of the former's. Next, in the middle level, the interdictor wants to maximize the minimum cost of using the system by attacking a limited number of (unprotected) terminals, which is achieved by having complete information about the intermodal operator's problem. Finally, following the interdiction, the intermodal operator makes the best use of available resources on the reduced intermodal network (and possibly fewer train services) to meet customer demand at the minimum cost. Thus, the indicated interaction amongst the three players can be cast as a tri-level fortification planning problem using the Defender-Attacker-Defender (DAD) framework.

It is important to consider the different types of decisions that these three players are making. At the highest level, the network operator needs to decide which terminals to protect. In the middle level, the attacker decides on what terminals to attack. Finally, in the lowest level, the intermodal operator aims to find the best load plan to serve all the customers which requires finding the best path for each shipper-receiver pair, and also the frequencies of train services to satisfy all the demands with the lowest cost.

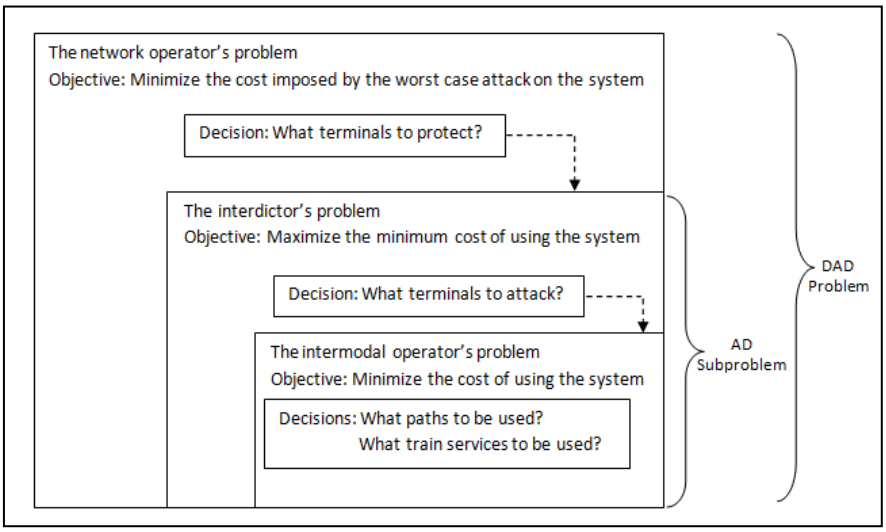

Figure 2-1: Hierarchical structure of the fortification planning

To have a better understanding of how a rail-truck intermodal transportation system works, it should be noted that this type of transportation comprises three distinct processes:

- Inbound drayage, i.e., trucking service from the shipper location to the origin intermodal terminal
- rail-haul between the intermodal terminals
- Outbound drayage, i.e., trucking service from the destination intermodal terminal to the receiver location.

A shipment that needs to be transported from the shipper's location to the receiver's location, first travels by trucks from the shipper's location to the origin intermodal terminal. In the terminal, it will be transshipped from trucks to train and the train is responsible for terminal to terminal journey of the shipment. In the destination terminal, it

will be transshipped from train to trucks and finally, trucks are responsible for final delivery of the shipment to receiver's location. Figure 2-2 shows this process.

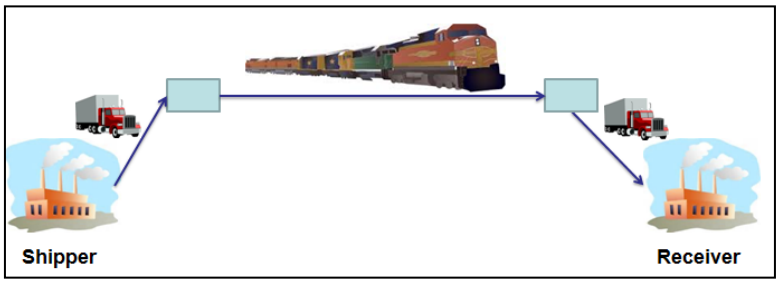

Figure 2-2: A Depiction of Rail-Truck Intermodal Transportation

The intermodal operator focuses on the entire routing of the shipments, and endeavors to find the minimum-cost way to satisfy customer demand, given the available connections between the intermodal terminals and shippers/ receivers, and also the existing pre-defined intermodal train services.

It is also important to note that this sort of nested interaction among the players, which aims to find the best fortification decision to preserve the functionality of the intermodal infrastructure in the aftermath of disruption, makes the problem fairly complex.

2.3 Defender-Attacker-Defender Framework

In this section, we provide a tri-level mathematical formulation for the fortification problem described earlier.

First, different components of the mathematical formulation, like assumptions, sets, parameters and decision variables, need to be defined and then the entire model is demonstrated.

2.4 Mathematical Model

2.4.1 Assumptions

- The demand has been defined for each shipper-receiver pair and is assumed to be fixed during the planning period.

- The locations of terminals, shippers and receivers are assumed to be known. Therefore, the distances between any two of them (the length of the line connecting them) can be calculated.

- The set of train services has been defined on the physical network and will be considered as an input to the model. The frequency of each service will be decided by solving the network operator's problem.

- It is assumed that terminals and rail links have enough capacity to handle the traffic and also it is assumed that there are always enough empty containers in origin terminals.

- It is assumed that if either the origin or the destination terminal of a given train service becomes interdicted, the train service would not be able to operate.

- It is assumed that if a given terminal becomes interdicted, the remaining terminals have enough capacity to make up for that.

- Direct trucking is allowed between each shipper-receiver pair to keep the intermodal operator's problem always feasible. Due to its high cost, this type of direct shipment normally won't be used when there is no attack to the system.

- It is assumed that a protected terminal cannot be interdicted.
- It is assumed that there is no congestion at the terminals.
- It is assumed that if intermediate terminals associated with an intermodal train service are interdicted, the train can still serve the remaining terminals on its route by bypassing those interdicted terminals.

2.4.2 Sets

I: Set of shippers indexed by i ($i \in I$)

L: Set of receivers indexed by l ($l \in L$)

J: Set of origin intermodal terminals which is the set of origin terminals for all shipper-receiver pairs and is indexed by j ($j \in J$)

K: Set of destination intermodal terminals which is the set of destination terminals for all shipper-receiver pairs and is indexed by k ($k \in K$)

V: Set of train services defined on the physical network and is indexed by $(v \in V)$. Each service is characterized by its origin terminal, destination terminal, intermediate stops (for loading/unloading operations), and its capacity which is the number of containers that each train of that service can take.

v_{jk}: Set of train services ($v_{jk} \subseteq V$) connecting terminal j ($j \in J$) to terminal k ($k \in K$).

R^v: The set of all service legs for a given train service $v \in V$ indexed by r. Each service leg of service $v \in V$ is defined as the rail link between any two consecutive stops of v. Therefore, the definition of service leg completely depends on the definition of service and the terminals at which it will stop. Let's take a look at Figure 2-3 to define this set. Suppose that train service v (depicted by the dashed line) travels from T_1 (origin) to T_5 (final destination) and has two intermediate stops at T_2 and T_3while bypassing T_4. In this case, the rail segment between T_1 and T_2, the rail segment between T_2 to T_3 and the rail segment between T_3 and T_5 are three service legs of this train service and therefore the set R^v is: $\{\{T_1T_2\}, \{T_2T_3\}, \{T_3T_5\}\}$.

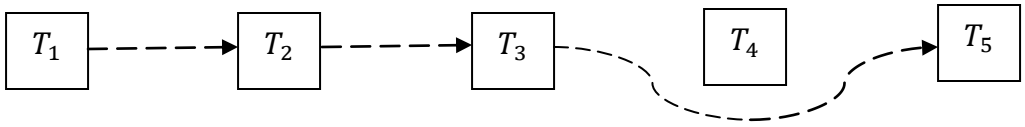

Figure 2-3. Train Service V defined on the network

$S^{r,v}$: The set of pairs of terminals, covered by train service $v \in V$, for which traveling between them entails using the service leg $r \in R^v$. Based on Figure 2-3, traveling from T_1 to T_2 needs to use the first leg, i.e. the leg $\{T_1T_2\}$. In addition to that, traveling from T_1 to T_3 and traveling from T_1 to T_5 also require using the first leg.

B^v: Set of origin and destination terminals of train service $v \in V$.

N: Set of all terminals in the physical network.

2.4.3 Parameters

$D_{i,l}$: The fixed demand between shipper $i \in I$ and receiver $l \in L$ during the planning horizon.

Fc^v: The fixed cost of forming train service $v \in V$ between its origin terminal and its destination terminal.

$c_{i,j}$: Inbound drayage cost or the cost of sending a container using a truck from the shipper $i \in I$ to the origin terminal j ($j \in J$).

$ct_{i,l}$: The cost of directly sending a container using a truck from the shipper $i \in I$ to the receiver l ($l \in L$).

$c'_{k,l}$: Outbound drayage cost or the cost of sending a container using a truck from the destination terminal k ($k \in K$) to the receiver $l \in L$.

$c^v_{j,k}$: Train service cost or the cost of sending a container with train service v ($v \in V$) from origin terminal j ($j \in J$) to the destination terminal k ($k \in K$) when service v passes between j and k, or simply $v \subseteq v_{jk}$.

α^v: The capacity of the train service $v \in V$.

w: The maximum number of terminals that the network owner can protect.

r: The maximum number of terminals that the interdictor can destroy.

2.4.4. Intermodal Operator's Decision Variables

$x_{i,j,l}$: Number of containers from shipper $i \in I$ to receiver $l \in L$ that use terminal $j \in J$ as their origin terminal.

$x'_{i,k,l}$: Number of containers from shipper $i \in I$ to receiver $l \in L$ that use terminal $k \in K$ as their destination terminal.

$x^{v}_{i,j,k,l}$: Number of containers from shipper $i \in I$ to receiver $l \in L$ that use intermodal train service $v \in V$ to travel from terminal $j \in J$ to terminal $k \in K$ when v passes between j and k, or $v \subseteq v_{jk}$.

$xt_{i,l}$: Number of containers from shipper $i \in I$ to receiver $l \in L$ which use direct trucking service.

n^{v}: Number of trains of service type $v \in V$ during the planning horizon (the frequency of the service type v).

2.4.5 Network Operator's Decision Variable

z_y: Reflects the protection of terminal y ($y \in N$) if z_y=1

2.4.6 Interdictor's Decision Variable

t_y: Indicates the interdiction of terminal y ($y \in N$) if t_y=1

2.4.7 Mathematical Formulation

$Min_z C(z)$

Subject to:

$$\sum_y z_y \leq w, \forall y \in N \quad (1)$$

$$z_y \in \{0,1\}, \forall y \in N \quad (2)$$

$$C(z) = Max_t\, C(t) \quad (3)$$

Subject to:

$$\sum_y t_y \leq r, \forall y \in N \quad (4)$$

$$t_y \in \{0,1\}, \forall y \in N \quad (5)$$

$$t_y + z_y \leq 1\,, \forall y \in N \quad (6)$$

$$C(t) = Min\left[\sum_{i\in I}\sum_{j\in J}\sum_{l\in L} c_{i,j}\, x_{i,j,l} + \sum_{i\in I}\sum_{k\in K}\sum_{l\in L} c'_{k,l}\, x'_{i,k,l} + \sum_{i\in I}\sum_{l\in L} ct_{i,l} xt_{i,l} + \sum_{i\in I}\sum_{j\in J}\sum_{v\in v_{jk}}\sum_{k\in K}\sum_{l\in L} c^v_{j,k} x^v_{i,j,k,l} + \sum_{v\in V} Fc^v n^v\right] \quad (7)$$

Subject to:

$$x_{i,j,l} = \sum_{v\in v_{jk}}\sum_{k\in K} x^v_{i,j,k,l} \qquad \forall i \in I, \forall j \in J, \forall l \in L \quad (8)$$

$$\sum_{v\in v_{jk}}\sum_{j\in J} x^v_{i,j,k,l} = x'_{i,k,l} \qquad \forall i \in I\,, \forall k \in K, \forall l \in L \quad (9)$$

$$\sum_{k\in K} x'_{i,k,l} + \sum_{i\in I}\sum_{l\in L} xt_{i,l} = D_{i,l} \qquad \forall i \in I\,, \forall l \in L \quad (10)$$

$$\sum_{i\in I}\sum_{(j,k)\in S^{r,v}}\sum_{l\in L} x^v_{i,j,k,l} \leq \alpha^v n^v \qquad \forall v \in V, \forall r \in R^v \quad (11)$$

$$n^v + t_y \leq 1 \qquad \forall v \in V, y \in B^v \quad (12)$$

$$n^v \geq 0, integer \qquad \forall v \in V \quad (13)$$

$$x_{i,j,l} \geq 0, integer \qquad \forall i \in I\,, j \in J, \forall l \in L \quad (14)$$

$$x'_{i,k,l} \geq 0, integer \qquad \forall i \in I\,, k \in K, \forall l \in L \quad (15)$$

$$x_{i,j,k,l}^{v} \geq 0, integer \qquad \forall i \in I\ , \forall v \in V \cap v_{jk}\ , \forall l \in L, \forall j \in J, \forall k \in K \qquad (16)$$

$$xt_{i,l} \geq 0, integer \qquad \forall i \in I, \forall l \in L \qquad (17)$$

2.4.8 Explanation of the Constraints

The objective function of the network operator's problem, the outer problem, tries to minimize the total cost. In order to do that, the network operator has to decide which terminals to fortify and this is done by the first constraint in which a limited number of terminals will be protected. Based on the second constraint, the decision to protect a given terminal is a binary decision. The third constraint of the network operator's problem is referring to the whole of the interdictor's problem. Based on this constraint, the interdictor wants to maximize the cost of using the system. Within the network interdictor's problem, the fourth constraint refers to the interdiction of some terminals among all terminals, by the interdictor. Based on this constraint, the interdictor has a limited budget to interdict a limited number of terminals in the network. The fifth constraint points to the binary nature of the interdictor's decision. The sixth constraint connects the decisions of the network operator and the decisions of the interdictor. According to this constraint, a protected terminal cannot be interdicted by the interdictor. The seventh constraint refers to the whole intermodal operator's problem. Based on this, the network operator tries to minimize the overall cost of using the system. The objective function of the intermodal operator's problem is minimization of the cost of using the drayage paths and the rail services. The overall cost of using the system can be divided into two parts; the variable cost and the fixed cost.

The first three terms of the objective function of the network operator refer to the variable cost, i.e. the cost of which is proportional to the number of containers being sent from a given shipper to a given receiver. Therefore, the first three terms of the objective function calculate the total variable cost over all of the shipper-receiver pairs. The cost of sending a container by a truck mainly reflects the operations required to load, unload and transfer the container as well as driver hours in the drayage path. The inbound drayage cost is the cost proportional to driver hours from the shipper's location to its origin terminal while the outbound drayage cost reflects the driver's cost from the destination terminal to the receiver's location. Also, the cost of sending a container directly from its shipper to its receiver reflects the driver's cost from the shipper to the receiver. The variable rail service cost points to the cost associated with loading/unloading of a container from its origin terminal to its destination terminal.

The fourth set of terms in the objective function denotes the fixed cost of forming train services of different types. The fixed cost of forming a train service reflects the cost of using human resources in the railway company (brakeman, engineer, and driver) and the cost of using the locomotive itself. This cost does not directly depend on the number of containers assigned to that service since for any number of containers (up to the train capacity) the same resources will be required.

Within the operator's problem, the eighth set of constraints points to the conservation of flow between a given origin terminal and all of destination terminals (those which are accessible from that origin terminal by different train services). In other words, the

containers that have been received by a given origin terminal will be transferred to all accessible destination terminals.

The ninth set of constraints is similar to the eighth set since it points to the conservation of flow in destination terminals. In other words, the containers that have been transferred to a given destination terminal have came from different origin terminals using available train services between them. Therefore, each destination terminal will send out completely what it has received from the origin terminals and nothing will be lost.

The tenth set of constraints states that demand must be satisfied for all shipper-receiver pairs. Therefore, the containers that have been transferred to a given receiver from different destination terminals have to be equal to the demand of the associated shipper-receiver pair.

The eleventh set of constraints calculates the frequency (the number of trains) of each train service. More precisely, the total number of containers that each train service can take during the planning horizon (the right hand side of the constraint) must be greater or equal to the total number of containers (from different shipper-receiver pairs) being transported on each of its service legs (the left hand side).

The twelfth set of constraint connects the interdictor's decision and the intermodal operator's decision in such a way that if a given terminal becomes interdicted by the interdictor, then none of the services originating or ending at that terminal can be used anymore by the network operator. Finally, the remaining sets of constraints (13, 14, 15,

and 16) are pointing to the integrality and non-negativity of network operator's decisions (frequency and traffic assignment variables).

2.5 Introducing a Realistic Case Study

In an effort to explain the complexity of the problem, we reproduce a portion of the intermodal service chain network introduced by Verma, Verter, and Zufferey (2012), which is represented via a geographical information system (GIS) model using ArcView (ESRI, 2008). All resulting mathematical models were solved using CPLEX 12.6.0 (IBM, 2014). Figure 2-4 and Figure 2-5 respectively depict 18 intermodal terminals and 37 customers in the network, which are the access points for 399 demand pairs (i.e., shipper-receiver pairs). A total of 62 types of intermodal train services differentiated by route, speed and intermediate stops are connecting these terminals. Among train services 31 services are of *regular* type and have been shown in Appendix A, and another 31 services are *express* services and are 25% faster. Finally, the network operator has resources to fortify a limited number of terminals, the interdictor has resources to destroy/ disrupt a limited number of (un-protected) terminals, and the network operator has to meet demand using the reduced intermodal network.

Terminals	Legend	Terminals	Legend	Terminals	Legend
Atlanta	*Atl*	Charlotte	*Cha*	Chicago	*Chi*
Cleveland	*Cle*	Cincinnati	*Cin*	Columbus	*Col*
Detroit	*Det*	Fort Wayne	*For*	Indianapolis	*Ind*
Jacksonville	*Jac*	Knoxville	*Kno*	Macon	*Mac*
New York	*NY*	Norfolk	*Nor*	Philadelphia	*Phi*
Pittsburgh	*Pit*	Richmond	*Ric*	Roanoke	*Roa*

Table 2-1: Terminal Legends

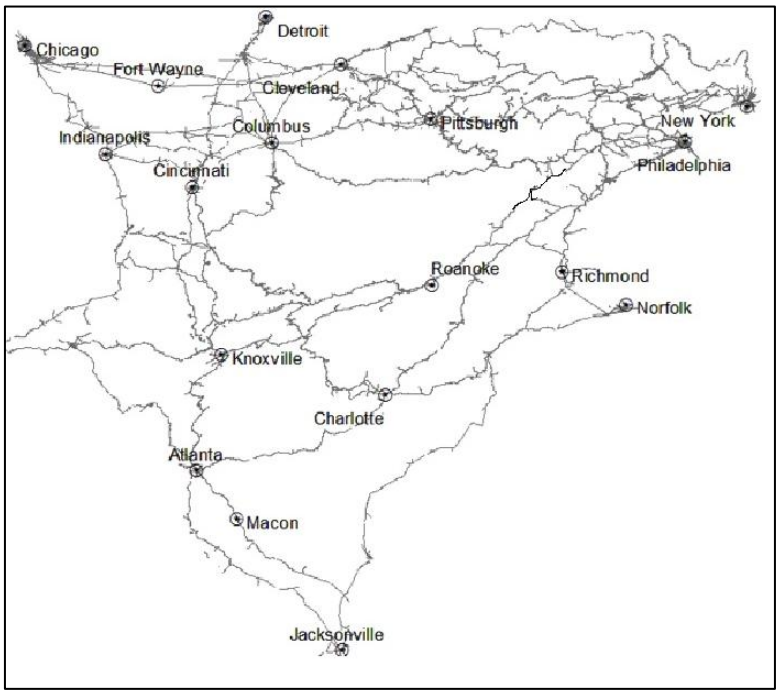

Figure 2-4: Location of 18 Terminals (Adapted from: Verma & Verter, 2010)

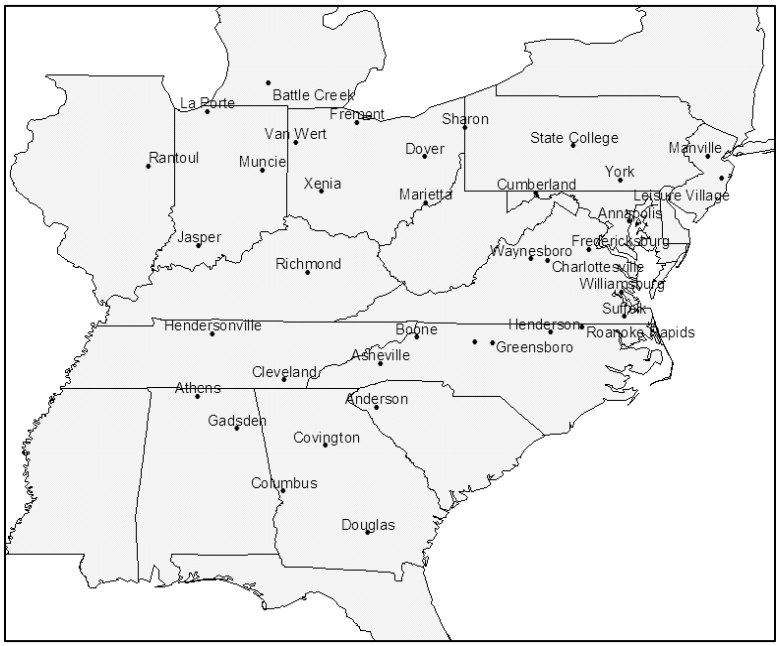

Figure 2-5: Location of 37 Customers (Adapted from: Verma & Verter, 2010)

2.5.1 Estimation of Parameters

Cost: In the United States, trucks can travel at a maximum speed of 50 miles/hour, but due to lights and traffic an average speed of 40 miles/hour is assumed (Verma & Verter, 2010). Normally drayage is charged in terms of the amount of time the crew (driver-truck) is engaged, and an estimate of 300USD/hour including the estimated hourly fuel cost is used. As indicated there are two types of intermodal train services viz. *regular* and *express*. Average intermodal train speed was calculated using the Railroad Performance Measure website (RPM, 2014), and was estimated to be 27.7 miles/ hour for *regular*, and 36.8 miles/hour for *express* service. Consistent with the published works, we estimated a rate of 0.875 USD per mile for *regular* and 1.164 USD per mile for *express* service. The hourly fixed cost of running a *regular* intermodal train is 500 USD per hour, which takes into consideration the hourly rates for a driver, an engineer, a brakeman, and an engine, which are 100 USD, 100 USD, 100 USD, and 200 USD, respectively. The *express* service is 50% more expensive at 750 USD per hour (Verma et al. 2012).

2.6 Numerical Analysis

In the first part of this section, the network operator (the Defender) has enough money to protect one terminal and the interdictor (the Attacker) has enough resources to disrupt one terminal while in the second part both of them have enough money to fortify/disrupt two terminals.

2.6.1 Part One: the Network Operator and the Interdictor Can Protect/Disrupt One Terminal

In this part of the numerical analysis, the network owner has eighteen different strategies of protecting terminals (given in the form of tables) and each strategy is then followed by seventeen possible attack strategies of the interdictor. After each attack strategy, the network operator tries to meet as many demands as possible with the least cost. Appendix B summarizes the results of attacking different terminals.

To show a typical interaction between the network owner and the interdictor, Table 2-2 , which is derived from Appendix B, describes the situation when the network operator (the first player) protects the terminal located in Atlanta and the interdictor (the second player), who knows the first player's decision, tries to interdict a terminal among the remaining unprotected terminals. For each combination of the first two players' decisions, the third player (the intermodal operator) decides to find the best set of services to satisfy demands with the least cost.

Defended Terminal	Attacked Terminal	Cost Imposed ($)	Computation Time (Sec)	Cost Saving ($)
Atl	Phi	12,263,378	221.4	378,200

Table 2-2: Results of defending/attacking 1 terminal

According to Table 2-2, the cost associated with defending Atlanta is 12.26 million dollars. This is in fact the maximum cost that the interdictor can impose to the system, by attacking the terminal located in Philadelphia, following the protection of the terminal

located in Atlanta. The cost saving of defending the terminal at Atlanta, and instead leaving Philadelphia unprotected, amounts to 378,200 dollars.

2.6.2 Part Two: the Network Operator and the Interdictor Can Protect/Disrupt Two Terminals

In this part of the numerical analysis, the network owner has 153 different strategies of protecting terminals (given in the form of tables) and each strategy is then followed by 136 possible attack strategies of the interdictor. After each attack strategy, the network operator tries to meet as many demands as possible with the least cost. Appendix C summarizes the results of attacking different pairs of terminals by the interdictor.

Defended Terminals	Attacked Terminals	Cost Imposed ($)	Computation Time (Sec)	Cost Saving ($)
NY, Atl	Chi, Ind	13,016,982	1,513	889,593

Table 2-3: Results of defending/attacking 2 terminals

According to Table 2-3, which is extracted from Appendix C, the best protection decision is to protect terminals located in New York and Atlanta and this decision results in the total cost of 13.01 million dollars. This is in fact the maximum cost that the interdictor can impose on the system, by attacking terminals located in Chicago and Indiana, following the protection of terminals located in New York and Atlanta. The cost saving of this protection decision is nearly 900,000 dollars which shows the extent to which suitable fortification planning can reduce the costs imposed on the system. Also, it is interesting to see that the cost saving in the case where two terminals are being protected/interdicted is much higher than the case in which one terminal is being

protected/interdicted. This clearly shows that the cost saving of fortification increases with the increase in the budget of attacker and defender.

2.7 Conclusion

In this chapter, a framework for defending rail-truck intermodal transportation is introduced. Then, a mathematical model that can capture the decisions of the players and their interactions has been proposed.

Also, a real case study of the intermodal chain of a railway company in the U.S. has been presented. Then, the mathematical model of the Defender-Attacker-Defender problem has been solved for the case study to find out the best decisions to protect the infrastructure. Due to the complexity of the problem, only two instances of the DAD model have been solved; the instances in which one terminal is going to be defended/attacked and the instance in which two terminals are going to be defended/attacked.

The results of applying the fortification planning to the case study reveal huge improvements in the cost of running the system in the aftermath of interdictions. In other words, after the occurrence of interdictions, the system which has a suitable fortification plan is able to satisfy demands with lower cost compared to the systems which are left unprotected.

The current model can be enhanced in a number of aspects. For example, these days, many customers are sensitive to the delivery time of their shipments and transportation

companies should take any action to deliver shipments on time. Adding such new aspects makes the model more realistic and more applicable for practical situations.

In terms of solving the model, the proposed DAD model is very difficult. Therefore, efficient solution techniques need to be developed to solve large instances of the DAD problem efficiently. All these new aspects will be pursued in the next chapter.

Summary of Contributions of Chapter Three

Presentations and Publications:

- Accepted for presentation at CORS 2014, Ottawa, Canada.
- Accepted for publication in the *Journal of Transportation Security*. DOI: 10.1007/s12198-014-0152-4.

Output:

- An efficient traffic-based heuristic solution technique for solving small instances of the DAD problem.

Chapter 3: Protection Planning of a Rail-Truck intermodal Terminal Network: Extensions and Traffic-based Solution Technique

3.1 Introduction

In this chapter, the tri-level defender-attacker-defender (DAD) approach proposed in Chapter Two will be enhanced in a number of directions so that it better fits to realistic situations. In addition to modeling enhancements, a new solution technique based on the traffic flow information is proposed that is able to solve this problem in an efficient manner. The proposed DAD will be applied to the realistic case study introduced in Chapter Two and then it will be solved by the developed solution technique. At the end, a variety of analyses has been done on the results to scrutinize the effects of fortification planning on the performance of the system.

3.2 Problem Description

In this section, the DAD model described in Chapter Two will be expanded in a number of directions. It is important to mention that two pertinent factors should be considered in making the routing decisions. *First*, since each intermodal terminal has a finite capacity, an interdiction may result in a situation where the remaining terminals in the network do not have enough capacity to meet demand. *Second*, punctuality is the mainstay of intermodal shipments (Nozick & Morlok, 1997; Verma et al, 2012), and hence late deliveries should be penalized as a function of the time delayed. Also, like the mathematical model presented in Chapter Two, direct trucking is permitted between each

shipper-receiver to ensure feasible solutions in the intermodal operator's problem. From the mathematical programming point of view, a path-based modeling approach has been selected. In this approach, a set of possible intermodal paths for a given shipper-receiver pair is identified in the pre-processing phase. Then, a single variable is attached to each path. Adopting the path based approach results in fewer variables in the intermodal operator's problem and this will facilitate solving this problem. Therefore, instead of attaching three variables to each intermodal path between a given shipper and a given receiver, only one variable will be used.

3.3 Assumptions

- The demand has been defined for each shipper-receiver pair and is assumed to be fixed during the planning period;
- The locations of terminals, shippers and receivers are assumed to be known. Therefore, the distances between any two of them can be calculated;
- The set of train services has been defined on the physical network and will be considered as an input to the model. The frequency of services will be decided by solving the network operator's problem;
- Rail links have enough capacity to handle the traffic and also it is assumed that there are always enough empty containers in origin terminals;

- If either the origin or the destination terminal of a given train service become interdicted, the train service would not be able to operate;
- If intermediate terminal associated with an intermodal train service is interdicted, the train can still serve the remaining terminals on its route;
- A protected terminal cannot be interdicted;
- It is assumed that that the waiting time to receive the handling operations is insignificant and thus there is no congestion at the terminals;
- Each terminal has finite traffic handling capacity, thus the remaining terminals in the network may not have enough capacity to make up for the capacity of interdicted terminals;
- Delivery dates are specified when placing the order, and a penalty cost per container per hour is incurred for late deliveries;

3.4 Path-based Defender-Attacker-Defender Framework

In this section, we develop a tri-level mathematical formulation for the fortification problem introduced in the previous chapter, and then propose two distinct solution techniques for solving it.

3.4.1 Mathematical Model

Our notation and the model are provided below.

Sets

I Set of shippers, indexed by i

J Set of receivers, indexed by j

P_{ij} Set of intermodal paths between shipper i and receiver j, indexed by p

K Set of intermodal terminals in the network, indexed by k

P_{ij}^{k} Set of intermodal paths between shipper i and receiver j which uses intermodal terminal k as either origin or destination.

V Set of intermodal train services defined on the network, indexed by v

L^{v} Set of service legs for train service v, indexed by l

$S^{l,v}$ Set of intermodal paths using service leg l of train service v

Variables

X_{ij}^{p} Number of containers using intermodal path p between shipper i and receiver j

XT_{ij} Number of containers using direct trucking service between shipper i and receiver j

N^{v} Number of train services of type v

$z_k = \begin{cases} 1 \text{ if terminal } k \text{ is protected} \\ 0 \quad \text{otherwise} \end{cases}$

$y_k = \begin{cases} 1 \text{ if terminal } k \text{ is interdicted} \\ 0 \quad \text{otherwise} \end{cases}$

Parameters

W Maximum number of terminals that the network owner can protect

R Maximum number of terminals that the interdictor can disrupt

C_{ij}^{p} Cost of transporting a container from shipper *i* to receiver *j* on intermodal path *p*

CT_{ij} Cost of sending a container using trucks on the shortest path from shipper *i* to receiver *j*

T_{ij}^{p} Expected travel time from shipper *i* to receiver *j* on intermodal path *p*

T_{ij} Delivery time using truck on the shortest path from shipper *i* to receiver *j*

$\bar{T}_{ij}$ Delivery due date promised by shipper *i* to receiver *j*

D_{ij} Number of containers demanded by receiver *j* from shipper *i*

PC_{ij} Penalty cost per container per hour between shipper *i* and receiver *j*

α^{v} Capacity of train service *v*

FC^{v} Fixed cost of operating train service *v*

U_{k} Capacity of intermodal terminal *k*

(P)

$$Min_{z} C(z) \tag{1}$$

subject to:

$$\sum_{k \in K} z_{k} \leq W \tag{2}$$

$$z_{k} \in \{0,1\} \qquad \forall k \in K \tag{3}$$

where,

$$C(z) = Max_{y} C(y) \tag{4}$$

subject to:

$$\sum_{k\in K} y_k \le R \tag{5}$$

$$y_k \in \{0,1\} \qquad \forall k \in K \tag{6}$$

$$y_k + z_k \le 1 \qquad \forall k \in K \tag{7}$$

where,

$$C(y) = Min(\sum_{i\in I}\sum_{j\in J}\sum_{\substack{p\in P_{ij} \\ T_{ij}^p > \bar{T}_{ij}}} \left(T_{ij}^p - \bar{T}_{ij}\right) PC_{ij} X_{ij}^p + \sum_{i\in I}\sum_{\substack{j\in J \\ T_{ij} > \bar{T}_{ij}}} \left(T_{ij} - \bar{T}_{ij}\right) PC_{ij} XT_{ij} + \sum_{v\in V} FC^v N^v \ ) \tag{8}$$

subject to:

$$\sum_{p\in P_{ij}} X_{ij}^p + XT_{ij} \ge D_{ij} \qquad \forall i \in I, \forall j \in J \tag{9}$$

$$\sum_{i\in I}\sum_{j\in J}\sum_{p\in P_{ij}\cap P_{ij}^k} X_{ij}^p \le U_k(1 - y_k) \qquad \forall k \in K \tag{10}$$

$$\sum_{i\in I}\sum_{j\in J}\sum_{p\in P_{ij}\cap S^{l,v}} X_{ij}^p \le \alpha^v N^v \qquad \forall v \in V, l \in L^v \tag{11}$$

$$N^v \ge 0, integer \qquad \forall v \in V \tag{12}$$

$$X_{ij}^p \ge 0, integer \qquad \forall i \in I, \forall j \in J, \forall p \in P_{ij} \tag{13}$$

$$XT_{ij} \ge 0, integer \qquad \forall i \in I, \forall j \in J \tag{14}$$

(P) depicts the tri-level optimization model that will be used to make protection planning decisions. It should be mentioned that $C(.)$is a multi-variable function of z and y such that, in each level of the problem, only one of these variables is considered and thus $C(.)$ reduces to a single-variable function. The *outer* level problem belongs to the network operator whose objective is to minimize total cost in the aftermath of disruptions by

fortifying a given number of intermodal terminals. Constraint set (3) enforces the binary nature of the terminal fortification decision. The *middle* level problem belongs to the interdictor who intends to maximize the total cost of using the system. Constraints set (5) depicts the finite resources available for interdiction or disruption of intermodal terminals, whereas (6) represents the binary nature of the interdiction decisions. Constraint set (7) combines the decisions of the network operator and the interdictor by prohibiting the disruption of fortified terminals. Finally, the *inner* level problem belongs to the network operator who intends to minimize the total cost of using the system. Note that this is a variant of the multi-commodity flow problem with capacity, delivery time, and penalty cost considerations. The objective function, i.e., (8), will capture the overall cost of moving shipments using rail-truck intermodal paths, any direct trucking service if applicable, the penalty costs for late deliveries, and the fixed cost of running different intermodal trains in the network. Constraint set (9) ensures the demand is satisfied either using the intermodal option or through the direct truck service. Constraint set (10) enforces the capacity at various terminals in the network, and that the interdicted terminals cannot be either origin or destination of intermodal paths to meet the demand. Constraint set (11) determines the number of intermodal trains of a specific type needed in the network. Finally, the sign and integrality restrictions are imposed through constraints set (12) to (14).

3.5 Numerical Analysis

3.5.1 Parameter Estimation:

Due Dates: Three different due dates have been defined: *long*, *regular*, and *short*. The distance (*d* in miles) between each shipper and each receiver was estimated in ArcView GIS (ESRI, 2008). Next, the travel time (in hours) was computed as *d/40*, where the denominator indicates the speed of trucks. Finally, constants of 10, 15 and 20 were added to the travel time to obtain, respectively, the s*hort*, *regular* and *long* delivery due dates for each shipper-receiver pair. The penalty cost is set at 40 dollars per container per hour of lateness. Also, the cost of running train services follows the calculations of the previous chapter.

Demand Levels and Terminal Capacity: The inner problem belonging to the intermodal operator was solved in CPLEX 12.1.0 (IBM, 2014) on the dataset used in Verma et al. (2012), and the solution was decoded to estimate the traffic volume through each intermodal terminal. It was assumed that the terminal utilization was 80%, and hence the terminal capacity is 1.25 times (i.e., 1 divided by 0.8) the traffic volume through each terminal, and the demand level was deemed *medium*. Finally, we assumed that *high* demand level would account for 95% of terminal capacity and hence multiplied the *medium* demand by 1.1875 (i.e., 95 over 80), whereas *low* demand would result from 65% terminal capacity.

3.6 Solution Algorithms

In this section, we will first comment on the computational burden of the problem and then outline various algorithms that can solve this problem. These solution algorithms are as follows.

- Complete enumeration
- Implicit enumeration
- Traffic-based heuristic

3.6.1 Complete Enumeration

Complete enumeration proceeds by determining an exhaustive combination for defending and interdicting terminals. For example, for the case of defending/attacking two terminals in the network of eighteen terminals, the number of combinations amounts into $\binom{18}{2}*\binom{16}{2}$=*18360* possible defense and attack strategies. For each defense and attack strategy, the network operator's problem is solved assuming that the terminals attacked under this strategy have been disrupted. For each given defense strategy, the effect of all the ensuing attack strategies will be compared. The worst-case disruption following each defense strategy yields the total cost associated with the adoption of that defense strategy. The defense strategy with the lowest associated cost will be selected as the best defense strategy. Applying this procedure to the current case study will result in protection of intermodal terminals in Philadelphia and in Atlanta. The CPU time for this problem setting was 902.14 seconds, and it ranged from 241.1 seconds to 2063.18 seconds for the other eight scenarios.

It is easy to see that the complete enumeration technique will become rather cumbersome if more than two terminals have to be considered for fortification and interdiction. For example, the number of strategies requiring evaluation for the "three terminals" example

would be *371,280*. Thus, there is a need for a more efficient solution technique. This will be elaborated in the next sections of this chapter.

3.6.2 Implicit Enumeration

Under implicit enumeration, we first obtain the list of the worst-case disruptions which has been provided by examining all of the attack strategies. For the case of attacking/defending two terminals, an exhaustive combination for interdicting two terminals for our problem instance will be translated into $\binom{18}{2} = 153$ possible attacks. Then, for each attack strategy, the intermodal operator's problem is solved assuming that the terminals listed under this strategy have been out of service. The resulting solution gives us the total cost associated with each attack strategy, and the worst-case disruption would result from the strategy with the highest cost. The corresponding strategy called for the interdiction of intermodal terminals in Philadelphia and in Atlanta. This information will be passed to the implicit enumeration scheme proposed in Scaparra and Church (2008a). This was coded in C# and the entire search took 76.5 seconds. This solution algorithm is using a considerably reduced search space collectively containing only the defense strategies that will prevent the worst-case disruption. We next provide detail on how this enumeration scheme works.

As indicated above, the decoded solution of the inner problem suggested highest cost by interdicting Philadelphia (*Phi*) and Atlanta (*Atl*) together. Hence, fortifying either or both these terminals would preclude the worst-case disruption. The implicit enumeration scheme starts at the root node, i.e., node 1, by finding the worst-case disruption without

fortification (i.e., *Phi* and *Atl*). At each node, we determine set **O**, which lists the terminals for which at least one must be protected to prevent the worst-case. For instance, at node 1, terminal *Phi* or *Atl* could be fortified. By selecting Phi randomly, we branch on either to protect it or not to protect it.

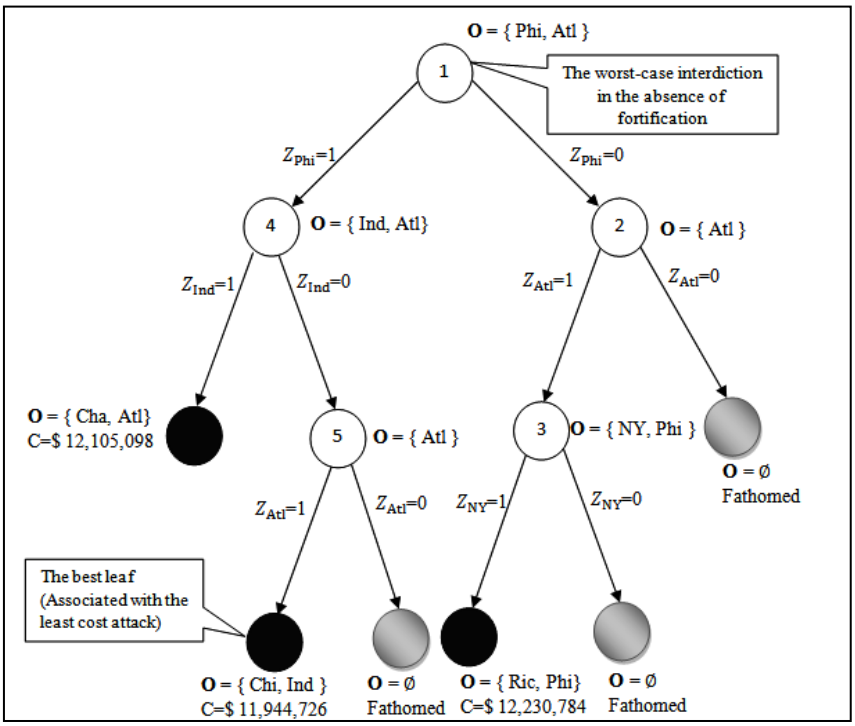

Figure 3-1: Tree Search

If *Phi* were not fortified, then the terminal at *Atl* would have to be considered for fortification (i.e., node 2). If even *Atl* is not fortified, then set **O** is empty thereby implying that none of the other fortifications can prevent the worst-case disruption, and the resulting node is fathomed (i.e., grey shade). This means that the worst-case attack at node 1 still possible. On the other hand, if *Atl* is fortified, then the worst-case disruption is prevented, and the elements for set **O** must be updated by solving the interdiction

problem with the latest information (i.e., *Atl* is fortified). Thus, the updated set **O** contains *NY* and *Phi* as elements representing the most disruptive interdiction given that *Atl* is fortified. At node 3, only one fortification resource is left, we continue the search process by arbitrarily selecting *NY*. If *NY* is not fortified, it is possible that it is disrupted together with *Phi* thereby resulting in a fathomed node. But if it is fortified, then the interdiction problem is solved given that *NY* and *Atl* are fortified. The updated set **O** contains *Atl* and *Ric*, both of which would be interdicted thereby resulting in a cost of around $12.2mn (i.e., dark shade).

At the left branch of node 1, if *Phi* were fortified, the interdiction problem is solved thereby resulting in terminals *Ind* and *Atl* in the updated set **O**. Arbitrarily selecting *Ind*, if it is fortified then the protection resources have been exhausted, and the resulting interdiction problem yields *Cha* and *Atl* terminals as the most disruptive. At the same time, no further branching is possible and the associated cost is around $12.1mn. But if *Ind* is not fortified, then the updated set **O** only contains *Atl* at node 5. If *Atl* is not fortified, then it will be attacked together with *Ind* thereby being fathomed. On the other hand, if *Atl* is fortified, then the interdiction problem is solved again to yield *Chi* and *Ind* as the most disruptive terminals, and the associated cost is around $11.9mn. The search cannot continue any further since all the defensive resources have been used.

The CPU time for the remaining eight scenarios ranged from 16.3 seconds to 336.24 seconds, which is quite good. We note that, given the definition of criticality for our problem instance, it is possible to arrive at the same solution more quickly by combining

information about the traffic flow through each terminal and (an adapted version of) the implicit enumeration of Scaparra and Church (2008a).

3.6.3 Proposed traffic-based heuristic

The proposed heuristic works in two steps. *First*, the capacitated multi-commodity flow problem for the network operator is solved (i.e., the inner level problem in ***(P)***). The resulting solution is decoded and the traffic volume through each terminal is estimated and ranked, in descending order, of throughput terminal traffic. Since there is enough resource to protect two terminals, fortifying the top two candidates on the list would make the worst-case disruption impossible.

In the *second* step, just like Scaparra and Church (2008a), the identity of the two terminals was supplied as input at the root node 1 in Figure 3-1. If *Phi* were fortified, then we update set **O** by including the third terminal from the list generated in step one. For instance, at node 4 in Figure 3-1, *Ind* would be selected from the list without solving the interdiction problem as in Scaparra and Church (2008a). If *Ind* is fortified then the protection resources are exhausted, and we select the fourth terminal on the list generated in step one, i.e., *Cha*, which would be interdicted along with *Atl*. The process continues as outlined in Figure 3-1, except that we have done away with the need to solve the interdictor's problem at each node and simply consult the list generated in step one. This has a positive bearing on the computational time, which for the given problem instance was 37.86 seconds compared to 76.5 seconds using the enumeration technique of Scaparra and Church (2008a).

It is important to reiterate that the proposed traffic-based heuristic worked well for the small problem instances in which only two terminals being fortified/attacked, but may not for much larger instances.

To conclude, the proposed heuristic is quicker than the other two solution techniques. Table 3-1 reports the relevant figures, where ***BC*** refers to the Base-Case (the situation in which the system performs its normal operations and no attack has happened), ***CE*** to complete enumeration, ***IE*** to the implicit enumeration scheme of Scaparra and Church (2008a), and ***Heuristic*** to the proposed traffic-based heuristic.

Due Date	Demand Level	CPU Time (Seconds)			
		BC	**CE**	**IE**	**Heuristic**
Short	Low	5.81	902.14	76.50	37.86
	Medium	7.90	1313.36	142.87	48.12
	High	1.48	260.48	17.91	9.32
Regular	Low	7.82	1362.13	123.33	49.52
	Medium	1.15	1282.12	285.51	32.57
	High	1.11	243.00	16.30	7.23
Long	Low	25.31	2063.18	336.24	149.87
	Medium	1.08	241.10	26.54	7.14
	High	9.66	859.00	96.80	55.72

Table 3-1 Summary of computation time

3.6.3.1 Numerical Analysis

In this subsection, we will first provide a snapshot of the solution for the nine scenarios developed using the due date and demand level combinations as outlined in section 4.2, and then comment on terminal utilization and network connectivity.

3.6.3.2 Analysis of Results

Following the enumeration, the resulting costs for all the leaf nodes (i.e., dark shade) was compared to conclude that the optimum strategy is to fortify *Phi* and *Atl*, which means that the interdictor would disrupt *Chi* and *Ind* and the system cost will be $11,944,726. Table 3-2 summarizes the results for the nine scenarios of due date and demand. For each scenario, three cases were considered: base case which is the normal situation of the system; interdiction without fortification, and interdiction with fortification. This categorization amounts to twenty-seven problem cases.

It is clear from all the nine scenarios that fortification improves the performance of the transportation system thereby resulting in lower costs vis-à-vis no protection. In fact, for the *short* due date setting, the performance improvement ranges from 7% for *low* to 9.2% for *high* demand levels. In other words, fortification has reduced the adverse effect of interdiction in each setting. It was noticed that the improvement was higher for scenarios where due dates were *short* and demand *high* versus *long* due date and *low* demand. Finally, express train service was mainly used with short due dates because of the pressure to deliver before the specified time and to prevent the penalty cost.

In terms of the traffic distribution, in the base case of all scenarios, no direct trucking has been used. With the occurrence of interdiction, the direct trucking service is taking place. Also, having fortification in place helps reduce the reliance of expensive truck-only transportation and return more traffic to the intermodal system which leads to an enormous cost reduction.

Due Date	Demand Level	Cases	OFV ($ mns)	Percent of Traffic		Intermodal Trains	
				Intermodal	Truck	Regular	Express
Short	Low	*Base Case*	9.93	100	0	25	12
		W/out Fort	12.84	46.22	53.78	16	6
		With Fort	11.94	66.07	33.93	19	5
	Medium	*Base Case*	10.99	100	0	26	10
		W/out Fort	14.34	44.05	54.95	17	6
		With Fort	13.26	66.19	33.81	19	5
	High	*Base Case*	13.61	100	0	36	14
		W/out Fort	17.80	43.18	56.82	15	8
		With Fort	16.15	59.81	40.19	19	11
Regular	Low	*Base Case*	9.67	100	0	36	0
		W/out Fort	12.71	46.23	53.77	22	0
		With Fort	11.78	66.08	33.92	24	0
	Medium	*Base Case*	10.70	100	0	36	0
		W/out Fort	14.20	43.05	54.95	23	0
		With Fort	13.07	66.18	33.82	25	0
	High	*Base Case*	13.26	100	0	48	3
		W/out Fort	17.65	43.18	56.82	27	0
		With Fort	16.18	63.82	34.18	32	1
Long	Low	*Base Case*	9.60	100	0	36	0
		W/out Fort	12.67	46.23	53.77	22	0
		With Fort	11.73	66.08	33.92	24	0
	Medium	*Base Case*	10.62	100	0	36	0
		W/out Fort	14.16	45.05	54.95	24	0
		With Fort	13.02	66.19	33.81	25	0
	High	*Base Case*	13.17	100	0	48	0
		W/out Fort	17.60	43.18	56.82	27	0
		With Fort	16.12	65.82	34.18	33	0

Table 3-2: Snapshot of the nine scenarios

3.6.3.3 Capacity and Network Connectivity

It should be clear that since interdiction of terminals renders them unusable, relevant traffic would have to be re-routed using alternative terminals thereby impacting their utilization. Since each terminal in the network has a finite capacity, it may not always be possible to reassign traffic to other terminals. In other situations, an interdiction may

result in shippers and/or receivers losing their connectivity to the intermodal network and in such cases demand would have to be met using direct trucking service. In this subsection, we analyze average capacity utilization of terminals and the lack of connectivity for the twenty-seven cases under the nine scenarios (Table 3-3). The lack of connectivity is defined as the total number of containers originating from customers who lost their connections to the network due to the interdiction divided by the total demand in the network.

Within each scenario, the *Base Case* has the highest average capacity utilization resulting from the connectedness of all shippers/ receivers and the proper working of all terminals, which also implies no direct truck service. Within each scenario, interdiction without fortification (i.e., *W/out Fort*) has the lowest capacity utilization since 23% of the customers have lost connectivity with the intermodal network, and have to make use of the direct trucking service to move shipments. It was noticed that interdiction with fortification (i.e., *With Fort*) yielded better capacity utilization than the without settings because the worst-case disruptions have been avoided, and relatively fewer customers lose connectivity to the intermodal network. In eight of the nine scenarios, 19% of the traffic loses connectivity and in one scenario only 3% of traffic is losing the connectivity. This shows that in the most difficult scenario, short due date and high demand, fortification is able to retain connectivity better than other scenarios. stemming from the fortification of *Phi* and *Atl*, and the interdiction of *Chi* and *Ind*. Finally, it was observed

that for a given due date level, average capacity utilization was linearly related to the demand level.

Due Date	Demand Level	Cases	Avg. Cap. Utz.	Number of terminals (utilization) Upto 25	Upto 50	Upto 65	Upto 80	Upto 90	Upto 100	% loss
Short	Low	*Base Case*	72%	0	0	1	14	3	0	0
		W/out Fort	53%	4	6	4	2	0	2	23
		With Fort	60%	3	3	3	7	2	0	19
	Medium	*Base Case*	80%	0	0	0	11	7	0	0
		W/out Fort	57%	4	3	6	2	1	2	23
		With Fort	66%	2	3	4	4	4	1	19
	High	*Base Case*	95%	0	0	0	0	0	18	0
		W/out Fort	66%	4	2	3	5	1	3	23
		With Fort	81%	2	0	5	2	1	8	3
Regular	Low	*Base Case*	72%	0	0	2	14	1	1	0
		W/out Fort	52%	4	7	4	1	0	2	23
		With Fort	62%	3	3	3	6	2	1	19
	Medium	*Base Case*	79%	0	0	0	10	7	1	0
		W/out Fort	55%	4	3	8	0	1	2	23
		With Fort	68%	2	3	4	5	1	3	19
	High	*Base Case*	96%	0	0	0	0	2	16	0
		W/out Fort	63%	3	4	2	6	0	3	23
		With Fort	81%	2	2	3	2	1	8	19
Long	Low	*Base Case*	71%	0	0	5	10	2	1	0
		W/out Fort	52%	4	6	5	1	0	2	23
		With Fort	62%	3	3	4	5	2	1	19
	Medium	*Base Case*	79%	0	0	2	8	7	1	0
		W/out Fort	55%	4	3	8	0	1	2	23
		With Fort	67%	2	3	5	3	3	2	19
	High	*Base Case*	96%	0	0	0	0	1	17	0
		W/out Fort	63%	4	3	7	1	0	3	23
		With Fort	81%	2	2	3	2	1	8	19

Table 3-3: Capacity Utilization and Connectivity

At the end of this section, it should be noted that although the simple flow-based heuristic developed here is able to solve the problem efficiently, for larger attack/defense budgets, it is quite incapable of doing so. Therefore there is a need to develop a new solution technique to cope with larger problem instances. In the next section a solution algorithm

based on decomposition will be introduced which is quite capable of dealing with the computational burden of large instances of this problem.

3.7 Conclusion

In this chapter, we developed a path-based version of the tri-level DAD framework to reduce the computational difficulty of this problem. The resulting complexity, and the model characteristics, motivated the development of an efficient solution technique. Specifically, a traffic-based heuristic has been proposed to solve small instances of the DAD problem on the realistic infrastructure of a class I railroad operator. Also, the computational performance of the proposed traffic-based heuristic was compared with the existing technique.

It should be mentioned here that the proposed solution technique in this chapter is using a combination of implicit enumeration of Scaparra and Church (2008a), to break the tri-level problem into a set of bi-levels, and then uses a traffic-based heuristic to solve each bi-level problems. Thus, the proposed method extends the method proposed by Scaparra and Church (2008a), which is only useful in bi-level settings, to be applicable for tri-level setting.

Preliminary results of applying the traffic-based solution technique to larger problem instances, i.e. problems with more than two attacks/defenses, show a declining trend in the quality of its solutions. This indicates the need for a more advanced solution technique for dealing with large-scale problem instances.

Summary of Contributions of Chapter Four

Presentations and Publications:

- Accepted for presentation at INFORMS 2014, San Francisco, U.S.
- Submitted to *European Journal of Operations Research*, Revise-and-Resubmit.

Output:

- An efficient decomposition-based heuristic solution technique for solving instances of the DAD problem.

Chapter 4: A Decomposition-based Solution Technique for Protection Planning of a Rail-Truck Intermodal Terminal Network

4.1 Introduction

In this chapter, a new solution technique to solve large instances of the DAD problem is proposed. The new solution technique benefits from decomposing the three-level DAD problem into smaller sub-problems which can be solved efficiently. This enables the proposed solution technique to solve fairly large problem instances. The new solution technique has been applied to different problem instances derived from the realistic case study defined in Chapter Two. The results of solving these instances by the decomposition based solution technique prove the merits of this solution technique in terms of the quality of the obtained solutions and computational time.

4.2 Decomposition based Heuristic

As it is mentioned in Chapter Three, the proposed traffic-based heuristic is not able to produce solutions of high quality for large problem instances of the DAD problem. This generates motivation for developing an efficient solution technique for larger instances of the DAD problem.

To begin with the new solution technique, it is important to note that problem ***(P)***, shown in section 3.4.1, is a very complex and difficult problem. In fact, it has been proved that even a bi-level problem is NP-hard (Jeroslow, 1985), and therefore (***P***), as a tri-level

problem, is at least NP-hard. In order to solve (***P***) efficiently, a **two** stage solution technique is proposed. In the ***first*** stage, an implicit enumeration technique as proposed in Scaparra and Church (2008a) is used to break the tri-level DAD problem into a set of smaller bi-level AD sub-problems (Figure 3-1). In the ***second*** stage, the proposed decomposition-based solution technique solves each resulting AD, and the set of decisions leading to the lowest cost subsequent attack is the best fortification plan.

4.2.1 The First Stage

The Implicit Enumeration technique reduces the computational burden of the outermost level (i.e., network operator) by implementing a rather simple but intuitive observation. It states that the optimal solution of the network operator should entail fortification of at least one of the terminals that would be interdicted in the worst-case attack (Scaparra and Church, 2008a).

It is important to reiterate that the implicit enumeration scheme of Scaparra and Church (2008a) reduces the tri-level DAD problem to a set of bi-level AD problems, and then each bi-level AD problem needs to be solved. After solving all the generated bi-level AD problems, we can determine the best protection plan. We next propose an efficient solution technique for the bi-level AD problems.

4.2.2 The Second Stage

The prevalent technique for solving AD problems is based on duality theory, wherein the dual of the inner problem is combined with the outer problem to create a single-level

problem (Wood, 2011). It is important to note that this approach would work only if the variables in the inner problem are real valued, or if integer, they can be relaxed without losing integrality. The innermost component of ***(P)*** contains train frequency variables, which are inherently integers, and hence cannot be relaxed without losing accuracy. To overcome this difficulty and to solve AD problems properly, we adapt the classical Bender's decomposition technique (Benders, 1962) to account for the integer variables in the inner problem, which is consistent with the approach in the literature (Gabriel, Shim, Conejo, de la Torre, & García-Bertrand, 2010; Losada, Scaparra, Church & Daskin, 2012).

The proposed decomposition breaks the bi-level AD problem into a master problem (MP) and a sub-problem (SP). In the first step, SP (which is the intermodal operator's problem) is solved to determine the routing plan and the optimum number of intermodal train services, wherein the latter are integer valued. The output of SP becomes the parameters used to build the MP, which is a single level interdictor's problem. To make this more explicit, we next outline the specific steps involved.

Once the SP is solved and the train frequency variables are fixed to their optimum (integer) values, the intermodal operator's problem exhibits unimodularity, i.e., which means that other integer variables could be relaxed without obtaining non-integer values (Wolsey, 1998). Thus, the dual of the intermodal operator's problem can be taken. To that end, we define three sets of dual variables corresponding to constraints (9) to (11) in ***(P)***.

$$\sum_{p\in P_{ij}} X_{ij}^{p} + XT_{ij} \geq D_{ij} \qquad \forall i \in I, \forall j \in J \quad (\omega_{ij}\ Positive) \qquad (9)$$

$$\sum_{i\in I}\sum_{j\in J}\sum_{p\in P_{ij}\cap P_{ij}^{k}} X_{ij}^{p} \leq U_k(1-y_k) \qquad \forall k \in K \qquad (\beta_k\ Negative) \qquad (10)$$

$$\sum_{i\in I}\sum_{j\in J}\sum_{p\in P_{ij}\cap S^{l,v}} X_{ij}^{p} - \alpha^{v}N^{v} \leq 0 \qquad \forall v \in V, l \in L^{v} \quad (\theta_l\ Negative) \qquad (11)$$

If the dual of the intermodal operator's problem is attached to the interdictor's problem, we end up with the following objective function:

$$Max_{y_k}\left(Max_{\omega,\beta,\theta}\left(\sum_{i\in I}\sum_{j\in J} D_{ij} * \omega_{ij} + \sum_{k\in K} U_k * \beta_k * (1-y_k)\right)\right) \qquad (15)$$

which can be simplified to the following form:

$$Max_{y,\omega,\beta,\theta}\left(\sum_{i\in I}\sum_{j\in J} D_{ij} * \omega_{ij} + \sum_{k\in K} U_k * \beta_k * (1-y_k)\right) \qquad (16)$$

Since this objective function is independent of variable θ, we can further simplify it to obtain the following objective function:

$$Max_{y,\omega,\beta}\left(\sum_{i\in I}\sum_{j\in J} D_{ij} * \omega_{ij} + \sum_{k\in K} U_k * \beta_k * (1-y_k)\right) \qquad (17)$$

This objective function is subject to the following constraints:

$$\omega_{ij} + \sum_{\{\forall k | p\in P_{ij}^{k}\}} \beta_k + \sum_{\{\forall l | p\in S^{l,v}\}} \theta_l \leq E_{ij}^{p} \qquad \forall i \in I, \forall j \in J, \forall p \in P_{ij} \qquad (18)$$

$$\omega_{ij} \leq E_{ij} \qquad \forall i \in I, \forall j \in J \qquad (19)$$

$$-\alpha^{v}\theta_l \leq FC^{v} \qquad \forall v \in V, \forall l \in L^{v} \qquad (20)$$

$$\sum_{k \in K} y_k \leq R \tag{21}$$

$$\omega_{ij} \geq 0 \qquad \forall i \in I, \forall j \in J \tag{22}$$

$$\beta_k \leq 0 \qquad \forall k \in K \tag{23}$$

$$\theta_l \leq 0 \qquad \forall l \in L^v \tag{24}$$

$$y_{\mathrm{k}} \in \{0,1\} \qquad \forall k \in K \tag{25}$$

where,

$$E_{ij}^p = \begin{cases} C_{ij}^p + \left(T_{ij}^p - \bar{T}_{ij}\right) PC_{ij}, \ if\ T_{ij}^p > \bar{T}_{ij} \\ C_{ij}^p, \quad otherwise \end{cases} \tag{26}$$

$$E_{ij} = \begin{cases} CT_{ij} + \left(T_{ij} - \bar{T}_{ij}\right) PC_{ij}, \ if\ T_{ij} > \bar{T}_{ij} \\ CT_{ij}, \quad otherwise \end{cases} \tag{27}$$

Note that (16)-(27) represents a single level problem that optimizes both the interdictor's and the dual of the intermodal operator's problem over all the variables.

It is important to note that the objective function (16) has some non-linear terms in the form of $\beta_k * (1 - y_k)$, since both β_{k} and y_{k} are decision variables, and therefore it cannot be solved easily. Therefore, we next outline a suitable linearization scheme to facilitate solving the combined single level AD problem.

4.2.3 Linearization Scheme

Each non-linear term of $\sum_{k \in K} U_k * \beta_k * (1 - y_k)$ can take two values depending on the value of the binary variable y_k. It can be $U_k * \beta_k$ if $y_k = 0$, or it is zero if $y_k = 1$. Now, we replace each term $\beta_k * (1 - y_k)$ by a new variable called φ_k, and add constraints sets (28) to (30) to ensure that φ_k will get the right values. Note that *M* is a large positive number.

$$\varphi_k \leq \beta_k + M * y_k \tag{28}$$

$$\varphi_k \geq -M * (1 - y_k) \tag{29}$$

$$\varphi_k \leq 0 \tag{30}$$

If $y_k = 0$, (28) and (29) will ensure that $\varphi_k \leq \beta_k$ and $\varphi_k \geq -M$, respectively. Note that the intersection of the boundaries of these three constraints is $\varphi_k \leq \beta_k$.

Also, because it is a maximization problem and β_k is negative, the correct value of φ_k would be β_k. On the other hand, if $y_k = 1$, the intersection of the boundaries of all the three inequalities would imply $\varphi_k = 0$.

To formalize the discussion in this section, we next introduce the notations and parameters used to outline the pseudo code for the decomposition algorithm to solve the bi-level AD problems (Figure 4-1). Finally, we depict the interaction between the master problem and the sub-problem in Figure 4-2.

Notations and Parameters

MP: Master problem

SP: Sub-problem

LB: Lower bound

UB: Upper bound

h: Index for iteration of the solution algorithm

Y_h: List of interdicted terminals in the MP at iteration h

OFV_{SP}^{*}: Objective function value of the sub-problem

OFV_{MP}^{*}: Objective function value of the Master problem

X_h: Vector of the optimal customer allocation to intermodal paths in iteration h

F_h: Vector of the optimal frequency of train services in iteration h

X^{*}: Vector of the optimal customer allocation to intermodal paths so far

Max_iteration: Maximum number of iterations

ε: The desired optimality gap

Initial values

$LB \leftarrow -\infty$

$UB \leftarrow +\infty$

$h \leftarrow 0$

$Y_0 = \emptyset$

While $(UB - LB > \varepsilon * LB)$and $(h \leq Max\_iteration)$

Solve *SP* (Y_h) to determine the best load plan X_h, the frequency of trains F_h and OFV_{SP}^{*}

If $(OFV_{SP}^{*} < UB)$, then: $F^{*} \leftarrow F_h$ and $X^{*} \leftarrow X_h$ and $UB \leftarrow OFV_{SP}^{*}$

If $(UB - LB \leq \varepsilon * LB)$, then go to the **Report**.

Solve *MP* (F_h) to determine the interdiction plan $Y_{h+1}$and OFV_{MP}^{*}

If $(OFV_{MP}^{*} > LB)$, then: $Y^{*} \leftarrow Y_{h+1}$ and $LB \leftarrow OFV_{MP}^{*}$

If $(UB - LB \leq \varepsilon * LB)$, then go to the **Report**.

$h \leftarrow h + 1$

Return to the **While** condition

Report F^*,X^*,Y^*, OFV_{MP}^* and OFV_{SP}^* as the outputs of the solution algorithm.

END

Figure 4-1: Pseudo code for the decomposition algorithm

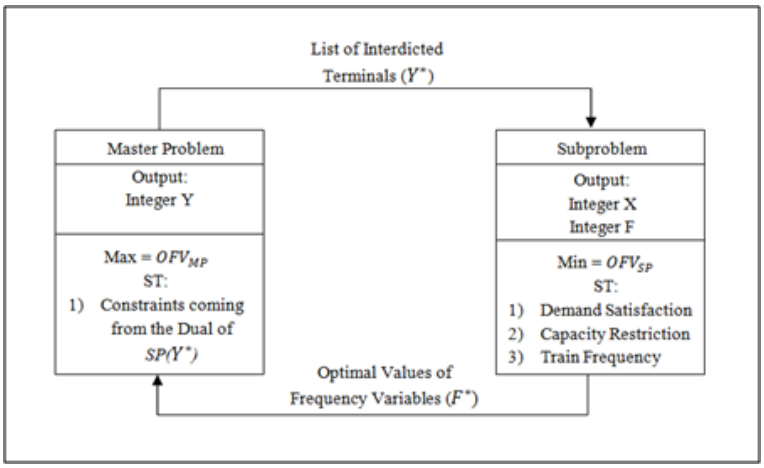

Figure 4-2: Interaction between the master problem and the sub-problem

4.3 Numerical Analysis

In this section, we first provide an outline of the case study developed using realistic publicly available information, along with the estimation of the relevant parameters. We then discuss the solution, algorithmic efficiency, and managerial insights.

4.3.1 Problem setting

The analytical framework developed in this section was applied to problem instances generated using the realistic railroad infrastructure of a class I railroad operator in the United States introduced earlier in section 2.5. Parameters like cost and terminal capacities are similar to what have been introduced in section 3.5. Also, in this section, we focus on *medium* level of the demand and due date.

Finally, we set the optimality gap ε in the decomposition algorithm to 1%, and the maximum number of iterations to 10.

4.3.2 Solution

The analytical framework was implemented in C# using CPLEX 12.6.0 concert technology on a PC with Core 2 Quad, 2.4 GHz processor with 4 GB of RAM. For expositional reasons, and also to demonstrate the efficiency of the proposed solution methodology, we define four scenarios. The *first* scenario, referred to as ***EX***, finds the exact solution for the proposed DAD problem and therefore it applies the optimal fortification. It makes use of the implicit enumeration, to transform DAD problem to a set of ADs, and then uses the complete enumeration technique to find the optimal solution of each AD problem. The *second* scenario, referred to as ***PH***, finds a heuristic solution for the DAD problem. It makes use of the implicit enumeration technique to transform the DAD to a set of ADs, and then uses the proposed decomposition-based heuristic to solve each produced AD. The *third* scenario, referred to as ***WC***, solves an AD problem to identify the critical terminals and then fortifies them. To find the solution of the AD problem, ***WC*** uses a complete enumeration. Note that, as explained in Figure 3-1, this is equivalent to providing the list of worst-case disruption to the root node to initialize the implicit enumeration scheme. *Finally*, for comparative assessment, we also indicate the solution for interdiction without fortification instances, and refer to them as ***NO***. It is important to reiterate that no terminal is defended under this scenario, which is qualified via ***NO**** in the last column in Table 4-1.

Number of terminals		Scenarios ($)			
Fortified	**Interdicted**	***EX***	***PH***	***WC***	***NO****
0	*0*	10,700,751			
1	*1*	12,620,928			12,842,074
2	*2*	13,073,754			14,202,436
3	*3*	12,746,283		13,894,151	15,174,754
4	*4*	12,717,366		14,180,059	15,731,475
5	*5*	12,777,930	12,818,637	13,073,155	16,293,981
6	*6*	12,517,981		13,030,159	16,487,783
7	*7*	12,236,503		13,256,471	16,600,378
8	*8*	15,793,979	12,474,923	16,655,991	16,681,282
9	*9*	15,206,223	12,284,193	16,735,853	16,769,569

Table 4-1: Objective function values for the four scenarios

The first row of Table 4-1 depicts the situation where no terminal is either fortified or interdicted; hereafter referred to as the *Base-Case*, and returns a single unique solution across all scenarios. The nine subsequent rows provide a snapshot of the results when both the number of terminals fortified and interdicted is increased. While we provide the details on the CPU time later in this section, it is important to indicate that the last two problem instances (i.e., shaded in grey) could not be solved within a reasonable amount of time. Hence, the reported solutions are the best ones encountered within the cut-off times of three hours and six hours for these two instances, respectively.

From Table 4-1 we derive **five** interesting points.

- *First*, all the scenarios with fortification outperform the one without, and that it exhibits increasing cost with higher numbers of interdicted terminals. The latter point should be clear since higher numbers of interdicted terminals implies increased reliance on the more expensive transportation option, i.e., direct truck service.

- *Second*, scenario ***WC*** does not provide a better solution than either ***EX*** or ***PH***. This result is consistent with observations of Church and Scaparra (2008a, b) and Brown et al. (2006) who advise against using the output of the interdiction model to make fortification decisions, since such strategies are suboptimal and will never provide the best protection against worst-case disruptions.

- *Third*, the proposed decomposition heuristic is able to find the optimal solution in all but one problem instance. This clearly proves the high quality of solutions obtained by this method.

- *Fourth*, for both ***EX*** and ***PH***, compared to ***WC***, the cost shows less fluctuations and even with the increase in the number of attacked/defended terminals it starts decreasing which is in sharp contrast with the trend observed in ***NO*** scenario. The cost associated with implementing each of these four defense scenarios has been plotted in Figure 4-3 for different numbers of attacked/defended terminals. It is obvious in this figure that ***PH*** demonstrates the best performance compared to other scenarios since it shows a very consistent and generally decreasing trend. We postulate that the costs would decrease further if the program was allowed to naturally terminate for the eight- and nine-terminals problem instances. This is because although the number of terminals interdicted increases, the defender is also able to fortify a larger number of (more important) terminals, which in turn forces the interdiction of terminals not likely to increase the resulting cost.

- *Fifth*, for the last two rows and within the specified cut-off time, the best encountered solutions with ***PE*** are much better than that with ***EX***. We elaborate on this when discussing the computational time. Also, the cost associated with implementing ***WC*** increases sharply for 8 and 9 attacked/defended terminals and this scenario indeed produces results as poor as the results of the ***NO*** scenario.

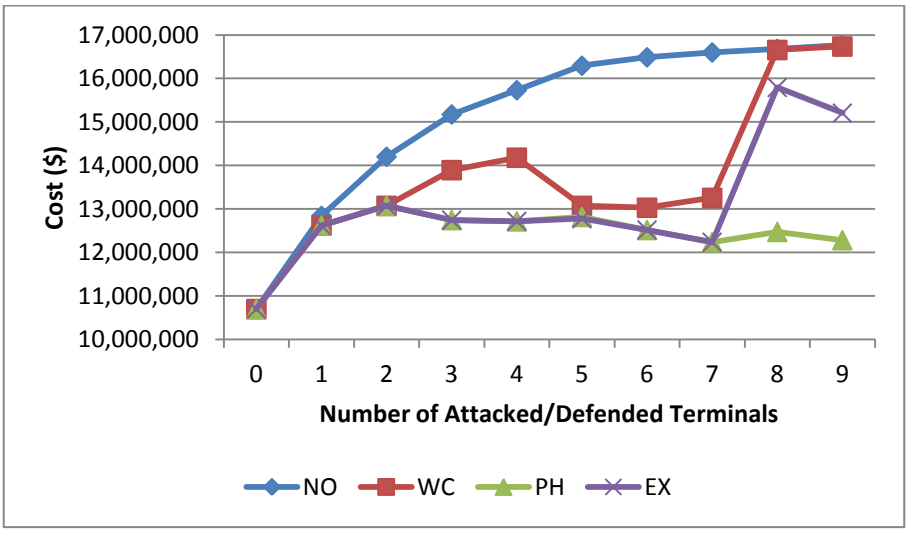

Figure 4-3: Cost imposed to the system following each defense scenario

Table 4-2 depicts the split of traffic between the rail-truck intermodal system and the expensive truck-only option under the different problem settings. As expected, the entire traffic uses the intermodal option when the infrastructure is functioning normally, i.e., *Base-Case*. Note that the proportion of shipments using the truck-only option increases with the number of terminals interdicted for the ***NO*** scenario, which is expected because fewer train services could be routed on the reduced network. Furthermore, as indicated in Table 4-1, ***WC*** results in a suboptimal fortification plan, since the proportion of traffic using the expensive truck-only option is only better than the ***NO*** scenario. Finally, under

both ***EX*** and ***PH***, the proportion of traffic using truck-only maxes out around 40%, which demonstrates the effectiveness of both fortification strategies in ensuring that the majority of the intermodal network are operational –irrespective of the interdiction budget. The above observations are entirely supported by the number of trains of both *regular* and *express* types being used in the four scenarios (Table 4-3). It should be evident that with the higher number of interdictions (and fortifications) faster trains are used when possible to avoid late deliveries.

Number of terminals		**Percent of traffic between T/ RT**			
Fortified	**Interdicted**	***EX***	***PH***	***WC***	***NO****
0	*0*	0/100			
1	*1*	28.3/71.7			34.4/65.6
2	*2*	33.9/66.1			55.0/45.0
3	*3*	33.7/66.3		51.4/48.6	64.9/35.1
4	*4*			56.1/43.9	79.9/20.1
5	*5*	38.2/61.8	40.3/59.7	47.5/52.5	84.1/14.9
6	*6*	30.5/69.5		41.7/58.3	90.4/9.6
7	*7*	26.0/74.0		46.5/53.5	93.4/6.6
8	*8*	75.8/24.2	28.5/71.5	96.0/4.0	95.0/5.0
9	*9*	66.2/33.8	24.7/75.3	98.3/1.7	99.1/0.9

Table 4-2: Traffic split between truck-only (T) and rail-truck intermodal (RT)

Number of terminals		**Number of Express/ Regular trains**			
Fortified	**Interdicted**	***EX***	***PH***	***WC***	***NO****
0	*0*	0/36			
1	*1*	0/28			0/27
2	*2*	0/25			0/23
3	*3*	1/26		1/20	0/20
4	*4*			1/19	0/12
5	*5*	1/24		1/20	0/10
6	*6*	0/26		0/24	0/6
7	*7*	1/29		1/22	0/5
8	*8*	0/13	1/30	0/4	0/4
9	*9*	1/15	0/31	0/3	0/1

Table 4-3: Number of intermodal train services

4.3.3 Computational Performance

We next comment on the computational performance of the proposed heuristic. Table 4-4 reveals that the number of possible outcomes needing evaluation increases exponentially with the number of terminals fortified and interdicted, which in turn impacts the CPU time. Although the computation time for both ***EX*** and ***WC*** is rather comparable, the latter results in suboptimal solutions and hence is not of much interest. ***PH*** is able to return solutions as good as ***EX***, except for one problem instance (Table 4-1), in much shorter time. It is easy to see that this is possible because while both ***EX*** and ***PH*** are benefiting from the implicit enumeration scheme to convert the tri-level problem into a set of bi-level AD problems, in the ***PH*** each of the resulting ADs is solved efficiently by the heuristic decomposition depicted in Figure 4-2 (and Section 4.2.2). In the ***EX***, on the other hand, each bi-level AD is solved by embarking on the complete enumeration of all the possible attack possibilities. In an effort to further highlight the effectiveness of the decomposition component of ***PH***, we have listed, under the title ***HD***, the total CPU time required for executing the heuristic decomposition, described in the pseudo code of Figure 4-2. It should be clear that in this table while both ***WC*** and the proposed decomposition scheme are solving bi-level AD problems to find the worst-case attack, the latter is able to return the solutions that ***WC*** returns, i.e. the highest quality solutions, in significantly lower CPU time. In fact, the performance of the proposed heuristic in solving AD problems is independent of the attack budget while the performance of the ***WC*** is sharply impaired by an increase in the attack budget. Finally, it is important to note that the major part of the computation time under ***PH*** must be attributed to the first stage,

i.e., the implicit enumeration scheme outlined previously, since the implicit enumeration transforms the DAD problem into ***too many*** bi-level ADs. Although each of the produced ADs can be solved very efficiently, by using the proposed decomposition heuristic, solving a lot of them will eventually increase the CPU time. In Chapter Five, we will demonstrate a metaheuristic-based tree search process, which enables us to transform the DAD problem to a fewer number of bi-level ADs so that the execution of ***PH*** can be expedited.

# Fortified/ Interdicted	**# Possible Outcomes**	***EX***	***PH***		***WC***
			Total	**HD**	
1	18	77	10	3.09	77
2	153	286	33	2.92	286
3	816	1,570	86	2.12	1,569
4	3,060	5,747	364	2.32	5,745
5	8,568	15,450	1,206	2.01	15,435
6	18,564	32,271	3,361	1.96	32,117
7	31,824	47,395	13,304	2.02	46,314

Table 4-4: CPU time (seconds) for the three fortification techniques

4.3.4 Insights

In this section, we comment on the intermodal terminals that should be fortified, and also provide some insights on their utilization under different problem instances. The terminals which are fortified are exactly the same for ***EX*** and ***PH***, except in one problem instance. For the five-terminal problem instance, the intermodal terminal at Chicago was fortified under ***EX***, and Jacksonville under ***PH***. As indicated earlier, since the output of the interdiction model is used to make fortification decisions in ***WC***, the list of terminals has less similarity to the other two.

Finally, it should be clear that since interdiction of terminals renders them unusable, relevant traffic would have to be re-routed using alternative terminals thereby impacting their utilization. Since each terminal in the network has a finite capacity, it may not always be possible to reassign traffic to other available terminals in the network. Also, an interdiction may result in shippers and/or receivers losing their connectivity to the intermodal network and in such cases demand would have to be met using direct trucking service. For expositional reasons, and without losing generality, we analyze terminal capacity utilization for three distinct problem instances: *Base-Case*; and, fortification/interdiction of three-terminal and seven-terminal problem instances (as shown in Table 4-5).

Number Fortified	**Number Attacked**	**Cases**	**Avg. Cap. Utz.**	**Number of Terminals on each Category of Utilization**						**% loss**
				<25	**<50**	**<65**	**<80**	**<90**	**<100**	
0	0	*Base-Case*	79%	0	0	0	10	7	1	0
	3	***NO***	46%	6	4	6	0	1	1	71.7
	7		26%	14	2	0	1	0	1	95
3	3	***WC***	61%	4	4	2	4	1	3	37
		EX	68%	3	3	1	7	3	1	24.7
		PH								
7	7	***WC***	58%	9	1	3	2	0	3	31.4
		EX	68%	10	0	2	2	2	2	1
		PH								

Table 4-5: Capacity utilization of the terminals

As expected the average capacity utilization of active terminals is the highest under the *Base-Case*, which results from normal functioning of all terminals and not using any direct trucking service. With no fortification, the average utilization drops from 46% to 26% when the number of terminals interdicted increases from three to seven and the loss

in connectivity increases from 71% to 95%. Therefore, with no fortification, it is almost impossible to connect shippers and receivers by the rail truck intermodal network when seven terminals have been attacked. It was interesting that the average capacity utilization under both ***EX*** and ***PH*** was always better than that under ***WC***. Also, with the increase in the number of fortified and attacked terminals from three to seven, while ***WC*** shows a drop in the average capacity utilization from 61% to 58%, the capacity utilization under ***EX*** and ***PH*** was stable at 68%. In terms of the loss in connectivity, with the increase in the number of fortified/attacked terminals, all the defense strategies, i.e. ***WC***, ***EX*** and ***PH***, show a decreasing trend. Specifically, the drop in the loss of connectivity under ***EX*** and ***PH*** is remarkable such that almost all the demands could be shipped by the rail-truck intermodal network. This highlights the importance of having suitable defense strategies in place which will enable the rail truck network to deliver almost all the demands from the shippers to the receivers even in the tough condition when seven terminals have been attacked.

4.4 Conclusion

In this chapter, we developed a decomposition-based heuristic to deal with larger instances on the realistic infrastructure of a class I railroad operator. In addition, the computational efficiencies of proposed heuristics were highlighted in relation to the existing techniques.

Computational experiments shed light on some interesting observations. First, spending the finite resources judiciously to fortify a given number of intermodal terminals would

improve the post-interdiction performance of the remaining intermodal transportation system dramatically. The cost saving of having such a suitable protection plan in place is an important input to high level decision makers who need to compare costs and benefits of launching this protection plan. Second, contrary to intuition, using the output of the Attacker-Defender problems, except for small instances, will never achieve the optimal fortification. This means that optimization of fortification should be addressed directly. Finally, in most of the cases, the proposed decomposition-based heuristic is capable of returning high quality solutions in a reasonable amount of time. Specially, the proposed heuristic for solving the AD problems is producing excellent results in a very short time.

Although the proposed heuristic decomposition, compared to other solution techniques, produces the best results, its performance in dealing with large instances drops sharply. Such a rapid decline in the computational performance can be attributed to the fact that the size of the problems are increasing so fast. Also, it might be the case that the tree search component of the decomposition based heuristic is not efficient enough in dealing with the sharp increase in the size of the solution space. Therefore, we conjecture that there might be a better way to cope with the increased size of the problem. This will constitute the inspiration for the next chapter where a more efficient solution technique for large-scale instances will be suggested.

Summary of Contributions of Chapter Five

Presentations and Publications:

- Accepted for presentation at CORS 2015, Montreal, Canada.
- Targeted at the *Transportation Research Part E: Logistics and Transportation Review*.

Output:

- An efficient heuristic solution technique for solving large-scale instances of the DAD problem.

Chapter 5: Tabu Search Metaheuristic for Solving Protection Planning in Rail-Truck Intermodal Transportation

5.1 Introduction

At the end of the previous chapter we conjectured the reason for the declining performance of the proposed decomposition-based heuristic on large instances. To see what exactly challenges the proposed decomposition technique in solving large scale instances of the DAD efficiently, Table 5-1 provides very useful information.

Number of terminals		**No of intermediate nodes**		
Fortified	**Interdicted**	**Leaves**	**Processed**	**Total**
2	*2*	3	6	11
3	*3*	14	25	49
4	*4*	54	100	199
5	*5*	198	370	739
6	*6*	745	1,387	2,773
7	*7*	2,722	5,281	10,561
8	*8*	8,566	17,817	35,633
9	*9*	27,551	60,410	120,819

Table 5-1: Rapid growth of size of the tree search

According to this table, the number of nodes produced by the implicit enumeration technique is increasing very fast when the number of attacks/defenses increases. More specifically, in each search tree like Figure 3-1, two types of nodes could be identified: processed nodes, and leaves. The processed nodes are those nodes in which a bi-level AD problem must be solved (this includes node 3, node 4, and all the dark shade nodes in Figure 3-1). The leaves are a subset of processed nodes which are the ending nodes of the

tree in which the worst-case attack is prevented in them (this only includes the dark shade nodes in Figure 3-1). The total column in this table indicates the total number of nodes produced in the search tree. For each problem instance, the difference between the total column and the process column indicates the number of nodes in which there is no need to solve a bi-level AD problem. The optimal solution is the set of decisions that lead to a leaf with the lowest objective function value. As it is clear in Table 5-1, with the increase in the number of attacks/defenses, the total number of nodes and especially the total number of processed nodes will increase dramatically. Although at each of these processed nodes the resulting bi-level problem will be solved very efficiently with the proposed solution technique, having too many of these nodes eventually increases the computational time and makes the proposed decomposition technique incapable of solving big instances of the DAD problem. To circumvent this issue, there is a need for another solution technique that bypasses all these intermediate nodes and produces the leaves directly. Such a technique should also act intelligently in the solution space and be able to find good solutions very fast.

5.2 Literature Review

5.2.1 Metaheuristics

Approximate solution techniques, or heuristics, have been used since the early days of operations research to deal with computationally difficult problems. Development of complexity theory in the early 1970's makes it clear that most of these problems are NP hard and, thus, there is little chance to find efficient exact solution techniques for them.

As a result of this conclusion, the role of heuristics in solving NP hard optimization problems has been recognized since in many cases heuristics are the only practical way to handle such problems.

The most prevalent and simplest heuristic approach is the local search technique (Gendreau, 2003). The local search can be imagined as an iterative search that begins with an initial feasible solution and then gradually improves it by applying some local modifications. At each iteration of this heuristic, local modifications will be applied to the current solution and among the produced solutions the best improving one will be selected. The search terminates when it faces a local optimum with regard to the local transformations that it applies.

A serious drawback of this heuristic is that the local optimum found, in most of the cases, is very far from the global optimum solution. In local search, primary factors that influence the quality of the solution obtained and computation time are the richness of the set of transformations that are performed at each iteration of the heuristic and the initial solution. In the late 1970's and the early 1980's, by inspiration from natural phenomenon, many other heuristic approaches were proposed which provided better results. The advent of these techniques, which Glover (1986) called *metaheurstics*, produced a lot of hope since they help the local searches escape from the local optimum trap.

Generally speaking, metaheuristics are approximate solution methods that establish a connection between local search procedures and higher-level search strategies. Creating this link makes the overall search process competent enough to cross over from local optima by implementing a thorough and robust search of the solution space.

While metaheuristics are not able to confirm the optimality of their solutions, this weakness seems negligible when considering the fact that exact procedures are often unable to find solutions whose quality is close to that obtained by metaheuritics. Such a good performance of metaheuristics in recent years, especially in dealing with real life optimization problems with a combinatorial nature, has made them the first choice in handling computationally difficult problems.

To better understand differences among metahueristics, there is a need to classify them based on their individual characteristics. Among different existing classifications, the most important and yet popular one is based on the number of solutions that the metaheuristic uses at the same time. In this regard, some metaheuristics work on a population of solutions while the others work on a single solution at a time. Algorithms working on a single solution are called single thread or trajectory methods and this category includes local search based metahueristics like Simulated Annealing, Tabu Search and Variable Neighborhood Search. On the other hand, algorithms that perform the search on a set of solutions and evolve them together are called population-based algorithms. This category includes methods like Genetic Algorithm, Ant Colony Optimization and Artificial Immune System.

Metahueritics have witnessed enhancements and improvements since their inception. As the latest development in metehuristics, hybrid metaheuristics have become more popular in the recent years since they take advantage of strengths of each of the individual components to better explore the search space. This hybridization includes the hybridization of population-based methods with trajectory methods, or hybridization of metahueristcs with optimization techniques.

5.2.2 Tabu Search

Tabu search was proposed independently by Glover (1986) and Hansen (1986), and has witnessed a continuous improvement since then. It has been successfully applied to a wide variety of problems and has produced remarkable results on hard combinatorial problems, such as quadratic programming (Merz & Freisleben, 2002), vehicle routing problems (Gendreau, Hertz, & Laporte, 1994; Taillard, Badeau, Gendreau, Guertin, & Potvin, 1997), and flow shop sequencing (Nowicki & Smutnicki, 1996).

Tabu search is based on the idea that intelligent problem solving must capitalize on the synergy of adaptive memory and responsive exploration. The emphasis on adaptive memory makes tabu search capable of exploiting strategies that mimic human problem solving skills. Having such an adaptive memory enables tabu search to search the solution space efficiently and effectively. Since local information gathered during the search forms a memory to guide the search, tabu search differs from local searches that do not take advantage of memory and thus depend only on semi-random processes that implement a form of sampling. Also, the emphasis on responsive exploration stems from the fact that a

bad strategic choice can often yield more information than a good random choice since the former is able to rectify its path and learn from the past but the later is unable to react to the new information.

To better see the difference between tabu search and a simple descent local search, let us assume that the goal is to minimize f(x) where $x \in X$ and the neighborhood of a given solution $x \in X$ is characterized by $N(x)$.

A simple descent method only allows moves to neighbor solutions that improve the current objective function value and it terminates the search when no improving solution can be found in the neighborhood of the current solution. The final x obtained by this method is indeed a local optimum, since it is at least as good as all the solutions seen so far.

Tabu search, on the other side, permits moves that may impair the current objective function value but the moves are chosen from a modified neighborhood $N^*(x) \subseteq N(x)$. Short term and long term memory structures are both playing roles in determining the specific composition of $N^*(x)$.

More specifically, short term memory is responsible to exclude certain elements of $N(x)$ to form $N^*(x)$. Long term memory, on the other hand, may expand $N^*(x)$ to include some solutions not directly found in $N(x)$ such as solutions found in the past history of the search that has been identified as high quality neighbors of these past solutions.

Tabu search, which extends the regular local search, has three main components:

- Search space and neighborhood structure;
- Tabu List; and
- Aspiration Criteria.

In the next few subsections, each of these components will be elaborated in more details.

Search space and neighborhood structure

The search space of tabu search is the set or collection of all possible solutions that can be considered during the search.

Closely related to the definition of the search space is that of neighborhood structure. If we denote the current solution by S, at each iteration of the tabu search, local transformations that can be applied on S produce a set of neighboring solutions denoted by $N(S)$ in the search space as the neighborhood of solution S.

Tabu List

A tabu list is one of the main distinctions of tabu search compared to the local search. The idea behind a tabu list is to prevent the search from returning back to where it came from and therefore prevent endless cycling from happening. This is achieved by declaring tabu moves that reverse the effect of recent moves. Tabu moves are usually stored in short term memory and the most commonly used form of implementing the tabu list is to prohibit reverse transformations from the current solution. In implementing the tabu list, one could record the complete solutions visited recently. Although this implementation is

accurate, it requires a lot of storage and may make the search expensive. Alternatively, one could record only the last few transformations that have happened on the current solution and add them to the tabu list to prohibit the reverse transformations.

Aspiration Criteria

While tabu lists are fundamental elements of tabu search, sometimes they are too restrictive and may prohibit attractive moves even when there is no danger of cycling. Therefore it is necessary to use algorithmic devices, called aspiration criteria, to override tabu lists. The simplest and probably most popular criterion is to allow a move listed in the tabu list if it leads to a solution with a better objective function than the currently best-known objective function.

5.3 A Simple Outline of Tabu Search Algorithm

Preliminary Steps

- **Find** an **initial solution**.
- **Set** the **best solution** to the initial solution and **set** the **best objective function value** based on the objective function value of the initial solution.
- **Set** the **initial tabu list** to **empty**.

While termination condition not reached **do**

- **Search** the allowable neighborhood of the current solution.
- **Find** the best solution in the allowable neighborhood.

- **Update** the best solution and best objective function value.
- **Form** the tabu list for the current solution.

End

5.4 Tabu search Implementation for solving the DAD problem

In this section, an application of tabu search in solving the DAD problem will be elaborated. First, we need to clearly define each component of the tabu search algorithm and then we outline the algorithm in a flowchart.

Solution Representation

Each feasible solution for the Defender's problem (network operator) is represented by a binary array of length n where n is the total number of terminals in the network. When a given cell i is filled with 1, the corresponding terminal, i.e. terminal i, will be defended. Therefore, the array contains m cells filled by 1 where m is the maximum number of terminals that the network operator can protect. The remaining $(n - m)$ cells in the solution array will be filled with 0.

Neighborhood Structure

At each iteration of the search, local transformations that can be applied on the current solution generate a set of neighborhood solutions in the search space. In this algorithm, the local transformation is defined as swapping the values of two cells when one cell contains one and the other contains zero. This type of transformation is called 1-swap and

is depicted in Figure 5-1 on a given solution array with 6 terminals ($n = 6$) and 3 defenses ($m = 3$). It should be noted that the total number of 1-swap movement on a solution array equals to $\binom{m}{1} * \binom{n-m}{1} = m * (n - m)$.

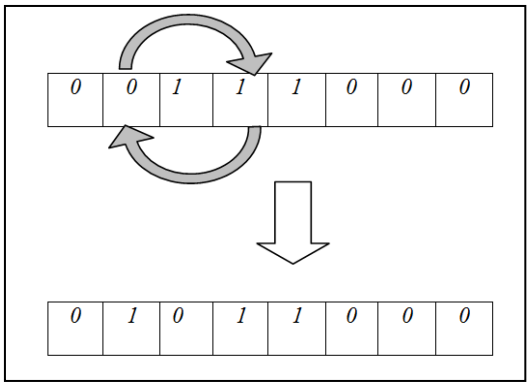

Figure 5-1: 1-swap movement

In the similar way, 2-swap transformation can be applied on a given solution in which two cells containing zero values will exchange their contents with two cells containing one values. Figure 5-2 shows an example of applying 2-swap transformation on a given solution. Also, the total number of 2-swap transformations on a solution array with n terminals and $(n - m)$ defended terminals equals to: $\binom{m}{2} * \binom{n-m}{2}$.

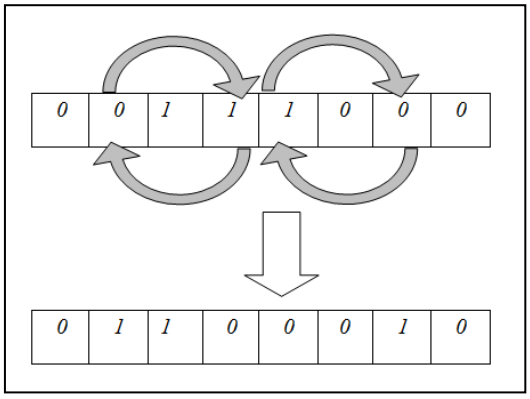

Figure 5-2: 2-swap movement

Tabu List

The tabu list contains information regarding the four recent swaps. Therefore, it is impossible to perform a swap operation between two cells if the reverse of that swap happened in the last four iterations of the algorithm. Also, it is important to note that when, at the end of an iteration, a swap is happening, the most recent swap is entering the list of tabu swaps and the oldest swap is exiting the tabu list and is not considered as a tabu swap any more. Therefore, we can think of the tabu list as a ***First in First out (FIFO)*** queue with the length of four in which with the entrance of a new swap the oldest swap leaves the queue. Figure 5-3 depicts the flow chart of the proposed tabu search. To fully understand this diagram, the following notation should be introduced.

N: Index of the number of iterations

I: Index of the number of iterations without improvement

S_0: The initial solution

S_c: The current solution

S_b: The best solution found in the neighborhood of S_c

At the beginning of the algorithm, both indexes are set at zero and the current solution is set at the initial solution. Also, maximum number of iterations is set at 10 and the maximum number of iterations without improvement is set at 4. Then, all the neighbors of the current solution will be analyzed and the best one will be selected. If the best neighbor

is improving the best solution found so far, then the search continues by increasing the index of number of iteration.

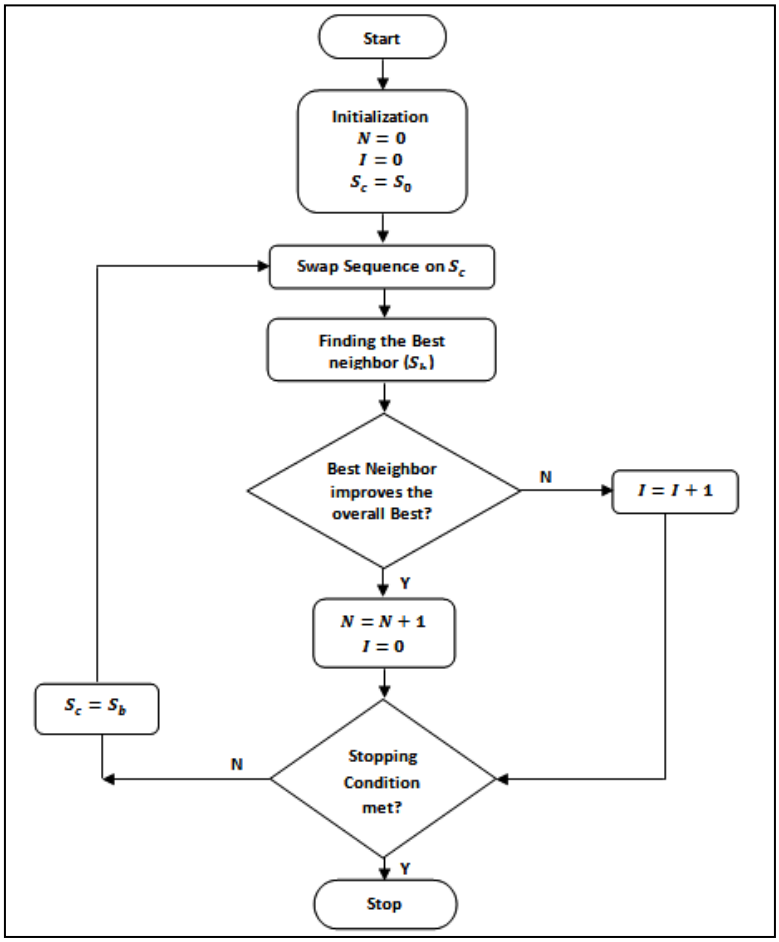

Figure 5-3: Flowchart of the proposed tabu search algorithm

Otherwise, the index of the number of iterations without improvement will be incremented. Following that, the stopping condition is checked. The search stops if either the number of iterations or the number of consecutive iterations without improvement reaches their pre-defined limits. If the search continues, the current solution will be replaced with the best solution found in the neighborhood of the previous iteration. In

other words, the current solution in each iteration, except for the first iteration, is the best solution found in the neighborhood of the previous current solution. The search continues until the stopping criteria are met. At the end, the best solution found so far will be reported as the output of this algorithm.

5.5 Numerical Analysis

In this section, we will pay attention to the results of solving the DAD model with the tabu search algorithm described in the previous section. To find the best setting, four different variants of the tabu search algorithm, depicted below, have been proposed and then coded in C# using CPLEX 12.6.0 concert technology on a PC with Core 2 Quad, 2.4 GHz processor with 4 GB of RAM. These variants are:

- **Variant 1**: In the first variant, the tabu search algorithm starts from a randomly generated solution. To generate the neighborhood of the current solution, 1-swap transformation is used.
- **Variant 2**: In the second variant, the tabu search algorithm begins with the output of the AD problem. In other words, the worst-case attack generated by the interdictor is the starting point of the tabu search algorithm. Then, a 1-swap transformation is used to generate the neighboring solutions.
- **Variant 3**: In the third variant, the tabu search algorithm begins with a random solution. The 2-swap transformation is used to generate the neighboring solutions.

- **Variant 4**: In the fourth variant, the tabu search algorithm begins with the output of the AD problem and the 2-swap transformation is employed to generate the neighboring solutions.

To compare the performances of these four variants of the tabu search algorithm, different instances of the DAD problem have been solved by these variants and the results have been analyzed according to their objective function values and the computation times. Also, to take into account the random starting point in both Variant 1 and Variant 3, each problem instance has been solved ten times by these two variants and the average objective function value and average computation time have been reported. Furthermore, it should be added here that at each of these ten runs, due to the randomness of the starting point, Variant 1 and Variant 3 may have similar starting points.

Table 5-2 shows the objective function values of solving the DAD problem for different problem instances (different number of attacked/defended terminals) by four distinct variants of the tabu search algorithm.

According to this table, all variants of the tabu search algorithm are capable of finding the optimal solution for different instances of the DAD problem and thus are quite effective and accurate.

Number of terminals		OFV found by Tabu Search			
Fortified	interdicted	Variant 1	Variant 2	Variant 3	Variant 4
1	*1*	12,620,928			
2	*2*	13,073,754			
3	*3*	12,746,283			
4	*4*	12,717,366			
5	*5*	12,744,060			
6	*6*	12,517,981			
7	*7*	12,236,503			
8	*8*	11,878,142			
9	*9*	11,598,194			

Table 5-2: Objective Function Values of Solutions Found by Four Variants of Tabu Search

Table 5-3 reveals the computational performance of these variants of the tabu search algorithm in solving different instances of the DAD problem.

According to Table 5-3, in comparing Variant 1 and Variant 2, both of which are based on 1-swap transformations, Variant 2 shows a much better computational performance. The reason why Variant 2 outperforms Variant 1 can be attributed to the fact that this variant of the tabu search is taking advantage of results of the AD model to start the search with. Although the output of the AD model is not the optimal solution for the DAD problem, it could be used as a good starting point.

Number of terminals		Computation Time of Tabu Search (Seconds)			
Fortified	**Interdicted**	**Variant 1**	**Variant 2**	**Variant 3**	**Variant 4**
1	*1*	13	11	15	12
2	*2*	210.3	42	759.2	42.9
3	*3*	424.3	209	3,501.7	3,031.5
4	*4*	968.5	379	7,620.3	3,858.4
5	*5*	1,174.2	324	7,613.6	3,395.7
6	*6*	1,724.0	407	8,126	4,551.6
7	*7*	1,669.8	906	11,664.5	5,549.2
8	*8*	2,144.1	917	29,601.2	7,240.9
9	*9*	3,270.9	1,668	40,256.62	12,680

Table 5-3: Computational Performance of Four Variants of Tabu Search

Also comparing Variant 3 and Variant 4, which both take advantage of 2-swap transformation, confirms that the output of the AD problem should be considered as a good starting point for the tabu search algorithm since Variant 4 outperforms Variant 3.

Examining the results of Variant 2 and Variant 4, which use the output of the AD model as the starting point but have different transformations to generate the neighborhood, makes it clear the extent to which the type of transformation can influence the computational performance. According to this table, while both Variants 2 and Variant 4 show almost the same performance on very small-scale problem instances, on larger instances, Variant 4 needs excessively longer computation time to find the optimal solution than Variant 2. This can be attributed to the fact that applying the 2-swap transformation produces more neighboring solutions than applying 1-swap transformation

and thus enlarges the size of the neighborhood at each iteration of the search. This makes 2-swap transformation less efficient than 1-swap transformation. The same trend is observable when comparing Variant 1 and Variant 3 and thus the 1-swap transformation is producing a better search space and is considered more efficient than the 2-swap transformation.

It should be concluded from this table that using the output of the AD problem, as the starting point, and having 1-swap transformation, to produce the neighborhood, are improving the performance of tabu search and thus V***ariant 2*** which benefits from both of these two factors should be considered as ***the optimal design*** of the tabu search in solving the DAD problem.

5.6 Insights

Comparing the results of Table 5-3 and Table 4-4 is very informative. It reveals that Variant 2, as the optimal design of tabu search, is a viable and efficient solution technique for solving big instances of the DAD problem. More specifically, for small instances, i.e. 4 attacks/defenses or fewer, the decomposition technique proposed in the previous chapter is performing better and should be considered as an efficient solution technique. This can be attributed to the fact that, in these small instances, the proposed decomposition-based technique produces fewer numbers of intermediate nodes and therefore is quite efficient for tackling problems of these sizes. On the other hand, for large problem instances, Variant 2 of the tabu search is performing much better than the decomposition-based solution technique and should be deemed as the dominant solution

technique for large problem instances. Consequently, depending on the number of attacks/defenses, the appropriate solution technique for solving the DAD problem can be identified such that for problems with ***relatively few attacks/defenses***, four or fewer , the proposed ***decomposition-based heuristic*** should be selected and for ***problems with more than four attacks/defenses***, V***ariant 2*** of the proposed tabu search should be picked.

5.7 Conclusion

In this chapter, a tabu search algorithm for solving the DAD problem has been introduced. The results of solving the DAD problem with this algorithm prove the competency of this algorithm in dealing with large-scale instances of such a difficult problem.

Chapter 6: Conclusion and Future Research

6.1 Conclusion

Despite the practical importance of rail-truck intermodal transportation, the research on this type of transportation is still in its infancy. In this dissertation, we proposed a set of models to improve the performance of this type of transportation in the wake of worst-case disruptions. In particular, each chapter of this dissertation plays an important role is attaining this objective.

In Chapter Two, the basic mathematical model for defending rail-truck intermodal transportation is put forward. Then, two small instances of the proposed model were applied to a realistic network of Norfolk Southern, a Class I railroad company in the US, and were solved by using CPLEX. The results indicate the effectiveness of having a sound fortification plan to hedge against worst-case attacks.

In Chapter Three, the basic model developed in Chapter Two was expanded. Also, a heuristic solution technique-based on the traffic flow information was proposed. The traffic-based heuristic proved to be an appropriate solution technique, in terms of efficiency and quality of solutions, in solving small-scale problems of fortification planning in the Norfolk Southern network.

In Chapter Four, a heuristic solution technique based on decomposition was proposed. In the first stage of this heuristic, the implicit enumeration (Scaparra and Church, 2008a) is used to break the DAD problem into a set of AD subproblems. In the second stage, each of the AD problems generated in the first stage is solved using a Bender's decomposition

approach. The Bender's decomposition approach for solving AD subroblems is quite efficient and is able to produce high quality results. Also, the decomposition based heuristic is able to solve DAD problems and yielding high quality solutions in a reasonable amount of time.

In Chapter Five, an efficient tabu search-based solution technique for solving DAD problems is introduced which is able to further improve the performance of the decomposition-based heuristic, developed in Chapter Four, especially in large-scale problem instances. Different variants for the tabu search-based heuristic, like the initial solution and the neighborhood structure, are compared. According to extensive experiments, it is determined that the tabu search heuristic that uses the result of the AD subproblem, as the initial solution, and takes advantage of 1-swap transformation, as the neighborhood structure, outperforms the other variants and thus should be considered in solving large instances of the DAD problem. Furthermore, depending on the size of the problem instance, the decomposition based heuristic, developed in Chapter Four, or the tabu search, developed in Chapter Five, should be used in solving the DAD problem instances.

6.2 Future Directions

The following suggestions will help improve applicability of this dissertation.

6.2.1 Network Design Considerations

The network operator is responsible for long terms decisions. In addition to protection planning, the network operator will be responsible for designing the network. More

specifically, the network operator could decide about the initial capacity of terminals and available services while both of them were assumed to be given in this thesis.

Terminal capacities could be endogenous to the model such that the initial allocation of capacity is performed to ensure that the remaining network always has enough capacity to meet the demand in the aftermath of disruptions.

Design of intermodal train services which is called service network design (Crainic, 2000) could be decided such that the network always keeps a certain amount of connectivity following interdictions. This reduces the need for the high-cost trucking system and therefore reduces the cost imposed to the transportation system.

To add more realism to the current DAD model, empty container distribution (Dejax & Crainic, 1987) on the network could also be integrated into the model. In the current model, we assumed that empty cars are always available in shippers/receivers locations. But, due to the imbalance on the demand, this may not be true and therefore, the network operator has to deliberately make a plan to deliver empty containers to the customers.

Obviously, adding these two important network design aspects to the network operator's responsibilities improves the quality of service for the customers on the demand side. However, this augmentation comes with the cost of increasing the size and the complexity of the current DAD model. For example, adding the capacity allocation problem to the network operator makes the DAD model a nonlinear mixed integer program which is inherently more difficult than the current mixed integer DAD model.

6.2.2 Uncertainty and Asymmetric Information

The current model can be augmented by adding uncertainty elements into different aspects of decision making. This suggestion is motivated by the fact that in reality the players may not have access to all the information they would need, especially about what the other players are opt to, and thus the symmetry of information may not be hold. Thus, developing models to work with asymmetric information is of high practical importance. For instance, the network operator may not know the exact number or the magnitude of attacks in advance. Thus, the operator may have to work with respective probability distributions to safeguard the network against the expected number of attacks or against expected magnitude of attacks.

Also, the success of attack and defense actions may not be guaranteed such that a given attack is successful with a certain probability or, in the same way, a given defense is successful with a certain probability.

6.2.3 Random Attacks

Instead of defending the system against worst-case attacks, we could consider defending the system against random attacks. The idea is that instead of safeguarding against unlikely worst-case attacks, it’s good to be prepared for high probability random disruptions in the system. Ideally, it is appropriate to be prepared for both kinds of disruptions, i.e. random and worst-case; at the same time which has been called the all-hazard approach by Zhuang and Bier (2007).

Embracing random disruptions, either instead of or together with worst-case ones, needs fundamental changes in the way the interdictor operates. Obviously, this will create more reasonable and realistic results but requires more computational changes as well.

6.2.4 Efficient Solution Methods for the Intermodal Operator's Problem

The intermodal operators' problem, or the inner-most problem, is a capacitated multi-commodity network flow problem with train frequency variables and is currently solved using the CPLEX solver.

Preliminary investigations showed that solving the intermodal operator's problem for a larger data set is very difficult and challenging for CPLEX. Therefore, new solution techniques, including heuristic ones, should be considered in solving the intermodal operator's problem for large scale instances. For instance, Benders decomposition (Benders, 1962) or dual-ascent methods (Barnhart, 1993) could be considered to solve the intermodal operator's problem in a more efficient way.

Solving the intermodal operator's problem more efficiently also enables a deeper evaluation of the efficiency of the proposed decomposition technique and the proposed tabu search since it allows solving a larger data set by them. This will reveal more insights about the weaknesses and strengths of these techniques.

References

AAR. (2014). Rail time indicators. Association of American Railroads- Policy and Economics Department. June 2014.

AAR. (2015). Rail Intermodal Keeps America Moving. Association of American Railroads- Policy and Economics Department. January 2015.

Aksen, D., Piyade, N., & Aras, N. (2010). The budget constrained r-interdiction median problem with capacity expansion. *Central European Journal of Operations Research*, *18*(3), 269-291.

Aksen, D., Aras, N., & Piyade, N. (2013). A bilevel p-median model for the planning and protection of critical facilities. *Journal of Heuristics*, *19*(2), 373-398.

Altay, N., and Green, W. G. (2006). OR/MS research in disaster operations management. *European Journal of Operational Research*, *175*(1), 475-493.

Assad, A. A. (1980). Models for rail transportation. *Transportation Research Part A: General*, *14*(3), 205-220.

Barnhart, C. (1993). Dual-ascent methods for large-scale multicommodity flow problems. *Naval Research Logistics (NRL)*, *40*(3), 305-324.

Benders, J. F. (1962). Partitioning procedures for solving mixed-variables programming problems. *Numerische mathematik*, *4*(1), 238-252.

Berman, O., Krass, D., & Menezes, M. B. (2007). Facility reliability issues in network p-median problems: Strategic centralization and co-location effects. *Operations Research*, *55*(2), 332-350.

Bräysy, O., & Gendreau, M. (2005). Vehicle routing problem with time windows, Part I: Route construction and local search algorithms. *Transportation science*, *39*(1), 104-118.

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *Tutorials in Operations Research: Emerging Theory, Methods, and Applications*, 102-123.

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

Bryan, J., Weisbrod, G., & Martland, C. D. (2007). Rail freight as a means of reducing roadway congestion: Feasibility considerations for transportation planning. Transportation Research Record: Journal of the Transportation Research Board, 2008(1), 75-83.

Buffy Rojas. (February 28, 2006). WalMart: Beyond Business Continuity Basics. In Continuity Insights. Retrieved March 2, 2013, from http://www.continuityinsights.com/articles/2006/02/walmart-beyond-business-continuity-basics.

Chopra, S., & Sodhi, M. S. (2012). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review (Fall 2004)*.

Church, R. L., Scaparra, M. P., & Middleton, R. S. (2004). Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers*, *94*(3), 491-502.

Church, R. L., & Scaparra, M. P. (2007). Protecting critical assets: the r-interdiction median problem with fortification. *Geographical Analysis*, *39*(2), 129-146.

Cormican, K. J., Morton, D. P., & Wood, R. K. (1998). Stochastic network interdiction. *Operations Research*, *46*(2), 184-197.

Crainic, T. G. (2000). Service network design in freight transportation. *European Journal of Operational Research*, *122*(2), 272-288.

Dejax, P. J., & Crainic, T. G. (1987). Survey paper-a review of empty flows and fleet management models in freight transportation. *Transportation Science*, *21*(4), 227-248.

ESRI, 2008. ArcView Geographical Information System: An ESRI product. http://www.esri.com

Evers, P. T., Harper, D. V., & Needham, P. M. (1996). The determinants of shipper perceptions of modes. *Transportation Journal*, *36*(2), 13-25.

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

Gabriel, S. A., Shim, Y., Conejo, A. J., de la Torre, S., & García-Bertrand, R. (2010). A Benders decomposition method for discretely-constrained mathematical programs with equilibrium constraints. Journal of the Operational Research Society, 61(9), 1404-1419.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems*. Butterworth-Heinemann.

Gendreau, M. (2003) An Introduction to Tabu Search", forthcoming in Handbook of Metaheuristics, F. Glover and G. Kochenberger (eds), *Kluwer*.

Gendreau, M., Hertz, A., & Laporte, G. (1994). A tabu search heuristic for the vehicle routing problem. *Management science*, *40*(10), 1276-1290.

Glover, F. (1986). Future paths for integer programming and links to artificial intelligence. *Computers & operations research*, *13*(5), 533-549.

Golden, B. (1978). A problem in network interdiction. *Naval Research Logistics Quarterly*, *25*(4), 711-713.

Grotschel, M., Monma, C. L., & Stoer, M. (1995). Design of survivable networks. *Handbooks in Operations Research and Management Science*, *7*, 617-672.

Grubesic, T. H., O'Kelly, M. E., & Murray, A. T. (2003). A geographic perspective on commercial Internet survivability. *Telematics and Informatics*, *20*(1), 51-69.

Haghani, A. E. (1989). Formulation and solution of a combined train routing and makeup, and empty car distribution model. *Transportation Research Part B: Methodological*, *23*(6), 433-452.

Hansen, P. (1986, March). The steepest ascent mildest descent heuristic for combinatorial programming. In *Congress on numerical methods in combinatorial optimization, Capri, Italy* (pp. 70-145).

Harper, D. V., & Evers, P. T. (1993). Competitive issues in intermodal railroad-truck service. *Transportation Journal*, *32*(3), 31-45.

IBM. (2014). CPLEX, Version 12.6.0. <http://www.ibm.org>

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

Jennings Barton E., Holcomb Mary C. (2007). The role and impact of rail truck intermodalism on efficient and effective transportation, Part 1, Logistics Quarterly, pp. 26-27 (available at: http://www.logisticsquarterly.com/issues/13-1/article2.html) (accessed on 26 September 2014)

Jeroslow, R. G. (1985). The polynomial hierarchy and a simple model for competitive analysis, Math. Programming, 32, 146–164

Kerivin, H., and Mahjoub, A. R. (2005). Design of survivable networks: A survey. *Networks*, *46*(1), 1-21.

Kim, N. S., & Van Wee, B. (2014). Toward a Better Methodology for Assessing CO2 Emissions for Intermodal and Truck-only Freight Systems: A European Case Study. International Journal of Sustainable Transportation, 8(3), 177-201.

Kumamoto, H., Henley, E. J. (1996). Probabilistic risk assessment and management for engineers and scientists.

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 & Operations Research*, *38*(1), 357-366.

Liberatore, F., Scaparra, M. P., & Daskin, M. S. (2012). Hedging against disruptions with ripple effects in location analysis. *Omega*, *40*(1), 21-30.

Lim, C., & Smith, J. C. (2007). Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions*, *39*(1), 15-26.

Losada, C., Scaparra, M. P., Church, R. L., & Daskin, M. S. (2012). The stochastic interdiction median problem with disruption intensity levels. *Annals of Operations Research*, *201*(1), 345-365.

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.

Macharis, C., & Bontekoning, Y. M. (2004). Opportunities for OR in intermodal freight transport research: A review. *European Journal of Operational Research*, *153*(2), 400-416.

Malik, K., Mittal, A. K., & Gupta, S. K. (1989). The k most vital arcs in the shortest path problem. *Operations Research Letters*, *8*(4), 223-227.

Merz, P., & Freisleben, B. (2002). Greedy and local search heuristics for unconstrained binary quadratic programming. *Journal of Heuristics*, *8*(2), 197-213.

Morlok, E. K., & Spasovic, L. N. (1994, August). Approaches to improving drayage in rail-truck intermodal service. In *TransTech Conference, 1995. Proceedings, 1995 Pacific Rim* (pp. 74-80). IEEE.

Mosleh, A., Bier, V. M., Apostolakis, G. (1988). A critique of current practice for the use of expert opinions in probabilistic risk assessment. *Reliability Engineering & System Safety*, *20*(1), 63-85.

Mouawad, J. (2005). Katrina's shock to the system. *New York Times*, *4*.

Murphy, P. R., & Hall, P. K. (1995). The relative importance of cost and service in freight transportation choice before and after deregulation: an update. *Transportation Journal*, *35*(1), 30-38.

NEHRP - National Earthquake Hazards Reduction Program, Introduction to emergency management.http://training.fema.gov/EMIWeb/EarthQuake/NEH0101220.htm (November 1, 2009).

Nowicki, E., & Smutnicki, C. (1996). A fast tabu search algorithm for the permutation flow-shop problem. *European Journal of Operational Research*, *91*(1), 160-175.

Nozick, L. K., & Morlok, E. K. (1997). A model for medium-term operations planning in an intermodal rail-truck service. *Transportation research part a: policy and practice*, *31*(2), 91-107.

O'Hanley, J. R., & Church, R. L. (2011). Designing robust coverage networks to hedge against worst-case facility losses. *European Journal of Operational Research*, *209*(1), 23-36.

Peng, P., Snyder, L. V., Lim, A., & Liu, Z. (2011). Reliable logistics networks design with facility disruptions. *Transportation Research Part B: Methodological*, *45*(8), 1190-1211.

RPM, 2014. Railroad Performance Measures. <http://www.railroadpm.org>. Accessed May 20, 2014.

Ratliff, H. D., Sicilia, G. T., & Lubore, S. H. (1975). Finding the n most vital links in flow networks. *Management Science, 21*(5), 531-539.

Rice, J. B., & Caniato, F. (2003). Building a Secure and Resilient Supply Network. *Supply Chain Management Review, V. 7, NO. 5 (Sep./Oct. 2003), P. 22-30: ILL*.

Scaparra, M. P., Church, R. L. (2008a). A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research,35*(6), 1905-1923.

Scaparra, M. P., Church, R. L. (2008b). An exact solution approach for the interdiction median problem with fortification. *European Journal of Operational Research, 189*(1), 76-92.

Scaparra, M. P., & Church, R. (2012). Protecting Supply Systems to Mitigate Potential Disaster A Model to Fortify Capacitated Facilities. *International Regional Science Review, 35*(2), 188-210.

Snyder, L. V., & Daskin, M. S. (2005). Reliability models for facility location: the expected failure cost case. *Transportation Science, 39*(3), 400-416.

Snyder, L. V., Scaparra, M. P., Daskin, M. S., & Church, R. L. (2006). Planning for disruptions in supply chain networks. *Tutorials in operations research*.

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

Taillard, É., Badeau, P., Gendreau, M., Guertin, F., & Potvin, J. Y. (1997). A tabu search heuristic for the vehicle routing problem with soft time windows. *Transportation science, 31*(2), 170-186.

Tufekci, S., & Wallace, W. (1998). Emerging area of emergency management and engineering. *IEEE Transactions on Engineering Management, 45*(2), 103-105.

US DOT (2010) Research and innovative technology administration: bureau of transportation statistics. ttp://www.bts.gov/publications/national_transportation_statistics. Accessed 3 December 2010

US DHS (2014) Department of homeland security. http://www.dhs.gov/what-critical-infrastructure. Accessed 26 August 2014

Verma, M., Verter, V., & Zufferey, N. (2012). A bi-objective model for planning and managing rail-truck intermodal transportation of hazardous materials. *Transportation research part E: logistics and transportation review*, *48*(1), 132-149.

Verma, M., & Verter, V. (2010). A lead-time based approach for planning rail–truck intermodal transportation of dangerous goods. *European Journal of Operational Research*, *202*(3), 696-706.

Whiteman, B., & Philip, S. (1999). Improving single strike effectiveness for network interdiction. *Military Operations Research*, *4*(4), 15-30.

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

Wolsey, L. A. (1998). *Integer programming* (Vol. 42). New York: Wiley.

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

Wood, R. K. (2011). Bilevel network interdiction models: Formulations and solutions. *Wiley Encyclopedia of Operations Research and Management Science*.

Wright, P. D., Liberatore, M. J., & Nydick, R. L. (2006). A survey of operations research models and applications in homeland security. *Interfaces*, *36*(6), 514-529.

Zhang, X., Zheng, Z., Zhu, Y., & Cai, K. Y. (2014). Protection issues for supply systems involving random attacks. Computers & Operations Research, 43, 137-156.

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.

Zhuang, J., & Bier, V. M. (2007). Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. Operations Research, 55(5), 976-991.

Appendix A: Defined Train Services on the Network

Service Number	Origin	Destination	Intermediate Stop(s)
1	Atlanta	Detroit	Knoxville
2	Atlanta	New York	Knoxville
3	Atlanta	Philadelphia	Charlotte, Richmond
4	Charlotte	Chicago	Indianapolis
5	Charlotte	Detroit	Columbus
6	Charlotte	New York	-
7	Chicago	Charlotte	Indianapolis, Cincinnati
8	Chicago	Jacksonville	Indianapolis, Atlanta
9	Chicago	New York	-
10	Chicago	Philadelphia	Pittsburg
11	Cincinnati	Jacksonville	Knoxville, Atlanta, Macon
12	Columbus	Norfolk	Pittsburgh
13	Detroit	New York	Columbus
14	Detroit	Philadelphia	Cleveland, Pittsburgh
15	Indianapolis	Atlanta	-
16	Indianapolis	New York	Cleveland
17	Indianapolis	Philadelphia	Columbus, Pittsburgh
18	Jacksonville	Chicago	Atlanta, Indianapolis
19	Jacksonville	Philadelphia	Richmond
20	Columbus	Philadelphia	Pittsburgh
21	New York	Atlanta	Roanoke, Knoxville
22	New York	Charlotte	Richmond
23	New York	Chicago	Cleveland, Fort Wayne
24	New York	Detroit	Columbus
25	New York	Indianapolis	Pittsburgh, Columbus
26	Philadelphia	Atlanta	Roanoke, Knoxville
27	Philadelphia	Chicago	Columbus, Fort Wayne
28	Philadelphia	Detroit	Pittsburgh, Cleveland
29	Philadelphia	Indianapolis	Cleveland, Columbus
30	Philadelphia	Jacksonville	Richmond
31	Philadelphia	Memphis	Roanoke

Appendix B

Defended Terminal	Attacked Terminal	Resulting Cost ($)
1	Chicago	11620650
2	Fort Wayne	10922063
3	Detroit	10957771
4	Cleveland	10833657
5	New York	10924925
6	Indianapolis	11906369
7	Columbus	11130345
8	Pittsburgh	11257889
9	Philadelphia	12263378
10	Cincinnati	10912389
11	Roanoke	10833657
12	Richmond	11645654
13	Norfolk	10942267
14	Knoxville	10965458
15	Charlotte	11515479
16	Atlanta	12641578
17	Macon	10834852
18	Jacksonville	11437338

Appendix C

Defended Terminal	Attacked Terminals	Resulting Cost ($)
1	Chicago, Fort Wayne	11497305
2	Chicago, Detroit	11697341
3	Chicago, Cleveland	11437820
4	Chicago, New York	11480154
5	Chicago, Indianapolis	13016982
6	Chicago, Columbus	11622864
7	Chicago, Pittsburgh	11671667
8	Chicago, Philadelphia	12771238
9	Chicago, Cincinnati	11486950
10	Chicago, Roanoke	11590971
11	Chicago, Richmond	12230896
12	Chicago, Norfolk	11516827
13	Chicago, Knoxville	11547768
14	Chicago, Charlotte	11922874
15	Chicago, Atlanta	13105000
16	Chicago, Macon	11409413
17	Chicago, Jacksonville	11895539
19	Fort Wayne, Detroit	10837946
19	Fort Wayne ,Cleveland	10739310
20	Fort Wayne, New York	10781656
21	Fort Wayne ,Indianapolis	11829614
22	Fort Wayne, Columbus	10920713
23	Fort Wayne ,Pittsburgh	11004526
24	Fort Wayne, Philadelphia	12097796
25	Fort Wayne, Cincinnati	10785805
26	Fort Wayne, Roanoke	10889826
27	Fort Wayne, Richmond	11530177
28	Fort Wayne, Norfolk	10815736
29	Fort Wayne, Knoxville	10845397
30	Fort Wayne, Charlotte	11368210
31	Fort Wayne, Atlanta	12633231
32	Fort Wayne, Macon	10708268
33	Fort Wayne, Jacksonville	11307913
34	Detroit, Cleveland	10775018
35	Detroit, New York	10823771
36	Detroit, Indianapolis	11790404
37	Detroit, Columbus	10962754
38	Detroit, Pittsburgh	11023391
39	Detroit, Philadelphia	12153466
40	Detroit, Cincinnati	10822129

41	Detroit, Roanoke	10926150
42	Detroit, Richmond	11566075
43	Detroit, Norfolk	10852022
44	Detroit, Knoxville	10873689
45	Detroit, Charlotte	11405170
46	Detroit, Atlanta	12597366
47	Detroit, Macon	10744592
48	Detroit, Jacksonville	11337900
49	Cleveland, New York	10721487
50	Cleveland, Indianapolis	11723616
51	Cleveland, Columbus	10947592
52	Cleveland, Pittsburgh	11075136
53	Cleveland, Philadelphia	12086612
54	Cleveland, Cincinnati	10729636
55	Cleveland, Roanoke	10833657
56	Cleveland, Richmond	11473582
57	Cleveland, Norfolk	10759513
58	Cleveland, Knoxville	10789227
59	Cleveland, Charlotte	11312041
60	Cleveland, Atlanta	12578167
61	Cleveland, Macon	10652099
62	Cleveland, Jacksonville	11251744
63	New York, Indianapolis	11743681
64	New York, Columbus	10908655
65	New York, Pittsburgh	10975388
66	New York, Philadelphia	13906575
67	New York, Cincinnati	10771683
68	New York, Roanoke	10896389
69	New York, Richmond	11482407
70	New York, Norfolk	10801560
71	New York, Knoxville	10809952
72	New York, Charlotte	11405490
73	New York, Atlanta	12647001
74	New York, Macon	10694146
75	New York, Jacksonville	11289176
76	Indianapolis, Columbus	11862696
77	Indianapolis, Pittsburgh	11813444
78	Indianapolis, Philadelphia	12931394
79	Indianapolis, Cincinnati	11801447
80	Indianapolis, Roanoke	11851345
81	Indianapolis, Richmond	12489059
82	Indianapolis, Norfolk	11777202
83	Indianapolis, Knoxville	11805689
84	Indianapolis, Charlotte	12222763
85	Indianapolis, Atlanta	13444974

86	Indianapolis, Macon	11669787
87	Indianapolis, Jacksonville	12193394
88	Columbus, Pittsburgh	11173583
89	Columbus, Philadelphia	12231529
90	Columbus, Cincinnati	10899648
91	Columbus, Roanoke	11003669
92	Columbus, Richmond	11643594
93	Columbus, Norfolk	10857559
94	Columbus, Knoxville	10959079
95	Columbus, Charlotte	11467288
96	Columbus, Atlanta	12747663
97	Columbus, Macon	10822111
98	Columbus, Jacksonville	11421755
99	Pittsburgh, Philadelphia	12328966
100	Pittsburgh, Cincinnati	10982105
101	Pittsburgh, Roanoke	11086126
102	Pittsburgh, Richmond	11726051
103	Pittsburgh, Norfolk	10977008
104	Pittsburgh, Knoxville	11041696
105	Pittsburgh, Charlotte	11560822
106	Pittsburgh, Atlanta	12817200
107	Pittsburgh, Macon	10904568
108	Pittsburgh, Jacksonville	11504213
109	Philadelphia, Cincinnati	12118403
110	Philadelphia, Roanoke	12216560
111	Philadelphia, Richmond	12734222
112	Philadelphia, Norfolk	12148403
113	Philadelphia, Knoxville	12164237
114	Philadelphia, Charlotte	12653748
115	Philadelphia, Atlanta	13626754
116	Philadelphia, Macon	12040937
117	Philadelphia, Jacksonville	12376534
118	Cincinnati, Roanoke	10874008
119	Cincinnati, Richmond	11513934
120	Cincinnati, Norfolk	10799918
121	Cincinnati, Knoxville	10827772
122	Cincinnati, Charlotte	11352392
123	Cincinnati, Atlanta	12605569
124	Cincinnati, Macon	10691255
125	Cincinnati, Jacksonville	11292095
126	Roanoke, Richmond	11607273
127	Roanoke, Norfolk	10903939
128	Roanoke, Knoxville	10927077
129	Roanoke, Charlotte	11477098
130	Roanoke, Atlanta	12602092

131	Roanoke, Macon	10796471
132	Roanoke, Jacksonville	11399010
133	Richmond, Norfolk	11543864
134	Richmond, Knoxville	11564054
135	Richmond, Charlotte	12034687
136	Richmond, Atlanta	12910642
137	Richmond, Macon	11436397
138	Richmond, Jacksonville	11853388
139	Norfolk, Knoxville	10859673
140	Norfolk, Charlotte	11382323
141	Norfolk, Atlanta	12647291
142	Norfolk, Macon	10722381
143	Norfolk, Jacksonville	11322026
144	Knoxville, Charlotte	11510000
145	Knoxville, Atlanta	12850683
146	Knoxville, Macon	10752042
147	Knoxville, Jacksonville	11350460
148	Charlotte, Atlanta	13255074
149	Charlotte, Macon	11274855
150	Charlotte, Jacksonville	11860872
151	Atlanta, Macon	12583258
152	Atlanta, Jacksonville	13120304
153	Macon, Jacksonville	11237401