

MACK-BLACKWELL

Rural Transportation Center

University of Arkansas
4190 Bell Engineering Center
Fayetteville, AR 72701
479.575.6026 – Office
479.575.7168 - Fax



Models for Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks MBTC DHS 1109

Student Researchers:

Orkun Baycik, B.S.
Julianna Bright, M.S.
Jessica Spicer, M.S.
Dia St. John, M.S.
Jessica Spicer, M.S.
Morgan Ulesich, B.S.
Taylor Kitchens, B.S.

Faculty Researchers:

Scott Mason, Ph.D.
Ashlea Bennett Milburn, Ph.D.
Edward A. Pohl, Ph.D.
Chase Rainwater, Ph.D.



Prepared for
Mack-Blackwell Rural Transportation Center
National Transportation Security Center of Excellence
University of Arkansas

ACKNOWLEDGEMENT

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2008-ST-061-TS003.

DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Table of Contents

<u>1</u>	<u>Introduction and Motivation</u>	2
<u>2</u>	<u>Literature Review</u>	4
2.1	<u>Inland Waterways</u>	4
2.2	<u>Supply Chain Risk and Resiliency</u>	7
2.3	<u>Supply Chain Disruption Models</u>	10
2.3.1	<i>Network Interdiction Models</i>	10
2.3.2	<i>Network Fortification Models</i>	11
2.3.3	<i>Post-fortification Fallibility</i>	12
2.3.4	<i>Dynamic Network Models</i>	14
2.4	<u>Perishability</u>	15
2.5	<u>Bi-level Network Design</u>	16
2.6	<u>Coevolutionary Algorithms</u>	19
<u>3</u>	<u>Mathematical Modeling Approaches</u>	20
3.1	<u>Multi-period p-median fortification model with post-fortification fallibility</u>	20
3.2	<u>Multi-period minimum cost network flow model with fortification</u>	22
3.3	<u>Tactical Risk Mitigation in a Perishable Commodity Supply Chain</u>	25
3.4	<u>Bi-Level Model</u>	31
3.5	<u>Tactical Risk Mitigation for Adaptive Adversaries</u>	38
3.6	<u>Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks</u>	42
<u>4</u>	<u>Model Analysis</u>	48
<u>5</u>	<u>Conclusions and Future Work</u>	49
	<u>Appendix A. Reliable Network Interdiction-Fortification Problem for Inland Waterways</u>	57
	<u>Appendix B. Student Poster Presentations from Conferences</u>	80
	<u>Appendix C. ISERC Presentations Slides</u>	83

1 Introduction and Motivation

Large-scale supply chain disruptions such as natural disasters, terrorist attacks, and transportation network failures can dramatically reduce supply chain effectiveness and result in significant economic loss. When items are delayed during transit due to a supply chain disruption, downstream factories may be without needed raw materials, increasing the likelihood that downstream warehouses and retailers may experience stockouts. When the items in transit are perishable, an additional level of concern is introduced, as items that spoil or degrade in quality can result in an even greater economic loss.

Events of this century, such as the 9/11 terrorist attacks, hurricane Katrina, and the 2002 West Coast port closures, have motivated the need for new supply chain models and decision support tools that consider the risks associated with such disruptions. The risk profile of a supply chain depends largely on the configuration of its transportation infrastructure components. Fortifying (securing) these components can increase the resiliency of a supply chain, where resiliency is defined as the ability of the system to return to an appropriate level of performance after disruption. Fortification investments specific to transportation infrastructure components can include increasing redundancy in the network via alternate paths or routes or facilities and improving the structural integrity of existing components (e.g., incorporating blast-resistant and/or earthquake-resistant materials). Unfortunately, such investments are expensive and fortification resources often are scarce.

Developing models to prioritize the allocation of scarce fortification resources and maximize network resiliency requires knowledge of both the likelihood and the magnitude of each disruption that the investments are intended to protect against. They also require knowledge of the cost of alternate fortification strategies, as well as the network resiliency that would result from employing each alternate strategy.

Determining the set of possible supply chain disruptions and their likelihoods of occurrence is difficult—this difficulty is further compounded by the fact that decision makers often have an imprecise understanding of the adversary trying to disrupt their supply chain, including his overarching goal or objective. For example, consider a terrorist as the adversary. His objective may either be 1) to damage network infrastructure component(s) that would cause the greatest economic loss, or 2) to damage the component(s) that are easiest or cheapest to

target. Accomplishing these two separate objectives may require an adversary to carry out very different sets of actions. Furthermore, we conjecture that an adversary's target is likely to change in response to the decision maker's fortification investments. Therefore decisions should be made that mitigate both present and future risk.

Finally, there are a number of circumstances in which a network's adversary has no known motivations, such as natural disasters. In these cases, while the occurrence of the disruption is random, it is subject to probability distributions that depend, for example, on geographies and weather patterns. The consideration of such random events complicates fortification efforts further due to the lack of a known adversarial objective to guide investment decision-making.

This project focuses on the development of mathematical models that maximize network resiliency when allocating scarce fortification resources for transportation infrastructure components in perishable commodity supply chain networks. Our assessment of supply chain risk is from an all-hazards perspective, wherein potential disruptions include both unplanned (i.e., natural disasters) and planned, albeit dynamically changing, adversarial actions (i.e., an adversary with an adaptive, evolving objective).

This project is differentiated from other research by its focus on inland waterway supply chains for perishable commodities. An additional distinguishing factor is that most previous research assumed disruptions were caused by an adversary whose objective was to maximize network disruption. Our modeling efforts attempt to account for all-hazard disruption scenarios to mitigate dynamic risk caused by an adversary with an unknown, adaptive objective.

Our implementation efforts focus on bulk transportation of corn on inland waterways in the United States. Ninety percent of U.S. corn that is destined for export travels via barge to the Gulf of Mexico using the Mississippi River system (Frittelli, 2005). Corn is a perishable commodity that will quickly degrade in quality if it is subjected to moisture or high temperatures during transport (Sinha and Muir, 1973). If corn degrades in quality, it may need to be sold at a reduced price, or be discarded altogether if it spoils. Thus, the economic impact of disruptions to the bulk corn supply chain can include spoilage costs in addition to delay costs experienced by downstream factories, warehouses, and retailers who need corn and/or corn by-products as inputs to their own processes. Events such as river locks being destroyed or damaged can significantly

delay barge traffic. Thus, the fortification actions that we consider include 1) improving the structural integrity of existing locks, dams and major bridges and 2) constructing alternate intermodal routes between existing supply chain nodes.

Our project is divided into three modeling phases. Phase I, focuses on models that allocate resources to waterway infrastructure components to increase resiliency when disruptions are caused by natural disasters. Phase II considers disruptions caused by an adversary with a known objective, and Phase III explores the formulation of models that incorporates the effects of an unknown adversarial objective.

2 Literature Review

2.1 Inland Waterways

The 25,000 miles of navigable inland waterways in the United States provide a cost-effective way to move more than 630 million tons of cargo by barge each year (Inland Waterway Navigation, 2009). Figure 1 illustrates the North American inland and intracoastal network. The barges move bulk commodities and raw materials such as coal, petroleum, grain, stone, gravel, fertilizer and steel. Figure 2 provides a break-out of the share by commodity of the 627 million tons of cargo moved by barge in 2006 (Inland Waterway Navigation, 2009). More than 60 percent of farm exports move on the inland waterways to downstream ports for export. The largest of these is grain with approximately 80 million tons moving by barge each year (Inland Waterway Navigation, 2009). The inland waterways provide the most economically and environmentally sound mode of transportation for moving goods and commodities. A single barge carries approximately 58 times more cargo than a tractor trailer and fifteen times more cargo than railcars, illustrated in Figure 3 (Inland Waterway Navigation, 2000). Figure 4 provides a fuel efficiency comparison for the various modes of freight transportation.

The Army Corps of Engineers maintains 12,000 miles of commercially-important navigable rivers. This segment includes 191 commercially active lock sites with 237 operable lock chambers. These locks and chambers provide essential infrastructure needed to move barges inland. They are especially vulnerable to attack, natural disaster or accidental events due to their age. “Over 50% of the locks and dams operated by the Corps are over 50 years old and are approaching the end of their design lives” (Inland Waterway Navigation, 2009).

The aging infrastructure creates significant concern, especially as “domestic freight is expected to increase by 67%” and movement by barge is the most economical and environmentally friendly method to increase movement of goods in the United States (Inland Waterway Navigation, 2009).

It should be evident that a disruption of services on inland waterways could have significant and undesirable consequences. A study by Global Insight modeled a 90-day closure of inland waterway routes on the Mississippi and Illinois rivers during the fourth quarter of 2005. This analysis modeled a variety of goods with the majority of it being grain (corn and soybean). Their analysis showed that the cost to move the goods on the inland waterway during this period was \$118.6 million. In contrast, they estimated the cost of a modal shift from the waterways to rail as \$428 million, and the cost of a modal shift from the waterways to highway as \$1.5 billion for this same 90-day period (Sigman, 2008). Clearly, the inland waterways play a significant role in the economic security of this country. Disruption of this vital resource could have significant economic consequences in the supply chain.



Figure 1. North American Inland and Intracoastal Waterways
(www.worldcanals.com/image/usa.gif)

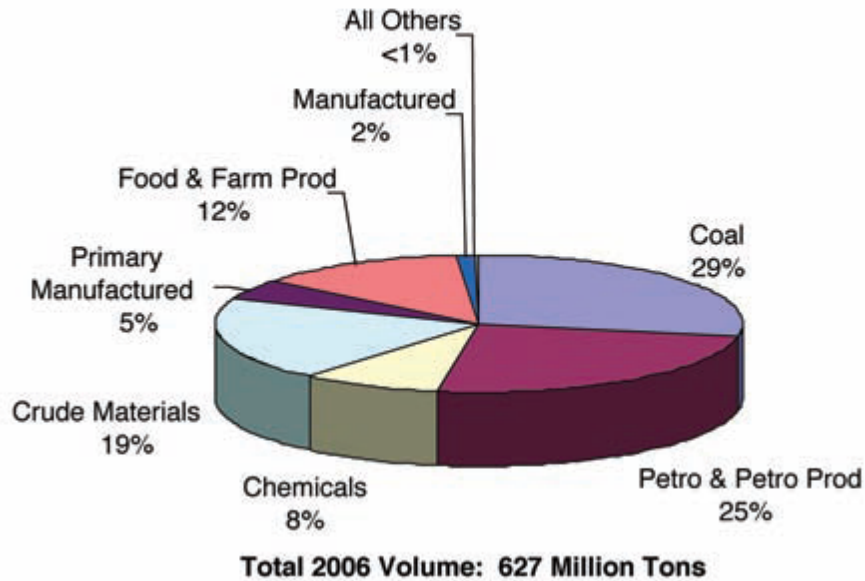


Figure 2. Inland Waterway Commodities Share by Tons (Inland Waterway Navigation, 2009)

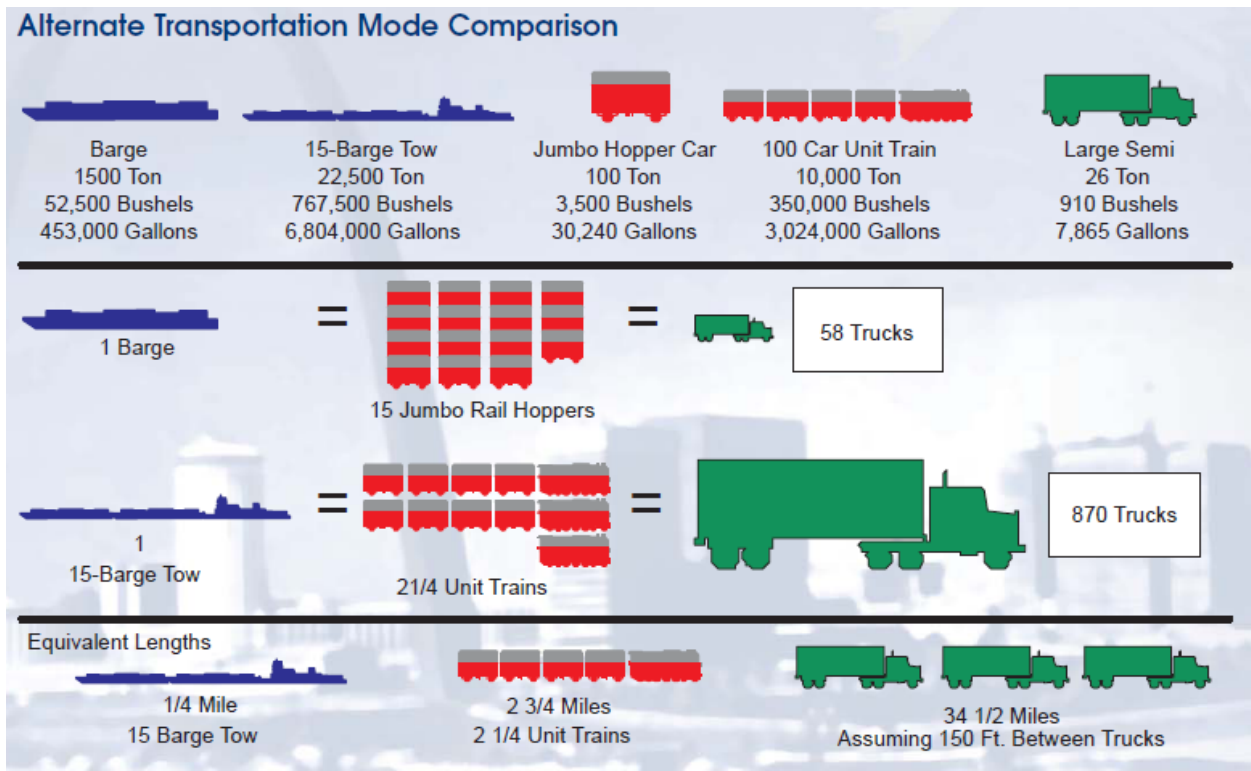


Figure 3. Comparison of Alternate modes of Transportation (Inland Waterway Navigation, 2000)

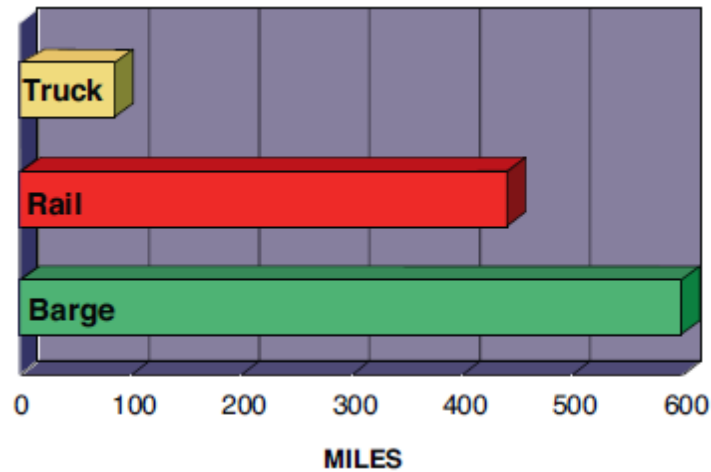


Figure 4. Average Distance One Gallon of Fuel Moves One Ton of Freight (Inland Waterway Navigation, 2009)

2.2 Supply Chain Risk and Resiliency

Network resilience is a topic that has been extensively studied by the telecommunications industry. Monma and Shallcross (1989) consider the problem of designing networks with 2-connected survivability constraints. Their objective is to minimize cost while maintaining a threshold survivability level (maintaining connectedness in the event that an arc fails). They present both network construction and network improvement heuristics for designing networks. Monma *et al.* (1990) examine the problem of constructing a minimum-weight, 2-connected spanning network. Their work is motivated by designing survivable communication and transportation networks. Grottschel *et al.* (1995) study the problem of designing networks with higher connectivity requirements so as to be able to survive network component failures. They provide integer program formulations, classes of valid and facet-defining inequalities, and polyhedral results. Eiselt *et al.* (1996) consider the problem of locating facilities so as to minimize the expected demand disconnected from other facilities in the event that one or multiple nodes fail. Such is the case when a network has unreliable nodes or links.

Qiao *et al.* (2007) examine the problem of allocating security resources to a water supply network. They develop an integrated, iterative resource allocation model to maximize the network's resilience using max-min linear programming, hydraulic simulation, and genetic

algorithms. They also present a number of measures of network resilience: connectivity, interconnectedness, and criticality (using interdiction). They find that low-order attack scenarios that have the greatest effect on network performance are the most important to guard against.

Bundschuh *et al.* (2005) formulate models of what they call robust and reliable supply chains with long term contracting. They consider the tradeoffs in an integrated supply chain between supplier reliability, emergency buffers and contingency supply, and expected service level versus cost. Dong (2006) presents a three-stage approach to developing a system-wide robustness index. Dong's index considers structural and functional aspects of network robustness. Dong identifies efficiency and robustness as critical measures of network performance. He also identifies two quantifiable measures (magnitude and likelihood) of network robustness. Haimes *et al.* (2008) consider the problems of protecting system assets and adding resilience to systems. They explore these problems in terms of emergence, resilience and preparedness and propose a framework to address them in large-scale systems. They also address issues of redundancy and robustness. Garg and Smith (2008) consider network survivability, a network's ability to remain operational despite component failures. They formulate a mixed-integer program to determine the minimal cost of a multi-commodity network subject to multiple simultaneous arc failures.

Arc and node failures, whether intentional or accidental, decrease reliability and introduce uncertainty into a network. The introduction of uncertainty can cause various network entities (suppliers, warehouses, customers, etc.) to modify their behavior depending on their level of risk preference. Different entities have different appetites for risk based on their objectives and previous experiences and, as such, typically adapt their behavior in reaction to perceived threats. Berman *et al.* (2007) analyze the effects of facility failure on network design. They enhance the P -median problem to explicitly account for facility failure. They find that as the probability of facility failure increases, facilities become more centrally located and, sometimes multiple facilities are allocated to the same location, a phenomenon which they refer to as co-location. Azaron *et al.* (2008) develop a multiobjective stochastic program considering risk. They consider supply, demand, processing, transportation, and capacity expansion costs as uncertain parameters. Their objectives are to minimize startup and continuing expenses while at the same time minimizing cost variance and the probability of not meeting a budget.

Recently, researchers have begun applying modern optimization tools (math models, algorithms, heuristics, etc.) to the network reliability problem. Liu and Iwamura (2000) examine the problem of k -terminal reliability in communications networks. They formulate a stochastic optimization model and use a simulation-based genetic algorithm for its solution. Yeh *et al.* (2002) continue the study of k -terminal reliability using 2-terminal reliability functions to evaluate k -terminal reliability. They generate 2-terminal reliability functions based on edge expansion diagrams using ordinary binary decision diagrams (OBDD). These 2-terminal reliability functions are then efficiently combined to construct k -terminal reliability functions. Srivaree-ratana *et al.* (2002) use a two-phase artificial neural network to estimate all-terminal network reliability. The first phase is trained on sample network topologies while the second phase uses results of the first phase, link reliabilities, and an upper bound on all-terminal network reliability for estimation.

In addition to estimating network reliability of existing networks, much effort has also gone into designing networks with reliability in mind. For example, Xu and Goulter (1999) consider the problem of designing a water distribution network to maximize the network's capacity reliability. This type of problem is generally referred to as the facility location problem (FLP). Snyder (2006) reviews articles on stochastic facility location models. He roughly divides the literature into two groups: stochastic location problems, in which the probability distribution of uncertain parameters is known, and robust location problems, in which the probability distribution of uncertain parameters is unknown. He observes that the objective of stochastic location models is usually to minimize an expected cost or to maximize an expected profit, while the objective of robust location problems is usually to minimize the maximum cost or regret.

Network node failure in the context of facility location is considered by Drezner (1987), who generalizes the P -median problem to consider unreliable facilities. Drezner (1987) formulates the problem using set-covering, and then develops a heuristic that can be used to find good solutions to large problem instances. Lin (2001) continues the study of the reliability of networks with unreliable nodes or arcs. Given an aggregate system demand d , Lin (2001) develops an algorithm based on minimal paths to evaluate the probability that the maximum flow of a network is at least d .

Networks may also experience arc failure. Work in this area is carried out by Berman and LeBlanc (1984) through an examination of the P -median problem with a different arc focus. Instead of unreliable arcs, they work with arcs that are of random length. Their work is motivated by the real-world problem of how to relocate urban ambulances in the afternoon to preposition them in anticipation of rush hour traffic congestion. They develop an iterative local-search heuristic to locate facilities, which can be moved at a cost. Andreas and Smith (2008) consider the two-path problem, wherein there are two paths between a supply node and a demand node and at least one of them must stay open at least some threshold percentage of the time. They formulate a nonlinear integer program and examine different solution strategies (pruning, coefficient tightening, lifting, and branch-and-bound partitioning schemes).

2.3 Supply Chain Disruption Models

The concept of supply chain risk and security can mathematically be represented using networks of various forms. The previous section discussed issues of network risk, reliability, robustness, and resilience. The remainder of the literature review focuses on models designed specifically to consider unique aspects of supply chain disruption.

2.3.1 Network Interdiction Models

Network interdiction is a specific class of network problems used for modeling supply chain disruption. The interdiction problem models an attacker-defender situation in which the attacker attempts to degrade performance of the defender's network. Two popular network metrics for this problem are maximum network flow and the shortest path between two nodes. Cormican *et al.* (1998) formulate a stochastic version of the interdiction problem. Their objective is to minimize the maximum expected flow through a network subjected to interdictions. They enhance their model to also account for uncertain arc capacities. Held *et al.* (2005) study the objective of maximizing the probability of significantly disrupting network flow. They demonstrate the efficiency of an algorithm developed by Riis and Schultz (2003) in obtaining solutions to their interdiction problem variant, and present reformulations of the problem.

Held and Woodruff (2005) also consider the objective of significantly disrupting flow, and explore the usefulness of local search-based heuristics in solving multi-stage network interdiction problems. Lim and Smith (2007) consider an attacker that disables a set of arcs to minimize the maximum profit that can be obtained from a multi-commodity network. They

consider both discrete (complete destruction of arcs) and continuous (partial reduction of arc capacities) interdiction. They compare a linearized model to a penalty model for the discrete case. For the continuous case, they use an optimal partition algorithm along with a heuristic which entails first solving the non-interdiction problem variant. Israeli and Wood (2002) examine an interdictor who seeks to maximize the shortest path between two nodes. They formulate a mixed-integer program to model the bi-level problem, and develop an efficient decomposition algorithm based on Benders decomposition to solve it.

Brown *et al.* (2005) develop a generic bi-level interdiction model that considers reconstitutability and can be applied to most infrastructure systems. They demonstrate their model on power grids, subways, and airports. The main contribution of their model is that of reconstitutability, i.e., how attacked system components are repaired and their performance is restored over time. Their findings are mixed: some systems, like highways, are relatively robust, while others, like fuel-distribution systems, are not.

2.3.2 Network Fortification Models

Once an analysis of the risk associated with elements of a system is complete, a so-called fortification effort is pursued. That is, resources are allocated in a manner that makes the system less susceptible to attack. For example, Haines *et al.* (1998) use a hierarchical holographic model to consider multiple perspectives concerning the fortification of a water system. They also define different types of fortification, including a mathematical definition of resilience.

Ezell *et al.* (2000) present a probabilistic infrastructure risk analysis model (IRAM) to analyze a small town's water supply. IRAM encompasses modeling, assessing, and managing system risk. The researchers focus on calculating critical and relevant measures to guide the allocation of scarce fortification resources.

Church *et al.* (2004) propose spatial optimization models in the form of the r -interdiction median problem and the r -interdiction covering problem. Later, Church and Scaparra (2007) extend this model to include the option of fortifying sites. They formulate an integer-linear program to allocate fortification resources to minimize the impact of an attack. They also consider how the act of fortifying affects which elements are considered critical. In their work, impact is measured in terms of degraded service level, increased operating costs, costs of repair, and time to recover.

McGill *et al.* (2007) present a framework that supports asset-level fortification-resource allocation. Their framework initially focuses on generating threat scenarios based on a target susceptibility matrix. It also considers interdictors' tendency to shift their aim from fortified infrastructure to less secure targets. Their framework differs from most other risk assessment methodologies in that it is asset-driven and not threat-driven. Smith *et al.* (2007) consider the fortification problem wherein the interdictor is also subject to an operating budget. They present optimal network design algorithms based on three different enemy attack strategies: attack arcs with the greatest capacities, with the greatest flows, or in such a way to optimally minimize the maximum flows. They model the scenario as a three-stage problem, consisting of constructing a network, inflicting damage to the network, and optimizing the remaining network.

Scaparra and Church (2008) present the r -interdiction median problem with fortification (RIMF) that minimizes the impact to r unprotected facilities by effectively allocating protective resources. They formulate a bi-level optimization problem and propose a specialized tree search algorithm to solve it. The benefit of their formulation is that it does not require an explicit enumeration of possible solutions. Scaparra (2006) also provides the p -median fortification problem (PMFP) which differs from the RIMF in that facilities fail randomly with a given probability as opposed to intelligent interdiction by an adversary as in RIMF. Golany *et al.* (2009) formulate the fortification-resource allocation problem using linear impact functions. Their formulation independently considers both probabilistic and strategic risks. They find that it is best to allocate resources to sites with the highest impact under probabilistic risk, while spreading resources to decrease the impact of the worst-case scenario is more effective for strategic risk.

2.3.3 *Post-fortification Fallibility*

A key assumption associated with the Scaparra and Church (2008) RIMF model and the Scaparra (2006) PMFP model is that resources allocated to fortify a facility render that facility infallible. In practice, this assumption is not realistic, and we are interested in incorporating post-fortification fallibility into our final model. A limited number of papers have also attempted to address this issue.

Church and Scaparra (2007) present the stochastic r -interdiction median problem, in which r facilities are attacked, but each attack is associated with a probability of success. They

develop two models based on this framework which find the best and worst case expected efficiency degradation. For varying values of r , this then allows the user to generate reliability envelopes which bound the expected efficiency loss for a given number of attacks. Snyder *et al.* (2006) observe that replacing the deterministic r -interdiction median problem in the second stage of Scaparra and Church (2008) RIMF model with the stochastic version would create the stochastic analogue of the RIMF. However, it is not clear how this analogue could be presented without the assumption that fortified facilities may not fail.

Zhan (2007) presents two models that make fortification decisions to decrease a facility's probability of failure subject to a budget. The objective of both models is to minimize total expected demand-weighted distance travelled from customers to facilities. The continuous version allows facility reliability to be increased in a continuous fashion subject to a budget, while the discrete version allows for reliability of a facility to be associated with one of a finite number of states, with specific costs associated with improving the reliability of a facility to a given state level. Zhan (2007) uses a monotonic branch-reduce-bound procedure to find optimal solutions to small instances of both problems.

Scaparra and Cappanera (2005) presented a scenario-based network fortification model with the objective of minimizing total expected cost of network flow. Scenarios correspond to attacks on user defined sets of facilities and fortification of a facility prevents failure regardless of whether the facility is attacked. Scaparra and Cappanera also provide a version of the model where attack corresponds to node capacity reduction and fortification of a facility merely reduces the impact of disruption from attack instead of completely preventing disruption. Peeta and Salman (2010) develop a bilevel stochastic program in which decisions are made to fortify arcs to increase the probability of arc survival. In the upper level program decisions are made subject to a budget with the objective of minimizing total expected cost of network flow, while the lower level program calculates the minimum cost flow for each failure scenario. They reformulate the problem as a single level optimization problem and provide an approximate solution procedure that gives a local optimum solution. While their model is capable of handling post-fortification fallibility, the computational results provided in their case study rely on the assumption that fortifying an arc reduces its probability of failure to zero.

2.3.4 Dynamic Network Models

Actions and decisions that occur with respect to supply chains are clearly not static. That is, time elements related to transportation, consumption, delays and inventory are pivotal factors that impact the supply chain's performance. Of course, this extends specifically to the analysis of supply chain risk, as we must consider the timing associated with any set of fortification, interdiction, and resource allocation decisions. In a general context, network models that consider time are often referred to as dynamic network models. Dynamic networks consist of duplicate nodes in a graph that represent a particular node over various time intervals of a fixed horizon (Jarvis and Ratliff, 1982). Time-dependent models have been considered in both continuous and discrete time contexts. Fleischer and Tardos (1998) extend discrete-time results to allow for continuous time models of some of the most standard dynamic models: maximum dynamic flows, quickest flows, lexicographically maximum flows and dynamic transshipments.

Many important applications require the construction and analysis of dynamic networks. For example, Chalmet *et al.* (1982) model the evacuation of a building as dynamic flow through a network. Work on dynamic network models is also rich in the application area of transportation. Ben-Akiva *et al.* (1991) consider dynamic models needed to analyze network performance under various traffic congestion patterns. Their work allows for updated information to impact real-time routing decisions. Of particular interest in the context of supply chain risk are the dynamic multicommodity flow problems studied by Hall *et al.* (2003). They allow flow values on arcs to vary with time and consider the specific complexity of dynamic multicommodity flow problems. Their results offer an example of the computational challenges surrounding many time-expanded problems. They show that the dynamic multicommodity flow problem belongs to the class of NP-Hard problems and offer efficient algorithms that benefit from assumptions and insights surrounding specific network topologies.

Interestingly, dynamic considerations have been given much less attention in the interdiction and fortification problems discussed previously. Among the few works that have pursued dynamic network interdiction, Derbes (1997) proposes a Lagrangian-based heuristic for interdicting a time-expanded transshipment network. His work finds near-optimal solutions for problems with up to 40,400 nodes and 153,419 arcs in less than one half hour. In addition, Malaviya *et al.* (2010) consider the best allocation of law enforcement resources over a fixed

horizon in order to interdict drug traffic. Their results identify arrest patterns that suggest stings on users served by common dealers as the most effective strategy for minimizing the maximum drug flow.

A lack of dynamic interdiction and fortification work has been formally recognized by leaders in the field. Smith (2009) identifies multi-period scenarios in which interdiction and fortification alternate over a finite horizon as one of the most pressing challenges that researchers face. He cites that existing methodologies used to solve small dynamic problems (two or three time periods) are unlikely to be extendable to real-life instances with extended horizons comprised of numerous periods. Most importantly, he points out that the lack of ability to solve dynamic interdiction/fortification problems means that a potential adversary may expose the weakness of a suboptimal time-dependent fortification priority list by delaying interdiction actions until the system is most vulnerable.

2.4 Perishability

The agriculture and health industries would benefit greatly from accurate modeling of perishable commodity supply chains. Significant economic loss can be seen each year in the form of food, blood, and medication spoilage. Apart from incorporating perishability through scenario construction (Pierskalla, 2004), perishability is primarily modeled in two ways: cost quantification of lost goods or focusing on other model resources in order to remove the potential for large-scale spoilage.

The most common approach for perishability considerations is accounting for spoilage in the form of system costs. Nagurney et al. (2011) model the blood supply chain with nodes for each process in the collection and distribution of blood. They assess a penalty cost for spoilage for every excess unit of flow that reaches the final demand node. Additionally, they decrease arc flow between nodes to account for blood destroyed during each processing phase.

Other researchers use perishability to motivate objectives that focus on other resources. Cetin (2009) presents a mathematical programming model for locating blood banks around hospitals and clinics. This approach minimizes total system distance. By minimizing the distance between blood supply and demand points, the time between blood collection and distribution should be minimized, thus decreasing the total system spoilage

2.5 Bi-level Network Design

Given a network of arcs and nodes, network interdiction problems study two opposing forces with competing objectives. There are two primary types of network interdiction problems. In maximum flow network interdiction, the interdictor's goal is to minimize the maximum flow that can pass through the network after the interdicted arcs have been removed. In shortest path network interdiction, the interdictor's goal is to maximize the length of the shortest path through the network after the removal of interdicted arcs. The competitive nature of these problems is an ideal application of bi-level programming. In a bi-level program, a leader chooses actions and then a follower reacts optimally based on those actions. In network interdiction, the leader is the interdictor, and the follower is the network traverser, either sending the maximum flow or traveling the shortest path through the network. Many exact solution approaches for standard bi-level programs are somewhat limited, particularly in terms of required computational time, and this has led to the development of heuristic approaches to bi-level network interdiction problems, especially for time-sensitive applications.

Military applications are a primary driver of these heuristic approaches. Practically, a useable methodology for solving network interdiction problems in a military setting needs to quickly produce quality answers. Cormican (1995) took advantage of the easy-to-solve subproblems of maximum flow network interdiction through the application of Bender's decomposition and extended it with an original "flow-dispersion" heuristic. This methodology gets good solutions, but the computational time required, even after the heuristic improvement, is prohibitive for quick turnaround military applications. Bingol (2001) used a lagrangian relaxation technique that relaxed the interdiction resource constraint to solve maximum flow network interdiction. This method solves quickly and the results for many problems are exact solutions, however the "problematic" instances of this problem, where maximum network flow is small, prove very difficult and the heuristic often yields large optimality gaps. Derbes (1997) applies a lagrangian relaxation technique to dynamic networks. Once again, this heuristic solves quickly but does not guarantee good solutions. In fact, the heuristic generates many possible solutions without guaranteeing feasibility and selects the best of the feasible solutions. When tested on dynamic networks, near-optimal solutions were found in only just over half of the test instances. Uygun (2002) extended Bingol's (2001) work trying to resolve the problematic test

instances. First, a better search method was used to find the lagrangian multiplier. Second, a branch-and-bound algorithm was incorporated on those problematic instances. Even with these additional measures, one in five of the problematic instances remain unsolvable, and the instances solved using the branch-and-bound method experienced severe run time increases. Royset and Wood (2007) extended this work with a specialized branch-and-bound method to determine the efficient frontier created by weighing two interdiction objectives, minimizing both maximum network flow and total interdiction cost. This methodology generally solved significantly faster than an exact integer programming approach.

Heuristic approaches are also appropriate than exact methods for problems with additional complicating elements. Gutfraind et al. (2010) consider a Markovian evader guided through the network by the least-cost path to the sink. In this case, they are able to reformulate the bi-level network interdiction model as a single level nonlinear 0-1 optimization problem. They then develop a heuristic based on betweenness centrality that quickly finds high-quality interdiction solutions. This simplification of the follower does not, however, generalize to all problem applications.

The literature for bi-level network interdiction heuristics is somewhat limited due to the high number of exact approaches available for these problems. Military applications rely heavily on heuristics due to the speed at which good solutions to these problems are required, but for most other applications the decrease in computational time requirements are not worth the associated increase in the optimality gap. This literature review can, however, be extended by opening the subject up to heuristics designed for other bi-level problem types.

Aksen et al. (2011) examined a p-median problem bilevel program formulated to plan and protect critical facilities. In their problem, the leader is the system planner and must decide where to open p critical service facilities and which of those facilities to protect with additional resources, making that facility immune to interdiction. The follower then makes interdiction decisions. They began by solving the problem exactly, which often must be done using an exponential time algorithm. In order to address this impractical computational requirement, they utilized a two-phase tabu search heuristic. The first phase uses tabu search to find the best p facility locations, and the second phase solves the remaining bi-level program exactly. This heuristic methodology resulted in significant time savings and worked well on a variety of problem sizes.

Lan et al. (2007) utilized a hybrid neural network and tabu search heuristic to solve bi-level programs. Tabu search is first used to select the binary variables, which are then fed into a neural network, which indicates if binary combinations are infeasible before another set is generated. This iteratively continues until tabu search termination. This method experienced some improvement over previous branch-and-bound approaches and is generalized for any bi-level program.

Rajesh et al. (2003) utilized a pure tabu search method to solve bi-level programs. They benchmarked their results on many well-known problems and achieved near optimal solutions in far less time than those previous methods in the literature. The heuristic is simple enough to be easily modified to apply to more complex bi-level formulations. Uno and Katagiri (2008) also use tabu search to solve a bi-level program that solves the defensive location problem, where the leader locates defensive facilities to keep the follower from reaching an important site. This methodology was shown to be more efficient than a random search algorithm and a genetic algorithm for seven test instances. These results indicate that tabu search is a good heuristic for solution generation to bi-level programs.

Tabu search is not, however, the only heuristic methodology that can be successfully applied to bi-level programs. Calvete et al. (2008) developed a genetic algorithm to solve linear bi-level problems. The method is contingent on the existence of an extreme point of the feasible region polyhedron of the problem as it applies a genetic algorithm to extreme point enumeration to find good solutions. This work is able to handle a higher level of complexity more efficiently than previously examined tabu search methods as long as the problem remains linear. They go on to show that the heuristic also works for quasiconcave bi-level problems provided the feasible region of shared constraints is a polyhedron, as the method still requires the location of an extreme point.

Kuo and Huang (2009) developed a particle swarm heuristic to solve linear bi-level programs. They compared their computational results with a genetic algorithm approach for four test problems with the particle swarm method outperforming the genetic algorithm in three of the four problems in terms of accuracy. The particle swarm method required slightly less computational time, but more importantly, the standard deviation of its computational time was lower than that of the genetic algorithm. This implies that the particle swarm method has higher stability than the genetic algorithm and produces more predictable run times. Kuo and Han

(2011) extended this work to utilize a hybrid genetic algorithm and particle swarm heuristic. They proposed three different hybrid methods, all of which outperformed the particle swarm or genetic algorithm heuristics alone. They are all, however, limited to linear bi-level programs.

Calvete et al. (2011) used a bi-level program to model a hierarchical production-distribution planning problem in which different decision makers control the production and distribution processes. They utilize an ant colony heuristic to solve the bi-level model, where a feasible solution to the associated multi-depot vehicle routing problem is constructed by the ants. The global pheromone trail is updated based on the distribution objective, and the production problem is resolved iteratively. The results of this work were repeated on a variety of problems, indicating method stability, but they were not compared to other methods.

While heuristics are not widely applied directly to bi-level network interdiction problems, they are extensively used on several other types of bi-level problems. The literature indicates that it is most important to develop a heuristic that best suits a specific problem, as there is no method that universally outperforms all others.

2.6 Coevolutionary Algorithms

Coevolutionary algorithms are a type of evolutionary algorithm in which individuals in one population are evaluated based on their interactions with individuals in another population. There are two main types of coevolutionary algorithms: competitive and cooperative. In competitive coevolutionary algorithms, individuals in one population are rewarded at the expense of those they interact with in the other, whereas individuals in cooperative coevolutionary algorithm are rewarded when they work well with the other population's individuals. This dual population structure is well suited to bi-level programs, so several bi-level implementations in the literature have utilized coevolutionary algorithms.

Deb and Sinha (2009) applied a coevolutionary algorithm to a bi-level multi-objective program, meaning both the leader and follower problems have more than one objective. This means that the coevolutionary part of the heuristic is primarily focused on a cooperative heuristic inside each subproblem. Their bi-level problem is structured so that any feasible solution to the upper level problem corresponds to the Pareto-optimal solution to the corresponding lower level problem. Their proposed heuristic was very successful in solving their problem.

Koh (2009) applied a coevolutionary particle swarm algorithm to bi-level variation inequalities for a highway transportation network. This heuristic maintains two particle swarms, each of a different species, with all members competing for the same placement in the network. This algorithm "easily obtained" the solution provided in the literature to all test problems.

Legillon et al. (2012) propose a cooperative coevolutionary algorithm for bi-level optimization. The basis of this algorithm is an incremental improvement to two different sub-populations, one for each level of the bi-level program, that periodically exchange information with one another. Unfortunately, there is little specific information on the exact operations performed on these populations.

3 Mathematical Modeling Approaches

In this section, we develop a set of mathematical models designed to assist in allocating resources for mitigating risks associated with infrastructure supporting the inland water ways. The goal is to explore model structures that will allow us to investigate the imperfect fortification, perishability issues associated with agriculture products, and the changing goals of an adversary over time.

3.1 Multi-period p -median fortification model with post-fortification fallibility

In this section a multi-period mathematical model is formulated that determines how and when to allocate resources to secure multi-modal infrastructure assets on the Upper Mississippi River. We begin our model development with the standard p -median fortification model since it considers random facility failures—an ideal way to consider the occurrence of natural disasters (Church, 2007; Snyder, 2006). In this model, facility fortification decisions are made with the objective of minimizing total expected distance traveled from each customer to their closest operational facility. The p -median fortification models found in the literature typically assume facilities can no longer fail once they have been fortified. We formulate a model extension for the more realistic scenario in which fortified facilities may still be vulnerable, i.e. are still at risk but at some reduced level. In our extension, the post-fortification failure probability of facility is nonzero, and is less than its pre-fortification probability of failure. The model extension also includes a multi-period planning horizon that allows for dynamic decision-making subject to a budget constraint, where fortification decisions are made for each facility in each time period. It

is assumed in this model that facilities that fail in one time period are operational again in the following time period, that is, the probability of failure for each facility is independent among time periods.

The basic model considers a set of facilities (or infrastructure components in our context) and a set of customers. Facilities are fallible, and their individual probabilities of failure can be reduced through the allocation of fortification actions subject to a budget in each time period. Optimal risk reduction decisions are determined by minimizing the total expected demand weighted distance from customers to facilities over the entire planning horizon.

We define J to be the set of existing facilities, I to be the set of customers served by those facilities, and T to be the set of time periods in the planning horizon. h_{it} is the demand of each customer $i \in I$ in time period t , and d_i^k is the distance from customer i to its k^{th} closest facility (note that this remains the same in each time period). The failure probability at the beginning of the first time period is given by p_j , for each facility $j \in J$. We let m_t denote the factor of fortification in time period t , such that the probability of facility failure is reduced by a factor of m_t if that facility is fortified in period t . b_t denotes the budget available in period t , while c_{jt} represents the cost of fortifying facility j in period t . Finally, we let w_{ij}^k be 1 if facility j is the k^{th} closest facility to customer i and 0 otherwise.

We define the binary variables z_{jt} , for each facility $j \in J$ and time period $t \in T$, to be 1 if facility j is fortified at time t and 0 otherwise. The continuous decision variables q_{it}^k , for all $k \in J$, $i \in I$, and $t \in T$ denote the post fortification failure probability of the k^{th} closest facility to customer i at the end of time period t . The continuous variables r_t represent the amount of unused budget from previous periods available for use in period t . The inclusion of this variable enables the model to save and accumulate budget over multiple periods in order to afford more expensive fortification actions in later periods. The complete math model is given below:

$$\min \sum_{t \in T} \sum_{i \in I} \sum_{k \in J} h_{it} d_i^k (1 - q_{it}^k) \prod_{l=0}^{k-1} q_{it}^l \quad (1)$$

$$s. t. \sum_{j \in J} c_{jt} z_{jt} \leq b_t + r_t \quad \forall t \in T \quad (2)$$

$$r_t = b_{t-1} + r_{t-1} - \sum_{j \in J} c_{j(t-1)} z_{j(t-1)} \quad \forall t = 2, \dots, |T| \quad (3)$$

$$r_1 = 0 \quad (4)$$

$$q_{i1}^k = \sum_{j \in J} w_{ij}^k (p_j (1 - m z_{j1})) \quad \forall i \in I, k \in J \quad (5)$$

$$q_{it}^k = \sum_{j \in J} w_{ij}^k (q_{i(t-1)} (1 - m z_{jt})) \quad \forall i \in I, k \in J, t = 2, \dots, |T| \quad (6)$$

$$z_{jt} \in \{0,1\} \quad \forall j \in J, t \in T \quad (7)$$

Our objective, (1), is to minimize total expected demand weighted distance traveled from customers to their closest operational facility over all time periods. Constraints (2) enforce a budget for each time period, while constraints (3) keep track of the budget remaining in each time period so that it may be rolled over for use in the next period. A time value of money factor can easily be added to constraints (3), should it be relevant to the application. Constraint (4) initializes the budget remainder in the first period to zero. Constraints (5) link the post fortification failure probabilities to the choice of facilities to be fortified for the first time period, where the previous probabilities of failure are given by the parameters p_j . Constraints (6) link the z binary fortification variables to the q variables representing the updated probabilities of failure for subsequent time periods.

Interestingly, this model can be reduced by substituting (3) – (6) into (1) and (2). This reduced representation leaves a knapsack constraint with a flexible right-hand resource constraint. Therefore, this problem falls into the difficult class of nonlinear knapsack problems that cannot be readily solved to optimality. However, there is opportunity to approximate the nonlinear objective with further evaluation of the function structure.

3.2 Multi-period minimum cost network flow model with fortification

In this section a minimum costs network flow model with fortification is proposed. Let L be the set of locks and dams and B be the set of bridges that cross the Upper Mississippi. Each

lock/dam combination $l \in L$ has an associated supply, d_l , of corn that enters the river at site l , which represent the locks/dams corresponding to the pool data. Let $W = L \cup B$. Then there is a set of directed arcs connecting these nodes in each of W , and which represent stretches of the river navigable by barge. Each arc has a corresponding travel cost per unit of corn by barge, c_{wr} where $w, r \in W$. We define D as the set of all supply nodes from which corn enters the river. Arcs with zero cost connect the nodes of D with the appropriate nodes in each of W . Let R denote the set of major intersections in the railroad network surrounding the Upper Mississippi, and let a set of directed arcs connecting these node represent railways, each with a corresponding cost of rail shipment per unit of corn, c_{ij} where $i, j \in R$. H is defined as the set of major intersections in the corresponding highway network, with associated highway links, and costs of moving one unit of corn by truck given by c_{hl} where $h, l \in H$.

Define s_0 as the sink of the network, located southern most of all the nodes. Let N , the set of nodes in the overall network be given by $N = W \cup R \cup H \cup s_0$. Then let A , the set of arcs in the overall network, be the set of all arcs associated with each of the afore mentioned node sets as well as appropriate directed arcs that link W to the set of rail nodes, R , the set of highway nodes, H . Costs on those arcs reflect the cost of transferring from one mode of transportation to another. If desired, fixed costs may be associated with these “multimodal arcs” that reflect the cost of establishing a transfer point. These fixed costs may then be incorporated into the objective. Each node in node set N has an associated capacity, k_j for each $j \in N$ that represents the amount of flow that can pass through node j .

For the purposes of our planning model we introduce T , the set of time periods. Net supply at each node $j \in N$ is given by b_{jt} in each time period $t \in T$. A positive b_{jt} corresponds to a supply node, a negative b_{jt} corresponds to a demand node, and a b_{jt} value of zero denotes a transshipment node. Over the course of the planning period, facilities may fail due to natural disaster or intentional attack. For the purposes of our model we will differentiate between “attacks” and “failures”. An attack occurs when conditions arise that threaten a facility. An unfortified facility will fail as a result of an attack with probability 1, while a fortified facility will withstand the attack. A particular combination of facility attacks over the planning horizon is referred to as a scenario and S denotes the set of possible scenarios that may occur over the planning horizon. For each scenario, a_{jst} is an input parameter that is one if facility j is attacked

in scenario s during time period t and zero otherwise. For each possible scenario, q_s denotes the probability that scenario $s \in S$ occurs. The model given below makes fortification decisions to protect facilities against failures. A certain number of fortifications per time period, Q_t is allowed. To ensure feasibility in the event of facility failures, we define u as a dummy source connected by an arc to demand node s_0 and v as a dummy sink connected by arcs to all supply nodes.

Our decision variables, Z_{jt} , are one if facility $j \in N$ is fortified in time period t and zero otherwise. The network flow variables, Y_{ijst} , represent the flow on arc (i, j) in time period t if scenario s occurs. The model is then given by:

$$\min \sum_{t \in T} \sum_{s \in S} q_s \sum_{(i,j) \in A} c_{ij} Y_{ijst} \quad (1)$$

$$s. t. \sum_{(j,i) \in A} Y_{jist} - \sum_{(i,j) \in A} Y_{ijst} = b_{jt} \quad \forall j \in N \setminus \{u, v\}, t \in T, s \in S \quad (2)$$

$$\sum_{i \in W, i \neq j} Y_{jist} \leq (1 - a_{jst})k_j + a_{jst}k_j \sum_{l=1}^t Z_{jl} \quad \forall j \in W, t \in T, s \in S \quad (3)$$

$$\sum_{j \in W} Z_{jt} = Q_t \quad \forall t \in T \quad (4)$$

$$\sum_{t \in T} Z_{jt} \leq 1 \quad \forall j \in W \quad (5)$$

$$Z_{jt} \in \{0,1\} \quad \forall j \in W, t \in T \quad (6)$$

$$Y_{ijst} \geq 0 \quad \forall (i,j) \in A, t \in T, s \in S \quad (7)$$

The objective of this multiperiod network flow model is to minimize the expected cost of all flows over all time periods, given the probabilities that various scenarios occur. The possible scenarios in S have the property that probabilities of each scenario occurring all sum to one. Each scenario corresponds to a set of “attacks” that are made on certain facilities during certain time periods. Constraint set (2) are the flow balance constraints that ensure flow balance is achieved at every node except the dummy sink and source in each time period. Constraint set (3) links the Y and Z variables, ensuring that flow cannot pass through a node that is attacked in a

given scenario and time period unless it has been fortified in that or a previous period. The structure of constraint set (3) also implies that if a facility/node fails in one time period that is operational again by the next time period. Note also that u and v may not be fortified, and are not included in the capacity or fortification constraints. The dummy source and sink are necessary to ensure feasibility as certain scenarios may otherwise render the problem infeasible. Constraint set (4) restricts the number of fortification actions that may take place in each time period. Constraint set (5) ensures that a facility is fortified no more than once in the planning horizon. Under current assumptions, a fortified facility cannot fail, therefore it seems reasonable over the entire planning horizon the total number of fortification actions will be less than or equal to the number of nodes. This multi-period network flow with fortification model will be the base for further extensions in the areas of perishability, post-fortification fallibility, and adaptive adversarial objectives. Even without further complexities, this model is challenging in terms of the number of scenarios that should be considered. To apply this model, the number of scenarios to possibly consider is exponential and most decisions associated with scenarios will be 0 in an optimal solution. Therefore, there is potential for a column generation-based procedure to improve the tractability of this formulation.

3.3 Tactical Risk Mitigation in a Perishable Commodity Supply Chain

It is assumed that there is a user-defined set of attack scenarios S , with $s \in S$ corresponding to one attack "plan" in which the input parameter a_{jts} is 1 if facility j is attacked in time period t under attack plan s . The probability that attack scenario $s \in S$ is carried out is given by the input parameter q_s . An attacked facility may fail or survive the attack. The probability of facility failure given an attack in time period t is given by the decision variables r_{jt} for facility j . The initial probabilities of facility failure given an attack in time period 1 are given as input parameters. For each attack plan $s \in S$, then, there are a number of possible "realized scenarios", $l \in L_s$ that correspond to each possible combination of realized failures and survivals of facilities under attack plan s . The input parameter k_{jtl} is 1 if facility j fails in time period t in realized scenario l of attack plan s . Each realized scenario $l \in L_s$ under attack plan $s \in S$ will occur with probability p_{ls} , which is a decision variable that depends on fortification decisions to facilities in previous and current time period. It makes sense that for a facility to actually fail that

it must both be attacked and succumb to that attack. In this model, it is assumed that fortification actions would affect the second component, whether a facility succumbs to an attack.

The network is given by a set of nodes, N , along with the arcset connecting those nodes, A . Each node in the overall network has a net supply in each time period, given by the input parameter b_{jt} for $j \in N$. The network contains one universal sink, u , and one universal source, v , that are connected to all non-transshipment nodes as appropriate to ensure feasibility in the event of facility failures. Prohibitively high costs and age values are placed on these arcs. Contained in N is the set of waterway infrastructure nodes, W , representing lock and dam combinations, bridges, and ports. All source nodes are elements of W , and net supply at each node is the positive difference in flow from the previous node to the current (current pool minus previous pool). Select elements of W are connected to intermodal transfer points, denoted by the set of I (note that u and v are also elements of I). These nodes are then connected to a rail/highway network. Each intermodal transfer point, $i \in I$ has an associated input parameter v_i that represents the age of the commodity as it reaches component i . This is the age of the commodity at point i provided that it travelled exclusively on the waterway up until transfer point i . A function, $f(age)$ represents the value of one unit of commodity at a given age. For each intermodal transfer point, i , there is a set of unique paths that connect the intermodal point to the demand sink, given by $P_{1i}, P_{2i}, \dots, P_{iK_i}$ (K_i denotes the number of paths originating at i and ending at the demand sink). Associated with each path P_{ki} originating at point i is d_{kit} , the amount of time required to travel path P_{ki} . In each time period t of each realized scenario of each attack plan, the amount of commodity flow on path P_{ki} is given by the decision variable μ_{sttik} .

The set of nodes that may be fortified (in other words, the set of nodes that may fail) is the set of waterway infrastructure nodes, W . The input parameter h_j denotes the length of disruption of facility j if it fails. The cost of fortifying facility $j \in W$ is given by e_{jt} , and the decision variable z_{jt} is 1 if facility $j \in W$ is fortified in time period t . A fortified facility's probability of failing under attack is reduced by input parameter θ for each fortification action. Resources may also be allocated to improve the resilience of existing transfer points. Let the decision variable z_{it} be 1 if investment is made in transfer point i , and let e_{it} represent the cost of such an action. If that investment is made, the cost and time required (i.e., amount added to age of product) to transfer modes will both be reduced. For each investment, the cost and time required to transfer are reduced by input parameters M and U , respectively.

The decision variables y_{ijts} represent the magnitude of flow on arc (i, j) in arcset A in time period t . The capacity of each node $j \in N$ is given by m_j . Costs are given by c_{ijt} , the cost of traversing arc (i, j) in time period t . The cost of switching from waterway to another mode of transportation is reflected in the cost of arcs connecting nodes in W to nodes in I . These costs may be reduced by investments in the transfer components, and so the c_{ijt} s are decision variables (although costs for non-mode transfer arcs may be treated as input parameters). Transfer links may only be used if they have been “opened”. Resources may also be allocated to open new intermodal transfer links, with fixed, one-time costs of o_{it} to open link point i in time period t . The binary decision variables f_{it} represent whether a link is opened in time period t . The link may be used in any subsequent periods after it has been opened, and variables corresponding to initial links present in the first time period are set to 1. The starting network then has a set of initial link points as well as potential link points that are being considered. Arcs connect the waterway nodes in W to initial and potential link points as appropriate (each link point adjacent to only one waterway node; waterway nodes may be adjacent to multiple link points). Costs and “age values” on those arcs reflect starting values in the first time period, with costs on the potential link points set to “starting” cost and age values were the link to be opened.

Decisions to improve the reliability of waterway nodes, the resilience of transfer nodes, and to open new transfer nodes are subject to a budget in each time period, given by input parameter ζ_t . Decisions are then made according to one of three objectives.

3.3.1 Notation

Input Parameters

S is the set of attack plans

T is the set of time periods

N is the set of nodes in the network

W is the set of waterway nodes

I is the set of intermodal transfer link nodes (each member of I is connected to exactly one member of W , but each member of W may be connected to multiple members of I)

L_s is the set of realized scenarios that may occur given attack plan $s \in S$ is carried out

a_{jts} is 1 if facility j is attacked in time period t under attack plan s

q_s is the probability that attack scenario $s \in S$ is carried out

k_{jtl_s} is 1 if facility j fails in time period t in realized scenario l of attack plan s

b_{jt} is net supply in each time period for $j \in N$

u is the universal sink

v is the universal source

$f(\text{age})$ represents the value of one unit of commodity at a given age

v_i that represents the age of the commodity as it reaches component $i \in I$

P_{ki} is the k th path originating at point i that ends at the sink at the “bottom” of the network

K_i denotes the number of paths originating at i and ending at the demand sink

h_j denotes the length of disruption of facility j if it fails

e_{jt} is the cost of fortifying facility $j \in W$ in time period t

e_{it} is the cost of investment in transfer point $i \in I$ in time period t

M is the amount by which cost of transfer is reduced if investment in transfer point $i \in I$ occurs

U is the amount by which the time required to transfer modes is reduced if investment in transfer point $i \in I$ occurs

m_j is the capacity of each node $j \in N$

o_{it} is the fixed, one-time cost of opening new intermodal transfer link $i \in I$

ζ_t is the budget for all investment decisions in time period t

θ is the amount by which a facility's probability of failure decreases given a fortification investment

r_{jt} is the probability of facility failure given an attack in time period t for facility j

p_{ls} is the probability that each realized scenario $l \in L_s$ under attack plan $s \in S$ (depends on fortification decisions to facilities in previous and current time period)

d_{kit} is the amount of time required to travel path P_{ki} in time period t

Decision Variables

μ_{sltik} is the amount of commodity flow on path P_{ki} in each time period t of each realized scenario $l \in L_s$ of each attack plan $s \in S$

z_{jt} is 1 if facility $j \in W$ is fortified in time period t

y_{ijtls} represents the magnitude of flow on arc (i, j) in arc set A in time period t under realized scenario l of attack plan s

c_{ijt} is the cost of traversing arc (i, j) in time period t (this made change based on investment decisions in intermodal transfer links)

f_{it} are binary decision variables representing whether a link to transfer point $i \in I$ is opened in time period t

3.3.2 Model

Objective 1 - Expected value of commodity: maximize

$$\sum_{s \in S} q_s \sum_{l \in L_s} p_{ls} \sum_{t \in T} \sum_{i \in I} \sum_{k=1}^{K_i} u_{sltik} f(d_{kit} + v_i)$$

Objective 2 – Expected cost of flow over all time periods: minimize

$$\sum_{s \in S} q_s \sum_{l \in L_s} p_{ls} \sum_{t \in T} \sum_{(i,j) \in A} c_{ijt} y_{sltij}$$

Objective 3 – Expected profit: maximize

$$\sum_{s \in S} q_s \sum_{l \in L_s} p_{ls} \sum_{t \in T} \left[\sum_{i \in I} \sum_{k=1}^{K_i} u_{sltik} f(d_{kit} + v_i) - \sum_{(i,j) \in A} c_{ijt} y_{sltij} \right]$$

Subject to:

$$\sum_{(j,i) \in A} y_{jiltls} - \sum_{(i,j) \in A} y_{ijtls} = b_{jt} \quad \forall j \in N \setminus \{u, v\}, t \in T, s \in S, l \in L_s \quad (1)$$

$$\sum_{\eta=t}^{t+h_j} \sum_{i \in W, (j,i) \in A} y_{jinls} \leq (1 - k_{jtls}) m_j \quad \forall j \in W, t \in T, s \in S, l \in L_s \quad (2)$$

$$\sum_{j \in N, (i,j) \in A} y_{ijtls} \leq m_i \sum_{l=1}^t f_{it} \quad \forall i \in I, t \in T, s \in S, l \in L_s \quad (3)$$

$$\sum_{t \in T} f_{it} \leq 1 \quad \forall i \in I \quad (4)$$

$$f_{i1} = 1 \forall i \in I \text{ such that transfer point } i \text{ is present in original network} \quad (5)$$

$$r_{j(t+1)} = r_{jt} - z_{jt}\theta \forall j \in W, t = 1, 2, \dots, |T| - 1 \quad (6)$$

$$p_{ls} = \prod_{t \in T, j \in W} [k_{jtls}a_{jts}r_{jt} + k_{jtls}(1 - a_{jts})(1 - r_{jt}) + (1 - k_{jtls})] \forall s \in S, l \in L_s \quad (7)$$

$$\mu_{sltik} \leq y_{mjtls} \forall s \in S, l \in L_s, t \in T, i \in I, k = 1, 2, \dots, K_i, (m, j) \in P_{ki} \quad (8)$$

$$\sum_{j \in W} e_{jt}z_{jt} + \sum_{i \in I} e_{it}z_{it} + \sum_{i \in I} o_{it}f_{it} \leq \zeta_t, \forall t \in T \quad (9)$$

$$c_{ji(t+1)} = c_{jit} - z_{it}M \forall (j, i) \in A \text{ such that } j \in W, i \in I, t = 1, 2, \dots, |T| - 1 \quad (10)$$

$$d_{ki(t+1)} = d_{kit} - z_{it}U \forall i \in I, k = 1, 2, \dots, K_i, t = 1, 2, \dots, |T| - 1 \quad (11)$$

$$y_{ijtls} \geq 0 \forall (i, j) \in A, t \in T, s \in S, l \in L_s \quad (12)$$

$$z_{jt} \in \{0, 1\} \forall j \in W \cup I, t \in T \quad (13)$$

$$f_{it} \in \{0, 1\} \forall i \in I, t \in T \quad (14)$$

$$c_{jit} \geq 0 \forall (j, i) \in A \text{ such that } j \in W \text{ and } i \in I, t \in T \quad (15)$$

$$(c_{jit} \text{ is an input parameter for all other arcs}) \quad (16)$$

$$d_{kit} \geq 0 \forall i \in I, k = 1, 2, \dots, K_i, t \in T \quad (17)$$

$$\mu_{sltik} \geq 0 \forall s \in S, l \in L_s, t \in T, i \in I, k = 1, 2, \dots, K_i \quad (18)$$

$$0 \leq p_{ls} \leq 1 \forall s \in S, l \in L_s \quad (19)$$

$$0 \leq r_{jt} \leq 1 \forall j \in W, t \in T \quad (20)$$

Constraints (1) enforce flow balance at all nodes in every time period, attack plan, and realized scenario, while constraints (2) ensures that for each of these, flow may not pass through failed nodes, for the duration of the node's failure. Constraint set (3) allow flow to pass through only those transfer nodes that have been opened, and constraints (4) ensure that each transfer node is opened at most once during the planning horizon (with constraints (5) "opening" those transfer nodes present in the initial network). For each waterway facility in each time period, constraints (6) update the facility's probability of failing under attack based on whether the facility has been fortified. Constraint set (7) calculates the probability of each realized scenario occurring for each attack plan, based on the individual waterway facilities' failure probabilities. Constraints (8) determine the amount of flow that travels on each non-waterway path to reach the network sink. A budget for the investment decisions of each time period is enforced through

constraint set (9). Costs and commodity age values are updated in constraint sets (10) and (11) based on investments in transfer links. While this model can be solved via nonlinear optimization software, the magnitude of decision variables is quite large. More specifically, the model requires a path-based, scenario-driven, action-set description. Any one of these three problem elements yields extensive complexity. Together, this complexity is multiplicative. In this case, approaches that generate both paths and scenarios in a decomposition structure provide an interesting avenue for future research. Of course, the dependence between these two entities complicates any decomposition structure even further and raises more general methodological questions relative to numerous fields of study.

3.4 Bi-Level Model

This model extends the previous ones by attempting to account for both the defender and attacker strategies in the context of the modeling framework. Consider a network given by a set of nodes, N , along with the arcset connecting those nodes, A , considered over a set of time periods T . Each node in the overall network has a net supply in each time period, given by the input parameter b_{jt} for $j \in N$. The network contains one universal sink, u , and one universal source, v . Contained in N is the set of waterway infrastructure nodes, W . All source nodes (as well as universal source and sink nodes) are elements of W , and net supply at each node is the positive difference in flow from the previous node to the current. All elements of W except u and v are connected to intermodal transfer points (ITP), denoted by the set of I . These nodes are then connected to a rail/highway network, represented by a single arc from each ITP directly to the sink.

It is assumed that there is a user-defined set of attack scenarios, S , with $s \in S$ corresponding to one attack “plan” in which the input parameter a_{js} is 1 if facility $j \in W$ is attacked under attack plan s (Note that only waterway nodes can be attacked). The decision variable, q_{st} is 1 if attack scenario s is carried out in time period t and 0 otherwise. An attacked facility may fail or survive the attack. The probability of facility failure given an attack in time period t is given by the decision variables r_{jt} for facility j . The initial probabilities of facility failure given an attack in time period 1 are given as input parameters. For each attack plan $s \in S$, then, there are a number of possible “realized scenarios”, $l \in L_s$ that correspond to each possible combination of realized failures and survivals of facilities under attack plan s . The input

parameter k_{jls} is 1 if facility j fails in realized scenario l of attack plan s . Each realized scenario $l \in L_s$ under attack plan $s \in S$ will occur in time period t with probability p_{lst} , which is a decision variable that depends on fortification decisions to facilities in previous time periods.

Fortification decisions are made with the decisions variable z_{jt} , which is 1 if facility $j \in W$ is fortified in time period t and 0 otherwise. Fortification of waterway infrastructure nodes, W , results in the reduction of that facility's probability of failure under attack by input parameter θ for each fortification action, and each fortification action of a waterway node has a cost of e_{jt} . The input parameter h_j denotes the length of disruption of facility j if it fails. Fortification actions of ITP nodes have an associated cost of e_{it} and result in the reduction of the cost required to transfer by input parameter M .

The decision variables y_{ijtl} represent the magnitude of flow on arc (i, j) in arcset A in time period t . The capacity of each node $j \in N$ is given by m_j . Costs are given by c_{ijt} , the cost of traversing arc (i, j) in time period t . The cost of switching from waterway to another mode of transportation is reflected in the cost of arcs connecting nodes in W to nodes in I . These costs may be reduced by investments in the transfer components, and so the c_{ijt} s are decision variables (although costs for non-mode transfer arcs may be treated as input parameters). Transfer links may only be used if they have been “opened”. Resources may also be allocated to open new intermodal transfer links, with fixed, one-time costs of o_{it} to open link point i in time period t . The binary decision variables f_{it} represent whether a link is opened in time period t . The link may be used in any subsequent periods after it has been opened, and variables corresponding to initial links present in the first time period are set to 1. The starting network then has a set of initial link points as well as potential link points that are being considered. Arcs connect the waterway nodes in W to initial and potential link points as appropriate (each link point adjacent to only one waterway node; waterway nodes may be adjacent to multiple link points). Costs and “age values” on those arcs reflect starting values in the first time period, with costs on the potential link points set to “starting” cost and age values were the link to be opened.

Decisions to improve the reliability of waterway nodes, the resilience of transfer nodes, and to open new transfer nodes are subject to a budget in each time period, given by input parameter ζ_t . The cost to attack facility j in time period t is given by ϵ_{jt} and the attacker is subject to a budget in each time period D_t . β_s is the base effectiveness of scenario s , which is an

input parameter that measures the attractiveness of each scenario. α_{st} is the fractional effectiveness of scenario s in time period t , which is effectively a measure of the fraction of its attractiveness that scenario s has maintained. The function, $f(z_{jt})$ calculates each scenario's effectiveness based on fortification decisions, and this value is divided by the scenario's base effectiveness to calculate its fractional effectiveness. The defender then makes fortification decisions in order to maximize expected profit, and the attacker makes decisions in order to maximize the fractional effectiveness of the chosen attack scenario. The joint consideration of scenarios and attack plans results adds computational requirements beyond those that can be handled in a reasonable amount of time for a large-scale problem. While this model is a unique contribution in terms of representing this real-world scenario, it requires for study to become implementable.

3.4.1 Notation

Input Parameters

S is the set of attack plans

T is the set of time periods

A is the set of arcs in the network

N is the set of nodes in the network

W is the set of waterway nodes

I is the set of intermodal transfer link nodes (each member of I is connected to exactly one member of W , but each member of W may be connected to multiple members of I)

L_s is the set of realized scenarios that may occur given attack plan $s \in S$ is carried out

a_{js} is 1 if facility j is attacked under attack plan s and 0 otherwise

k_{jls} is 1 if facility j fails in realized scenario l of attack plan s

b_{jt} is net supply in each time period for $j \in N$

u is the universal sink

v is the universal source

$f(\text{age})$ represents the value of one unit of commodity at a given age

v_i that represents the age of the commodity as it reaches component $i \in I$

P_{ki} is the k th path originating at point i that ends at the sink at the “bottom” of the network

K_i denotes the number of paths originating at i and ending at the demand sink

h_j denotes the length of disruption of facility j if it fails

e_{jt} is the cost of fortifying facility $j \in W$ in time period t

e_{it} is the cost of investment in transfer point $i \in I$ in time period t

M is the amount by which cost of transfer is reduced if investment in transfer point $i \in I$ occurs

U is the amount by which the time required to transfer modes is reduced if investment in transfer point $i \in I$ occurs

m_j is the capacity of each node $j \in N$

o_{it} is the fixed, one-time cost of opening new intermodal transfer link $i \in I$

ζ_t is the budget for all investment decisions in time period t

θ is the amount by which a facility's probability of failure decreases given a fortification investment

β_s is the base effectiveness of scenario s

ϵ_{jt} is the attack cost of facility j in time period t

D_t is the attack budget for time period t

Decision Variables

r_{jt} is the probability of facility failure given and attack in time period t for facility j

p_{lst} is the probability that each realized scenario $l \in L_s$ happens in time period t under attack plan $s \in S$ (depends on fortification decisions to facilities in previous and current time period)

q_{st} is 1 if attack scenario s is carried out in time period t

d_{kit} is the amount of time required to travel path P_{ki} in time period t

μ_{stik} is the amount of commodity flow on path P_{ki} in each time period t of each realized scenario

$l \in L_s$ of each attack plan $s \in S$

z_{jt} is 1 if facility $j \in W$ is fortified in time period t

α_{st} is the fractional effectiveness of scenario s in time period t

y_{ijtl_s} represent the magnitude of flow on arc (i, j) in arcset A in time period t under realized scenario l of attack plan s

c_{ijt} is the cost of traversing arc (i, j) in time period t (this made change based on investment decisions in intermodal transfer links)

f_{it} are binary decision variables representing whether a link to transfer point $i \in I$ is opened in time period t

$f(z_{jt})$ is the function that calculates each scenario's effectiveness based on fortification decisions

3.4.2 Formulation

Using this notation, a bi-level optimization model is formulated to represent the competing objectives associated with this problem. The outer problem represents the defender whose objective is to maximize the expected profit. This profit is calculated by subtracting transportation cost, dependent on the mode of transportation used to ship the product, from the value of the commodity at its destination considering perishability by calculating end value based on product age. This leading problem is subject to flow balance and budgetary constraints and accounts for post fortification fallibility, meaning fortification actions decrease a facility's probability of failure under attack but does not make it immune to attack actions. The inner problem represents the attacker whose objective is the maximize the fractional effectiveness of the chosen scenario, a value that is calculated based on whether or not facilities included in that attack scenario have been fortified. This follower problem is subject to budgetary constraints. The formulation of the bi-level problem is given as

Outer (Defender) Problem

$$\text{maximize } \sum_{t \in T} \sum_{s \in S} q_{st} \sum_{l \in L_s} p_{ls} \left[\sum_{i \in I} \sum_{k=1}^{K_i} \mu_{stik} f(d_{kit} + v_i) - \sum_{(i,j) \in A} c_{ijt} y_{stij} \right]$$

subject to

$$\sum_{(j,l) \in A} y_{jltls} - \sum_{(i,j) \in A} y_{ijltls} = b_{jt} \quad \forall j \in N \setminus \{u, v\}, t \in T, s \in S, l \in L_s \quad (1)$$

$$\sum_{\eta=t}^{t+h_j} \sum_{i \in W, (j,i) \in A} y_{ji\eta ls} \leq (1 - k_{jtls}) m_j \quad \forall j \in W, t \in T, s \in S, l \in L_s \quad (2)$$

$$\sum_{j \in N, (i,j) \in A} y_{ijltls} \leq m_i \sum_{l=1}^t f_{it} \quad \forall i \in I, t \in T, s \in S, l \in L_s \quad (3)$$

$$\sum_{t \in T} f_{it} \leq 1 \quad \forall i \in I \quad (4)$$

$$f_{i1} = 1 \quad \forall i \in I \text{ such that transfer point } i \text{ is present in original network} \quad (5)$$

$$r_{j(t+1)} = r_{jt} - z_{jt} \theta \quad \forall j \in W, t = 1, 2, \dots, |T| - 1 \quad (6)$$

$$p_{lst} = \prod_{j \in W} [k_{jls} a_{js} r_{jt} + k_{jls} (1 - a_{js}) (1 - r_{jt}) + (1 - k_{jls})] \quad \forall s \in S, t \in T, l \in L_s \quad (7)$$

$$\mu_{sltik} \leq y_{mjtls} \quad \forall s \in S, l \in L_s, t \in T, i \in I, k = 1, 2, \dots, K_i, (m, j) \in P_{ki} \quad (8)$$

$$\sum_{j \in W} e_{jt} z_{jt} + \sum_{i \in I} e_{it} z_{it} + \sum_{i \in I} o_{it} f_{it} \leq \zeta_t, \quad \forall t \in T \quad (9)$$

$$c_{ji(t+1)} = c_{jit} - z_{it} M \quad \forall (j, i) \in A \text{ such that } j \in W, i \in I, t = 1, 2, \dots, |T| - 1 \quad (10)$$

$$d_{ki(t+1)} = d_{kit} - z_{it} U \quad \forall i \in I, k = 1, 2, \dots, K_i, t = 1, 2, \dots, |T| - 1 \quad (11)$$

$$y_{ijltls} \geq 0 \quad \forall (i, j) \in A, t \in T, s \in S, l \in L_s \quad (12)$$

$$z_{jt} \in \{0, 1\} \quad \forall j \in W \cup I, t \in T \quad (13)$$

$$f_{it} \in \{0, 1\} \quad \forall i \in I, t \in T \quad (14)$$

$$c_{jit} \geq 0 \quad \forall (j, i) \in A \text{ such that } j \in W \text{ and } i \in I, t \in T \quad (15)$$

$$(c_{jit} \text{ is an input parameter for all other arcs}) \quad (16)$$

$$d_{kit} \geq 0 \quad \forall i \in I, k = 1, 2, \dots, K_i, t \in T \quad (17)$$

$$\mu_{sltik} \geq 0 \quad \forall s \in S, l \in L_s, t \in T, i \in I, k = 1, 2, \dots, K_i \quad (18)$$

$$0 \leq p_{ls} \leq 1 \quad \forall s \in S, l \in L_s \quad (19)$$

$$0 \leq r_{jt} \leq 1 \quad \forall j \in W, t \in T \quad (20)$$

Inner (Attacker) Problem

$$\text{maximize } \sum_{t \in T} \sum_{s \in S} \alpha_{st} q_{st} t$$

subject to

$$\sum_{s \in S} \sum_{j \in W} \epsilon_{jt} \alpha_{js} q_{st} \leq D_t \quad \forall t \in T \quad (22)$$

$$\sum_{s \in S} q_{st} = 1 \quad \forall t \in T \quad (23)$$

$$\frac{f(z_{jt})}{\beta_s} = \alpha_{st} \quad \forall t \in T, s \in S \quad (24)$$

$$\alpha_{st} \geq 0 \quad \forall t \in T, s \in S \quad (25)$$

$$q_{st}, z_{jt} \text{ binary } \forall t \in T, s \in S, j \in W \quad (26)$$

Constraints (1) enforce flow balance at all nodes in every time period, attack plan, and realized scenario, while constraints (2) ensures that for each of these, flow may not pass through failed nodes, for the duration of the node's failure. Constraint set (3) allow flow to pass through only those transfer nodes that have been opened, and constraints (4) ensure that each transfer node is opened at most once during the planning horizon (with constraints (5) “opening” those transfer nodes present in the initial network). For each waterway facility in each time period, constraints (6) update the facility's probability of failing under attack based on whether the facility has been fortified. Constraint set (7) calculates the probability of each realized scenario occurring for each attack plan in each time period, based on the individual waterway facilities' failure probabilities. Constraints (8) determine the amount of flow that travels on each non-waterway path to reach the network sink. A budget for the investment decisions of each time period is enforced through constraint set (9). Costs and commodity age values are updated in constraint sets (10) and (11) based on investments in transfer links. Constraints (22) enforce the attack decisions budget in each time period. Constraints (23) ensure only one scenario is carried out in each time period. Constraints (24) calculate the fractional effectiveness of each scenario in each time period. Interestingly, the inner problem itself is challenging to solve and its structure does no lend itself to simplifying techniques.

3.5 Tactical Risk Mitigation for Adaptive Adversaries

In this section we attempt to model an adaptive adversary in our modeling framework. The network is given by a set of nodes, N , along with the arc set connecting those nodes, A , considered over a set of time periods T . Each node in the overall network has a net supply in each time period, given by the input parameter b_{jt} for $j \in N$. The network contains one universal sink, u , and one universal source, v . Contained in N is the set of waterway infrastructure nodes, W . All source nodes (as well as universal source and sink nodes) are elements of W , and net supply at each node is the positive difference in flow from the previous node to the current. All elements of W except u and v are connected to intermodal transfer points (ITP), denoted by the set of I . These nodes are then connected to a rail/highway network, represented by a single arc from each ITP directly to the sink. Each of these ITP/arc combinations has an associated input parameter w_i that represents the per unit commodity end-value lost by transporting goods on the non-waterway network.

It is assumed that there is a user-defined set of attack scenarios, S , with $s \in S$ corresponding to one attack “plan” in which the input parameter a_{js} is 1 if facility $j \in W$ is attacked under attack plan s (Note that only waterway nodes can be attacked). Similarly, there is a user-defined set of fortification scenarios, G , with $g \in G$ corresponding to one fortification “plan” in which the input parameter z_{jg} are 1 if facility $j \in N$ is fortified under fortification plan g . The probability that attack scenario $s \in S$ is carried out in time period t is conditional on the fortification actions in the previous period and is given by the input parameter q_{stg} . An attacked facility may fail or survive the attack. The probability of facility failure given an attack in time period t is given by the decision variables r_{jt} for facility j . The initial probabilities of facility failure given an attack in time period 1 are given as input parameters. For each attack plan $s \in S$, then, there are a number of possible “realized scenarios”, $l \in L_s$ that correspond to each possible combination of realized failures and survivals of facilities under attack plan s . The input parameter k_{jls} is 1 if facility j fails in realized scenario l of attack plan s . Each realized scenario $l \in L_s$ under attack plan $s \in S$ will occur in time period t with probability p_{lst} , which is a decision variable that depends on fortification decisions to facilities in previous time periods.

Fortification decisions are made with the decisions variable x_{gt} , which is 1 if fortification plan g is carried out in time period t and 0 otherwise. Fortification of waterway infrastructure

nodes, W , results in the reduction of that facility's probability of failure under attack by input parameter θ for each fortification action, and each fortification action of a waterway node has a cost of e_{jt} . The input parameter h_j denotes the length of disruption of facility j if it fails. Fortification actions of ITP nodes have an associated cost of e_{it} and result in the reduction of the cost required to transfer by input parameter M .

The decision variables y_{ijts} represent the magnitude of flow on arc (i, j) in arc set A in time period t . The capacity of each node $j \in N$ is given by m_j . Costs are given by c_{ijt} , the cost of traversing arc (i, j) in time period t . The cost of switching from waterway to another mode of transportation is reflected in the cost of arcs connecting nodes in W to nodes in I . These costs may be reduced by investments in the transfer components, and so the c_{ijt} s are decision variables (although costs for non-mode transfer arcs may be treated as input parameters). Transfer links may only be used if they have been “opened”. Resources may also be allocated to open new intermodal transfer links, with fixed, one-time costs of o_{it} to open link point i in time period t . The binary decision variables f_{it} represent whether a link is opened in time period t . The link may be used in any subsequent periods after it has been opened, and variables corresponding to initial links present in the first time period are set to 1. The starting network then has a set of initial link points as well as potential link points that are being considered. Arcs connect the waterway nodes in W to initial and potential link points as appropriate (each link point adjacent to only one waterway). Costs on those arcs reflect starting values in the first time period, with costs on the potential link points set to “starting” cost and were the link to be opened.

Decisions to improve the reliability of waterway nodes, the resilience of transfer nodes, and to open new transfer nodes are subject to a budget in each time period, given by input parameter ζ_t . Decisions are then made in order to minimize the system cost of disruption, which requires an input parameter, D_t , representing the ideal travel cost of the network if all goods were transported on the waterway.

3.5.1 Notation

Input Parameters

S is the set of attack plans

G is the set of fortification plans

T is the set of time periods

A is the set of arcs in the network

N is the set of nodes in the network

W is the set of waterway nodes

I is the set of intermodal transfer link nodes (each member of I is connected to exactly one member of W , but each member of W may be connected to multiple members of I)

L_s is the set of realized scenarios that may occur given attack plan $s \in S$ is carried out

a_{js} is 1 if facility j is attacked under attack plan s and 0 otherwise

q_{stg} is the conditional probability that attack scenario $s \in S$ is carried out in time period t given the fortification plan $g \in G$ chosen in time period $t - 1$

k_{jls} is 1 if facility j fails in realized scenario l of attack plan s

b_{jt} is net supply in each time period for $j \in N$

u is the universal sink

v is the universal source

h_j denotes the length of disruption of facility j if it fails

e_{jt} is the cost of fortifying facility $j \in W$ in time period t

e_{it} is the cost of investment in transfer point $i \in I$ in time period t

M is the amount by which cost of transfer is reduced if investment in transfer point $i \in I$ occurs

m_j is the capacity of each node $j \in N$

o_{it} is the fixed, one-time cost of opening new intermodal transfer link $i \in I$

ζ_t is the budget for all investment decisions in time period t

θ is the amount by which a facility's probability of failure decreases given a fortification investment

w_i is the per unit profit loss associated with using ITP i

D_t is the attack budget for time period t

$j \in W$ is fortified in fortification scenario $g \in G$ and 0 otherwise

Decision Variables

r_{jt} is the probability of facility failure given an attack in time period t for facility j

p_{lst} is the probability that each realized scenario $l \in L_s$ happens in time period t under attack plan

$s \in S$ (depends on fortification decisions to facilities in previous and current time period)

y_{ijtl_s} represent the magnitude of flow on arc (i, j) in arcset A in time period t under realized scenario l of attack plan s

c_{ijt} is the cost of traversing arc (i, j) in time period t (this made change based on investment decisions in intermodal transfer links)

f_{it} are binary decision variables representing whether a link to transfer point $i \in I$ is opened in time period t

x_{gt} is 1 if fortification plan g is carried out in time period t

3.5.2 Formulation

Objective – System Disruption Cost:

$$\text{minimize } \sum_{t \in T} \sum_{s \in S} \sum_{g \in G} q_{stg} x_{g(t-1)} \sum_{l \in L_s} p_{ls} \left[\sum_{i \in I} w_i y_{iutls} + \left(\sum_{(i,j) \in A} c_{ijt} y_{stlij} - D_t \right) \right]$$

subject to

$$\sum_{(j,l) \in A} y_{jilt_s} - \sum_{(i,j) \in A} y_{ijtl_s} = b_{jt} \quad \forall j \in N \setminus \{u, v\}, t \in T, s \in S, l \in L_s \quad (1)$$

$$\sum_{\eta=t}^{t+h_j} \sum_{i \in W, (j,i) \in A} y_{ji\eta l_s} \leq (1 - k_{jtl_s}) m_j \quad \forall j \in W, t \in T, s \in S, l \in L_s \quad (2)$$

$$\sum_{j \in N, (i,j) \in A} y_{ijtl_s} \leq m_i \sum_{l=1}^t f_{it} \quad \forall i \in I, t \in T, s \in S, l \in L_s \quad (3)$$

$$\sum_{t \in T} f_{it} \leq 1 \quad \forall i \in I \quad (4)$$

$$f_{i1} = 1 \quad \forall i \in I \text{ such that transfer point } i \text{ is present in original network} \quad (5)$$

$$r_{j(t+1)} = r_{jt} - z_{jt} \theta \quad \forall j \in W, t = 1, 2, \dots, |T| - 1 \quad (6)$$

$$p_{lst} = \prod_{j \in W} [k_{jls} a_{js} r_{jt} + k_{jls} (1 - a_{js}) (1 - r_{jt}) + (1 - k_{jls})] \quad \forall s \in S, t \in T, l \in L_s \quad (7)$$

$$\sum_{g \in G} x_{gt} \leq 1 \quad \forall t \in T \quad (8)$$

$$\sum_{j \in W} \sum_{g \in G} e_{jt} z_{ig} x_{gt} + \sum_{i \in I} \sum_{g \in G} e_{it} z_{ig} x_{gt} + \sum_{i \in I} o_{it} f_{it} \leq \zeta_t, \quad \forall t \in T \quad (9)$$

$$c_{ji(t+1)} = c_{jit} - \left(\sum_{g \in G} z_{ig} x_{gt} \right) M \quad \forall (j, i) \in A \text{ such that } j \in W, i \in I, t = 1, 2, \dots, |T| - 1 \quad (10)$$

$$y_{ijtls} \geq 0 \quad \forall (i, j) \in A, t \in T, s \in S, l \in L_s \quad (11)$$

$$f_{it} \in \{0, 1\} \quad \forall i \in I, t \in T \quad (12)$$

$$x_{gt} \in \{0, 1\} \quad \forall i \in I, t \in T \quad (13)$$

$$c_{jit} \geq 0 \quad \forall (j, i) \in A \text{ such that } j \in W \text{ and } i \in I, t \in T \quad (14)$$

$$(c_{jit} \text{ is an input parameter for all other arcs}) \quad (15)$$

$$0 \leq p_{ls} \leq 1 \quad \forall s \in S, l \in L_s \quad (16)$$

$$0 \leq r_{jt} \leq 1 \quad \forall j \in W, t \in T \quad (17)$$

Constraints (1) enforce flow balance at all nodes in every time period, attack plan, and realized scenario, while constraints (2) ensures that for each of these, flow may not pass through failed nodes, for the duration of the node's failure. Constraint set (3) allow flow to pass through only those transfer nodes that have been opened, and constraints (4) ensure that each transfer node is opened at most once during the planning horizon (with constraints (5) “opening” those transfer nodes present in the initial network). For each waterway facility in each time period, constraints (6) update the facility's probability of failing under attack based on whether the facility has been fortified. Constraint set (7) calculates the probability of each realized scenario occurring for each attack plan in each time period, based on the individual waterway facilities' failure probabilities. Constraints (8) ensure at most one fortification plan is chosen in each time period. A budget for the investment decisions of each time period is enforced through constraint set (9). Costs are updated in constraint set (10) based on investments in transfer links.

3.6 Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks

In this model formulation, the network is given by a set of nodes, N , along with the arc set connecting those nodes, A , considered over a set of time periods T . Each node in the overall

network has a net supply in each time period, given by the input parameter b_{jt} for $j \in N$. The network contains one universal sink, u , and one universal source, v . Contained in N is the set of waterway infrastructure nodes, W . All source nodes (as well as universal source and sink nodes) are elements of W , and net supply at each node is the positive difference in flow from the previous node to the current. All elements of W except u and v are connected to intermodal transfer points (ITP), denoted by the set of I . These nodes are then connected to a rail/highway network, represented by a single arc from each ITP directly to the sink. Each of these ITP/arc combinations has an associated input parameter w_i that represents the per unit commodity end-value lost by transporting goods on the non-waterway network.

It is assumed that there is a user-defined set of attack scenarios, S , with $s \in S$ corresponding to one attack “plan” in which the input parameter a_{js} is 1 if facility $j \in W$ is attacked under attack plan s (Note that only waterway nodes can be attacked). Similarly, there is a user-defined set of fortification scenarios, G , with $g \in G$ corresponding to one fortification “plan” in which the input parameter z_{jg} are 1 if facility $j \in N$ is fortified under fortification plan g . The probability that attack scenario $s \in S$ is carried out in time period t is conditional on the fortification actions in the previous period and is given by the input parameter q_{stg} . An attacked facility may fail or survive the attack. The probability of facility failure given an attack in time period t is given by the decision variables r_{jt} for facility j . The initial probabilities of facility failure given an attack in time period 1 are given as input parameters. For each attack plan $s \in S$, then, there are a number of possible “realized scenarios”, $l \in L_s$ that correspond to each possible combination of realized failures and survivals of facilities under attack plan s . The input parameter k_{jls} is 1 if facility j fails in realized scenario l of attack plan s . Each realized scenario $l \in L_s$ under attack plan $s \in S$ will occur in time period t with probability p_{lst} , which is a decision variable that depends on fortification decisions to facilities in previous time periods.

Fortification decisions are made with the decisions variable x_{gt} , which is 1 if fortification plan g is carried out in time period t and 0 otherwise. Fortification of waterway infrastructure nodes, W , results in the reduction of that facility's probability of failure under attack by input parameter θ for each fortification action, and each fortification action of a waterway node has a cost of e_{jt} . The input parameter h_j denotes the length of disruption of facility j if it fails. Fortification actions of ITP nodes have an associated cost of e_{it} and result in the reduction of the

cost required to transfer by input parameter M . The decision variables y_{ijts} represent the magnitude of flow on arc (i, j) in arc set A in time period t . The capacity of each node $j \in N$ is given by m_j . Costs are given by c_{ijt} , the cost of traversing arc (i, j) in time period t . The cost of switching from waterway to another mode of transportation is reflected in the cost of arcs connecting nodes in W to nodes in I . These costs may be reduced by investments in the transfer components, and so the c_{ijts} are decision variables (although costs for non-mode transfer arcs may be treated as input parameters). Transfer links may only be used if they have been “opened”. Resources may also be allocated to open new intermodal transfer links, with fixed, one-time costs of o_{it} to open link point i in time period t . The binary decision variables f_{it} represent whether a link is opened in time period t . The link may be used in any subsequent periods after it has been opened, and variables corresponding to initial links present in the first time period are set to 1. The starting network then has a set of initial link points as well as potential link points that are being considered. Arcs connect the waterway nodes in W to initial and potential link points as appropriate (each link point adjacent to only one waterway). Costs on those arcs reflect starting values in the first time period, with costs on the potential link points set to “starting” cost and were the link to be opened. Decisions to improve the reliability of waterway nodes, the resilience of transfer nodes, and to open new transfer nodes are subject to a budget in each time period, given by input parameter ζ_t . Decisions are then made in order to minimize the system cost of disruption, which requires an input parameter, D_t , representing the ideal travel cost of the network if all goods were transported on the waterway.

3.6.1 Notation

Sets

u is the universal sink

v is the universal source

S is the set of attack plans

G is the set of fortification plans

T is the set of time periods

A is the set of arcs in the network

N is the set of nodes in the network

W is the set of waterway nodes

I is the set of intermodal transfer link nodes (each member of I is connected to exactly one member of W , but each member of W may be connected to multiple members of I)

L_s is the set of realized scenarios that may occur given attack plan $s \in S$ is carried out

Pre-Assigned Parameters

a_{js} is 1 if facility j is attacked under attack plan s and 0 otherwise

z_{jg} is 1 if facility $j \in W$ is fortified in fortification scenario $g \in G$

q_{stg} is the conditional probability that attack scenario $s \in S$ is carried out in time period t given the fortification plan $g \in G$ chosen in time period $t - 1$

k_{jls} is 1 if facility j fails in realized scenario l of attack plan s

b_{jt} is net supply in each time period for $j \in N$

h_j denotes the length of disruption of facility j if it fails

e_{jt} is the cost of fortifying facility $j \in W$ in time period t

e_{it} is the cost of investment in transfer point $i \in I$ in time period t

M is the amount by which cost of transfer is reduced if investment in transfer point $i \in I$ occurs

m_j is the capacity of each node $j \in N$

o_{it} is the fixed, one-time cost of opening new intermodal transfer link $i \in I$

ζ_t is the budget for all investment decisions in time period t

θ is the amount by which a facility's probability of failure decreases given a fortification investment

w_i is the per unit profit loss associated with using ITP i

D_t is the attack budget for time period t

Decision Variables

r_{jt} is the probability of facility failure GIVEN AN ATTACK in time period t for facility j

p_{lst} is the probability that each realized scenario $l \in L_s$ happens in time period t under attack plan

$s \in S$ (depends on fortification decisions to facilities in previous and current time period)

y_{ijtls} represent the magnitude of flow on arc (i, j) in arcset A in time period t under realized scenario l of attack plan s

c_{ijt} is the cost of traversing arc (i, j) in time period t (this made change based on investment decisions in intermodal transfer links)

f_{it} are binary decision variables representing whether a link to transfer point $i \in I$ is opened in time period t

x_{gt} is 1 if fortification plan g is carried out in time period t

3.6.2 Formulation

$$\begin{aligned} \text{minimize } & \sum_{t=2}^T \sum_{s \in S} \sum_{g \in G} q_{stg} x_{g(t-1)} \sum_{l \in L_s} p_{lst} \left[\sum_{i \in I} w_i y_{iutls} + \left(\sum_{(i,j) \in A} c_{ijt} y_{ijtls} - D_t \right) \right] \\ & + \sum_{s \in S} q_s \sum_{l \in L_s} p_{ls1} \left[\sum_{i \in I} w_i y_{iul1s} + \left(\sum_{(i,j) \in A} c_{ij1} y_{ij1ls} - D_1 \right) \right] \end{aligned}$$

subject to

$$\sum_{(1,i) \in A} y_{1itsl} = b_{1t} \quad \forall t \in T, s \in S, l \in L_s \quad (1)$$

$$\sum_{(j,i) \in A} y_{jitsl} - \sum_{(i,j) \in A} y_{ijtls} = b_{jt} \quad \forall j \in N \setminus \{u, v\}, t \in T, s \in S, l \in L_s \quad (2)$$

$$\sum_{\eta=t}^{t+h_j} \sum_{i \in W, (j,i) \in A} y_{ji\eta ls} \leq (1 - k_{jtls}) m_j \quad \forall j \in W, t \in T, s \in S, l \in L_s \quad (3)$$

$$\sum_{i \in I, (j,i) \in A} y_{jitsl} \leq m_j \quad \forall j \in W, t \in T, s \in S, l \in L_s \quad (4)$$

$$y_{iutsl} \leq m_i \sum_{t=1}^t f_{it} \quad \forall i \in I, t \in T, s \in S, l \in L_s \quad (5)$$

$$\sum_{t \in T} f_{it} \leq 1 \quad \forall i \in I \quad (6)$$

$$r_{j(t+1)} = r_{jt} - \left(\sum_{g \in G} z_{ig} x_{gt} \right) \theta \quad \forall j \in W, t = 1, 2, \dots, |T| - 1 \quad (7)$$

$$p_{lst} = \prod_{j \in W} [k_{jls} a_{js} r_{jt} + k_{jls} (1 - a_{js}) (1 - r_{jt}) + (1 - k_{jls})] \quad \forall s \in S, t \in T, l \in L_s \quad (8)$$

$$c_{ji(t+1)} = c_{jit} - \left(\sum_{g \in G} z_{ig} x_{gt} \sum_{\mu=1}^t f_{i\mu} \right) M \quad \forall (j, i) \in A \text{ such that } j \in W, i \in I, \\ t = 1, 2, \dots, |T| - 1 \quad (9)$$

$$\sum_{g \in G} x_{gt} = 1 \quad \forall t = 1, 2, \dots, |T| - 1 \quad (10)$$

$$x_{gt} = 0 \quad \forall g \in G, t = |T| \quad (11)$$

$$\sum_{j \in W} \sum_{g \in G} e_{jt} z_{jg} x_{gt} + \sum_{i \in I} \sum_{g \in G} e_{it} z_{ig} x_{gt} + \sum_{i \in I} o_{it} f_{it} \leq \zeta_t, \quad \forall t \in T \quad (12)$$

$$0 \leq p_{lst} \leq 1 \quad \forall t \in T, s \in S, l \in L_s \quad (13)$$

$$0 \leq r_{jt} \leq 1 \quad \forall j \in W, t \in T \quad (14)$$

$$y_{ijtsl} \geq 0 \quad \forall (i, j) \in A, t \in T, s \in S, l \in L_s \quad (15)$$

$$c_{ijt} \geq 0 \quad \forall (j, i) \in A \text{ such that } j \in W \text{ and } i \in I, t \in T \quad (16)$$

$$f_{it} \in \{0, 1\} \quad \forall i \in I, t \in T \quad (17)$$

$$x_{gt} \in \{0, 1\} \quad \forall i \in I, t \in T \quad (18)$$

Constraint (1) ensures that the source node moves the net supply to the legitimate node. Constraint (2) is the flow balance constraint. Constraint (3) guarantees that if a node fails, then it cannot transport the goods until the failure is eliminated. Constraint (4) allows the movement of goods from facility nodes to the related ITPs. Constraint (5) ensures that if an ITP is not open, then it cannot flow the goods. Constraint (6) guarantees that an ITP can be opened at most once during the planning horizon. Constraint (7) updates the probability of node failures by considering the fortification actions applied in the previous period. Constraint (8) calculates the probability of each realized scenario for each attack plan in each time period, based on the probability of node failures. Constraint (9) updates the cost of moving the goods by considering

the investments in ITPs. Constraint (10) enforces that exactly one fortification plan must be utilized in each period. Constraint (11) guarantees that there will be no fortification during the last period. Constraint (12) is the budget constraint. Constraints (13) to (16) are the sign restrictions and constraints (17) and (18) define the binary variables.

Appendix A summarizes an alternate modeling approach to the problem described in the earlier sections. In Appendix A, a multi-objective, multi-period, bi-level attacker defender mixed integer linear programming approach is defined. Both of the outer and inner optimization models are capital budgeting problems with constraints on “losses” due to attacks. Each separate adversarial objective or strategy is modeled as a different loss function. Each loss function represents a different level of network disruption. This modeling framework draws upon robust optimization ideas using a conditional variance at risk approach.

4 Model Analyses

The focus of this research was the development of a portfolio of new optimization models that account for dynamic fallible fortification and mitigating risk against adaptive adversaries. As discussed with the models in Section 3, there are a host of challenges surrounding these new modeling frameworks. In an effort to begin exploration into these approaches, we considered black-box solvers for the single-objective problem variants proposed in Section 3.5 and 3.6 and developed heuristic approaches for the bi-level model described in Section 3.4.

In each the fortification planning models studied, the resulting formulation was a nonconvex mixed-integer linear program. To handle this, we utilized the open-source nonlinear solver Couenne. In our experimentation, representative small models could be solved to optimality in a reasonable time. However, the key factor driving solution was both the number of scenarios accounted for and the number of response action states available to the adversary. Obviously, the more scenarios available to the decision-maker, the more possibilities that can be considered. However, it also clear that each of these scenarios is associated with a low probability event that is difficult to estimate. This raises the challenge of how to obtain accurate input data for models larger than those explored in our work. This separate area of concern should be of particular interest to researchers interested in the accurate elicitation of probabilities for threat-events.

For bi-level problems, we developed a co-evolutionary heuristic approach. As stated earlier, the concept of bi-level co-evolutionary heuristics is to maintain two separate populations, one for each of the bi-level sub-problems. These populations are separately manipulated and then information is periodically exchanged between them. In our method, genetic algorithms are performed separately on two populations, one for the attacker problem and one for the defender problem. The chromosomes for both populations are of an identical structure. That is, all chromosomes contain genes for both defender and attacker decisions. Genetic algorithms are performed separately on each of these populations. For the defender problem population, chromosome fitness is determined based on the defender objective to maximize expected profit. Similarly for the attacker problem population, fitness is determined based on the attacker objective to maximize the fractional effectiveness of the selected attack scenario. For each solution in both populations, the global genetic algorithm fitness is tested. To determine the global fitness of a chromosome, first the defender and attacker objectives are calculated for that chromosome. These values are subtracted from the objective value of the optimal solution to each sub-problem. These differences are normalized and summed to determine the global fitness value. This value is then minimized to determine the global solution to the problem. The global fitness calculation ensures that the global solution is a tradeoff solution for the two objectives. The procedure described provided solutions in quickly. The main challenge faced was how to assess the solutions obtained. Our investigation suggested that a tradeoff solution was an appropriate starting point for the development of a robust set of fortification decisions. Given the lack of alternative methods to compare against, this hypothesis remains in place and this work serves to provide a baseline approach for which additional bi-level heuristic work for adaptive adversarial settings can be measured.

5 Conclusions and Future Work

This goal of this effort was to explore modeling paradigms for developing decision support tools capable of assisting homeland security and inland waterway infrastructure managers with allocating scarce resources to mitigate risks across inland waterway infrastructure in order to reduce the risk of supply chain disruptions in the inland waterways. The models developed as part of this effort represent an initial step in trying to characterize the complex behavior associated with an adaptive advisory. The models formulated as part of this effort each present a

unique set of challenges when it comes to solution approaches for problems of reasonable sizes. While these are strategic decisions, and would only need to be made 1 a year or at most quarterly, the complexity of the current model formulations make that a challenge for even reasonably sized problems. Future research is needed to explore solution methods that will enable us to deal with the non-linearity's associated with the perishability issues, the stochastic elements associated with the probabilistic variables and extensive set of possible scenarios, and the complexity that arises in a bi-level modeling framework. Future efforts will focus on exploring reasonable solution approaches for this class of models.

References

- Andreas, A. and J. Smith (2008). Mathematical programming algorithms for two-path routing problems with reliability considerations. *INFORMS Journal on Computing* 20(4):553.
- Aksen, Deniz, Necati Aras, and Nuray Piyade. “A bilevel p-median model for the planning and protection of critical facilities.” *Journal of Heuristics* (2011): 1-26.
- Azaron, A., K. Brown, S. Tarim, and M. Modarres (2008). A multiobjective stochastic programming approach for supply chain design considering risk. *International Journal of Production Economics* 116(1):129 – 38.
- Bayrak, Halil, and Matthew D. Bailey. “Shortest path network interdiction with asymmetric information.” *Networks* 52.3 (2008): 133-140.
- Ben-Akiva, M., A. De Palma, and I. Kaysi (1991), Dynamic network models and driver information systems, *Transportation Research Part A: General*, Volume 25, Issue 5, Pages 251-266.
- Berman, O., D. Krass, and M. B. C. Menezes (2007). Facility reliability issues in network p-median problems: Strategic centralization and co-location effects. *Operations Research* 55(2):332–350.
- Berman, O. and B. LeBlanc (1984). Location-relocation of mobile facilities on a stochastic network. *Transportation Science* 18(4):315.
- Bingol, Levent. *A lagrangian heuristic for solving a network interdiction problem*. Naval Postgraduate School. Monterey, CA. 2001.
- Brown, G., M. Carlyle, J. Salmerón, and K. Wood (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In J. C. Smith, ed., *INFORMS TutORials in Operations Research*, pages 102–123. Baltimore, MD: INFORMS.
- Boyer, K.D., & Wilson, W. (2005, March 14). Estimation of Demands at Pool Level. *Navigation Economics Technologies Program*, prepared for the US Army Corps of Engineers.
- Bundschuh, M., D. Klabjan, P. Pei, and D. Thurston (2005). Modeling robust and reliable supply chains. Submitted.

- Calvete, Herminia I., Carmen Gal, and Mara-Jos Oliveros. "Bilevel model for production distribution planning solved by using ant colony optimization." *Computers & Operations Research* 38.1 (2011): 320-327.
- Calvete, Herminia I., Carmen Gale, and Pedro M. Mateo. "A new approach for solving linear bilevel problems using genetic algorithms." *European Journal of Operational Research* 188.1 (2008): 14-28.
- Cetin, E., Sarul, L. S., 2009. A blood bank location model: A multiobjective approach. *European Journal of Pure and Applied Mathematics* 2(1), 112-124.
- Chalmet, L. G., R. L. Francis, and P. B. Saunders (1982), *Network Models for Building Evacuation*, Management Science, Vol. 28, No. 1, pp. 86-105.
- Church, R. and M. Scaparra (2006). Analysis of facility systems' reliability when subject to attack or a natural disaster. *Reliability and Vulnerability in Critical Infrastructure: A Quantitative Geographic Perspective*. A. T. Murray and T. H. Grubestic, eds. Springer-Verlag, New York.
- Church, R. and M. Scaparra (2007). Protecting critical assets: The r-interdiction median problem with fortification. *Geographical Analysis* 39(2):129–146.
- Church, R., M. Scaparra, and R. Middleton (2004). Identifying critical infrastructure: The median and covering facility interdiction problems. *Annals of the Association of American Geographers* 94(3):491–502.
- Cormican, K., D. Morton, and R. Wood (1998). Stochastic network interdiction. *Operations Research* 46(2):184 – 97.
- Cormican, Kelly J. *Computational Methods for Deterministic and Stochastic Network Interdiction Problems*. Naval Postgraduate School. Monterey, CA. 1995.
- Deb, Kalyanmoy, and Ankur Sinha. "Solving bilevel multi-objective optimization problems using evolutionary algorithms." *Evolutionary Multi-Criterion Optimization*. Springer Berlin Heidelberg, 2009.
- Derbes, D., (1997), "Efficiently Interdicting A Time-Expanded Transshipment Network", Master's Thesis, Naval Postgraduate School, Monterey, California.

- Derbes, H. Dan. *Efficiently Interdicting a Time-Expanded Transshipment Network*. Naval Postgraduate School. Monterey, CA. 1997.
- Dong, M. (2006). Development of supply chain network robustness index. *International Journal of Services Operations and Informatics* 1(1):54–66.
- Drezner, Z. (1987). Heuristic solution methods for 2 location-problems with unreliable facilities. *Journal of The Operational Research Society* 38(6):509–514.
- Eiselt, H., M. Gendreau, and G. Laporte (1996). Optimal location of facilities on a network with an unreliable node or link. *Information Processing Letters* 58(2):71–74.
- Ezell, B. C., J. V. Farr, and I. Wiese (2000). Infrastructure risk analysis of municipal water distribution system. *Journal of Infrastructure Systems* 6(3):118 – 122.
- Fleischer, L. and E. Tardos (1998), Efficient continuous-time dynamic network flow algorithms, *Operations Research Letters*, Volume 23, Issues 3-5, Pages 71-80.
- Frittelli, J.F. 2005. CRS Report for Congress. Grain Transport: Modal Trends and Infrastructure Implications. January 5, 2005.
- Garg, M. and J. Smith (2008). Models and algorithms for the design of survivable multicommodity flow networks with general failure scenarios. *Omega* 36(6):1057–1071.
- Golany, B., E. Kaplan, A. Marmur, and U. Rothblum (2009). Nature plays with dice—terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research* 192(1):198–208.
- Grotschel, M., C. Monma, and M. Stoer (1995). Polyhedral and computational investigations for designing communication networks with high survivability requirements. *Operations Research* 43(6):1012–1024.
- Gutfraind, A., A. Hagberg, D. Izraelevitz, and F. Pan (2010) Interdiction of a Markovian Evader. *arXive preprint arXiv: 1009.0556*.
- Hagberg, Aric, et al. *Interdiction of a Markovian evader*. No. LA-UR-08-06551; LA-UR-08-6551. Los Alamos National Laboratory (LANL), 2008.
- Haimes, Y., K. Crowther, and B. Horowitz (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. *Systems Engineering* 11(4):287–308.

- Haimes, Y. Y., N. C. Matalas, J. H. Lambert, B. A. Jackson, and J. F. Fellows (1998). Reducing vulnerability of water supply systems to attack. *Journal of Infrastructure Systems* 4(4):164 – 177.
- Hall, M. S. A. and S. Hippler (2003), “Multicommodity Flows over Time: Efficient Algorithms and Complexity,” *Proc. Int’l Colloquium on Automata, Languages and Programming (ICALP ‘03)*.
- Hartel, Pieter H., and Hugh Glaser. “The resource constrained shortest path problem implemented in a lazy functional language.” *Journal of Functional Programming* 6.1 (1996): 29-45.
- Held, H., R. Hemmecke, and D. L. Woodruff (2005). A decomposition algorithm applied to planning the interdiction of stochastic networks. *Naval Research Logistics* 52(4):321 – 328.
- Held, H. and D. L. Woodruff (2005). Heuristics for multi-stage interdiction of stochastic networks. *Journal of Heuristics* 11(5-6):483 – 500.
- Inland Waterway Navigation: Value to the Nation, U.S. Army Engineer Institute for Water Resources, (2000). www.CorpsResults.us, IWR Publication Office, Pg 3, Accessed 25 April 2010.
- Inland Waterway Navigation: Value to the Nation, U.S. Army Engineer Institute for Water Resources, (2009). www.iwr.usace.army.mil/inside/products/pub/docs_pub/VTN/VTNInlandNavBro_lores.pdf Accessed 25 April 2010.
- Israeli, E. and R. Wood (2002). Shortest-path network interdiction. *Networks* 40(2):97–111.
- Israeli, Eitan, and R. Kevin Wood. “Shortestpath network interdiction.” *Networks* 40.2 (2002): 97-111.
- Jarvis, J. J. and H. D. Ratliff (1982), Some Equivalent Objectives for Dynamic Network Flow Problems, *Management Science*, Vol. 28, No. 1, pp. 106-109.
- Koh, Andrew. “A Coevolutionary Particle Swarm Algorithm for Bi-Level Variational Inequalities: Applications to Competition in Highway Transportation Networks.” *Natural intelligence for scheduling, planning and packing problems*. Springer Berlin Heidelberg, 2009. 195-217.

- Kuo, R. J., and C. C. Huang. "Application of particle swarm optimization algorithm for solving bi-level linear programming problem." *Computers & Mathematics with Applications* 58.4 (2009): 678-685.
- Kuo, R. J., and Y. S. Han. "A hybrid of genetic algorithm and particle swarm optimization for solving bi-level linear programming problemA case study on supply chain model." *Applied Mathematical Modeling* 35.8 (2011): 3905-3917.
- Lan, Kuen-Ming, et al. "A hybrid neural network approach to bilevel programming problems." *Applied Mathematics Letters* 20.8 (2007): 880-884.
- Legillon, Francois, Arnaud Liefoghe, and E. Talbi. "CoBRA: A cooperative coevolutionary algorithm for bi-level optimization." *Evolutionary Computation (CEC), 2012 IEEE Congress on. IEEE*, 2012.
- Lim, C. and J. Smith (2007). Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions* 39(1):15–26.
- Lin, Y. K. (2001). A simple algorithm for reliability evaluation of a stochastic-flow network with node failure. *Computers and Operations Research* 28(13):1277–1285.
- Liu, B. and K. Iwamura (2000). Topological optimization models for communication network with multiple reliability goals. *Computers and Mathematics with Applications* 39(7–8):59–69.
- Malaviya, A., C. Rainwater, and T.C. Sharkey (2010), Multi-stage Network Interdiction Models with Applications to City-level Drug Enforcement, to appear in 2010 Industrial Engineering Research Conference Proceedings.
- McGill, W. L., B. M. Ayyub, and M. Kaminsky (2007). Risk analysis for critical asset protection. *Risk Analysis* 27(5):1265 – 1281.
- Monma, C. and D. Shallcross (1989). Methods for designing communications networks with certain 2-connected survivability constraints. *Operations Research* 37(4):531–541.
- Monma, C. L., B. S. Munson, and W. R. Pulleyblank (1990). Minimum weight two-connected spanning networks. *Mathematical Programming, Series A* 46(2):153 – 171.

- Qiao, J., D. Jeong, M. Lawley, J.-P. Richard, D. Abraham, and Y. Yih (2007). Allocating security resources to a water supply network. *IIE Transactions* 39(1):95 – 109.
- Peeta, S., Salman, F.S., Gunneç, D. and Viswanath, K. (2010) ‘Pre-disaster investment decisions for strengthening a highway network’, *Computers & Operations Research*, Vol. 37, No. 10, pp.1708–1719.
- Pierskalla, W. P., 2004. Supply chain management of blood banks. In: Brandeau, M. L., Sanfort, F., Pierskalla, W. P., Editors, *Operations Research and Health Care: A Handbook of Methods and Applications*. Kluwer Academic Publishers, Boston, Massachusetts, 103-145.
- Rajesh, J., et al. “A tabu search based approach for solving a class of bilevel programming problems in chemical engineering.” *Journal of Heuristics* 9.4 (2003): 307-319.
- Riis, M. and R. Schultz (2003). Applying the minimum risk criterion in stochastic recourse programs. *Computational Optimization and Applications* 24(2):267–287.
- Royset, Johannes O., and R. Kevin Wood. “Solving the bi-objective maximum-flow network-interdiction problem.” *INFORMS Journal on Computing* 19.2 (2007): 175-184.
- Scaparra, M. and P. Capanera (2005). Optimizing security investments in transportation and telecommunication networks. *INFORMS 2005*, San Francisco.
- Scaparra, M. and R. Church (2008). An exact solution approach for the interdiction median problem with fortification. *European Journal of Operational Research* 189(1):76–92.
- Sigman, S., “Vulnerable Infrastructure Equals Economic Risk,” *Logistics Today*, 1 September, 2008.
- Sinha, R.N., and W.E. Muir (1973). Grain Storage: Part of a System. The AVI Publishing Company, Inc., Westport, Connecticut.
- Smith, J.C. (2009), “Basic Interdiction Models,” In: *Encyclopedia of Operations Research and Management Science* (edited by J. Cochran), Wiley, Hoboken, NJ.
- Smith, J. C., C. Lim, and F. Sudargho (2007). Survivable network design under optimal and heuristic interdiction scenarios. *Journal of Global Optimization* 38(2):181 – 199.
- Snyder, L. (2006). Facility location under uncertainty: a review. *IIE Transactions*

- Snyder, L., M. Scaparra, M. Daskin, and R. Church (2006). Planning for disruptions in supply chain networks. In M. P. Johnson, B. Norman, and N. Secomandi, eds., *TutORials in Operations Research*, pages 234–257. Baltimore, MD: INFORMS.
- Srivaree-ratana, C., A. Konak, and A. Smith (2002). Estimation of all-terminal network reliability using an artificial neural network. *Computers and Operations Research* 29(7):849–868.
- Uno, Takeshi, and Hideki Katagiri. “Single-and multi-objective defensive location problems on a network.” *European Journal of Operational Research* 188.1 (2008): 76-84.
- Uygun, Adnan. *Network interdiction by Lagrangian relaxation and branch-and-bound*. Dissertation. Naval Postgraduate School. Monterey, CA. 2002.
- Xu, C. and I. Goulter (1999). Reliability-based optimal design of water distribution networks. *Journal of Water Resources Planning and Management* 125:352.
- Yeh, F., S. Lu, and S. Kuo (2002). OBDD-based evaluation of k-terminal network reliability. *IEEE Transactions on Reliability* 51(4):443– 451.
- Zhan, R. L. (2007). *Models and algorithms for reliable facility location problems and system reliability optimization* (Unpublished doctoral disserataon). University of Florida, Gainesville, FL.

Appendix A

Reliable Network Interdiction-Fortification Problem for Inland Waterways

1 Problem Description

The goal of this appendix is explore ways to solve the Reliable Network Interdiction-Fortification Problem (RNIFP) for inland waterways, specifically the Upper Mississippi given an attacker who can switch among multiple attack strategies in response to the fortifications. We are particularly concerned about perishable commodities such as grain, whose value diminishes with time due to spoilage and therefore are sensitive to delays caused by network disruptions.

2 High-level Model

The Multiperiod Robust Network Fortification Problem with Adaptive Adversary (MRNFP-AA) is modeled here as a multi-objective multi-period bi-level attacker-defender MILP. Both the outer and inner optimization models are capital budgeting models with constraints on “losses” due to attacks. Each separate adversarial objective or strategy is modeled as a different loss function. Each loss functions is a different measure of network disruption. This model draws on robust optimization ideas.

2.0.1 Attacker's Problem Statement

Given $G = (N, A)$, a time-expanded capacitated water transportation network for perishable commodities, and a set of measures of network disruption (loss functions, which capture transportation and spoilage costs) corresponding to different attack strategies, choose y , the set of nodes to attack, by following the strategy that results in the largest losses, subject to an attack budget B_{0t} , the defender's fortification efforts w and x , uncertain attack success p , and post-fortification fallibility r .

2.0.2 Defender's Problem Statement

Given $G = (N, A)$, a time-expanded capacitated water transportation network for perishable commodities, and an attacker with multiple strategies as described above, determine which nodes (that is, locks) to reinforce against attack (w) or to add intermodal transfer capacity to x in order to minimize the attacker's ability to disrupt the network, no matter which strategy and loss

function they to use, subject to budget constraints B_{1t} , uncertain attack success p , and post-fortification fallibility r . As currently formulated, the inner problem is a robust optimization model. This model uses probability information to relax the uncertainty set by discarding the least probable $1 - \beta_i$ % of possible attacks.

2.1 Parameters

- $G = (N, A)$: A directed graph. Nodes represent locks or dams and arcs represent pools.
- T : The set of time periods in the model, indexed by t .
- I : The index set of loss functions, indexed by i .
- a_j : The cost to attack node $j \in N$.
- b_j : The cost to open an IMTF at node $j \in N$.
- c_j : The cost to fortify node $j \in N$.
- B_{0t} : The attacker's budget for period $t \in T$.
- B_{1t} : The defender's budget for period $t \in T$.
- P_j : Before reinforcement, the probability that node $j \in N$ fails when attacked.
- r_j : After reinforcement, the probability that node $j \in N$ fails when attacked.
- $\beta_i \in (0, 1)$: Probability threshold for each attacker objective $i \in I$.
- $L_i(w, x, y; p, r)$: A function that measures the loss for each feasible triple of decisions (w, x, y) given node failure probabilities (p, r) according to attacker objective $i \in I$. Since attack successes are uncertain, L_i is a random variable. The sample space of L_i is $\Omega_i \subseteq \mathbb{R}$.
- $\mathcal{U}_{\beta_i}^i \subset \Omega_i$ is the uncertainty set for each attacker objective $i \in I$, defined so that $Pr(\mathcal{U}_{\beta_i}^i) = \beta_i$, and for all $l_i \in \mathcal{U}_{\beta_i}^i$ and $l'_i \in \Omega_i \setminus \mathcal{U}_{\beta_i}^i$, $Pr(l_i) > Pr(l'_i)$. In other words, $\mathcal{U}_{\beta_i}^i$ contains the most probable β_i % of losses for objective $i \in I$.

2.2 Decision Variables

- w_{jt} : For each node $j \in N$, $w_{jt} = 1$ if a fortification action is applied to node j in period $t \in T$, and 0 otherwise.
- x_{jt} : For each node $j \in N$, $x_{jt} = 1$ if an IMTF is constructed during period $t \in T$, and 0 otherwise.

- y_{jt} : For each node $j \in N$, $y_{jt} = 1$ if node j is attacked in period $t \in T$, and 0 otherwise.
- L : The maximum loss from all the loss functions $L_i \in I$ over the most likely $\beta\%$ of losses for each loss function L_i .

2.3 Outer Problem: Attacker

$$\text{Maximize } H(w, x, z) \quad (1)$$

Subject to:

$$\sum_{j \in N} a_j y_{jt} \leq B_{0t} \quad \forall t \in T \quad (2)$$

$$y_j \in \{0, 1\} \quad \forall j \in N \quad (3)$$

2.4 Inner Problem: Defender

$$H(w, x, z) = \text{Minimize } L \quad (4)$$

Subject to:

$$\sum_{j \in N} c_j w_{jt} + b_j x_{jt} \leq B_{1t} \quad \forall t \in T \quad (5)$$

$$L \geq L_i(w, x, y) \quad \forall i \in I \quad (6)$$

$$L_i(w, x, y) \in \mathcal{U}_{\beta_i}^i \quad \forall i \in I \quad (7)$$

$$w_{jt}, x_{jt} \in \{0, 1\} \quad \forall j \in N, \forall t \in T \quad (8)$$

2.5 Modeling Reinforcement and Loss

This model captures the attacker's changing objectives in the inner objective function. The attacker is always trying to maximize the defender's minimum loss, but they will try to attack the least-defended aspect of the system and force the defender to spread their resources thinly. The changing objectives are modeled as different loss functions in the inner objective function. Some of these loss functions operate at different scales and therefore some experimentation will be required to harmonize them.

A successful attack is modeled as closing a node for several periods. Reinforcement actions reduce the number of periods that a node remains closed and/or the loss due to node closure. They also reduce the probability of a successful attack. The other possible action is building an intermodal transfer facility (IMTF), which reduces the cost and time to transfer cargo from the river to rail or roads.

2.5.1 Economic Loss

The first loss function captures the direct economic loss due to node closure. The value of flow through a node during the period t is denoted by λ_{jt} and includes spoilage cost as well as transportation. During a successful attack on an unreinforced node without an IMTF, all flow is assumed to be destroyed - i.e. the loss is λ_{jt} . In subsequent periods the flow must be offloaded at smaller riverside docks, which have greatly reduced capacity compared to water transport. This capacity restriction results in a δ_{1jt} % increase in total cost, much of which is due to spoilage while waiting to unload, although transportation cost increases as well. A second successful attack on a closed node extends the closure period.

Constructing an IMTF reduces the cost to offload product onto rail and trucks by δ_{2jt} %; that is, the marginal cost increase is $\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$. The cost increases are indexed by time because transportation rates vary by season and because capacity restrictions may result in spoilage costs while waiting to offload. Reinforcement shortens the time to reopen a node from H_j to h_j . Table 2 summarizes the losses for each of the cases. Determining the parameters for this particular loss function is expected to require solving a max-flow problem in the underlying time-expanded network.

Turning this around, for a given node $j \in N$ in time period $t \in T$, the reinforcement, IMTF, and attack actions of the last H_j periods must be considered. It is important not to double count the losses due to a successful attack on a closed node. The definitions of the decision variables are given

	No IMTF	Open IMTF
Unreinforced	<ul style="list-style-type: none"> • λ_{jt} in period of attack • $\delta_{1jt}\lambda_{jt}$ in next $H_j - 1$ 	$\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$ for H_j periods
Reinforced	<ul style="list-style-type: none"> • λ_{jt} in period of attack • $\delta_{1jt}\lambda_{jt}$ in next $h_j - 1$ 	$\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$ for h_j periods

Note that $H_j > h_j$.

Definition 2.1.

$$L_{jt}(w, x, y, \omega) = \max\{\lambda_{jt}\omega_{jt}(1 - X_{jt}) \quad (9)$$

$$\lambda_{jt}\omega_{j\tau}(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad t - h_j \leq \tau \leq t - 1 \quad (10)$$

$$\lambda_{jt}\omega_{j\tau}(1 - W_{j\tau})(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad (11)$$

$$t - H_j \leq \tau \leq t - h_j - 1\}$$

Linearizing this gives:

$$l_{jt}^\omega \geq \omega_{jt}(1 - X_{jt}) \quad (12)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad \forall t - h_j \leq \tau \leq t - 1 \quad (13)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(1 - W_{j\tau})(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad \forall t - H_j \leq \tau \leq t - h_j - 1 \quad (14)$$

$$l_{jt}^\omega \geq 0 \quad (15)$$

2.5.2 Difference between relaxed worst-case and best-case losses

Defending against a large but unlikely loss may divert resources from smaller but more likely attacks. This is the motivation behind relaxing the uncertainty set. The defender would in general prefer to invest in reinforcements in a way that minimizes the range of losses; in effect, they are attempting to increase the convergence of their reinforcement efforts. When the worst-case loss is large but unlikely, investing heavily in reducing the worst-case loss may leave the defended vulnerable to smaller but likely losses.

While variance or absolute deviation may seem like natural measures of this objective, the use of dynamic scenario probabilities in the model makes them computationally challenging. The range of losses is instead proxied by the worst-case loss in the most likely $\beta\%$ and $1 - \beta\%$ of the losses. Another CVaR constraint is introduced for $1 - \beta\%$ case, and the worst-case loss over the small uncertainty set, called $(1 - \beta) - UC$ is found the same way as over the current set, called $\beta - UC$.

Definition 2.2.

$$L_2(w, x, y, \omega) = \max_{\omega | P_\omega \in \beta - UC} L(w, x, y, \omega) - \max_{\omega | P_\omega \in (1 - \beta) - UC} L(w, x, y, \omega) \quad (16)$$

2.5.3 Approximate Expected Loss

While calculating the expected loss directly leads to a nonlinear programming problem, using the percentiles of the distribution of log-probabilities leads to a way to proxy it. Create n CVaR constraints for the percentiles β_i , $i = 1..n$. This model is formulated with $n = 10$ and $\beta_i = 0, 0.1, \dots, 0.9$. An auxiliary decision variable f_ω^i is introduced, with $f_\omega^i = 1$ if p_ω is in the i th

percentile and 0 otherwise. The total number of scenarios in the i th percentile is $\sum f_{\omega}^i$, and estimate the probability of each one as $\frac{0.1}{\sum f_{\omega}^i}$.

Definition 2.3.

$$E(L(w, x, y, \omega)) = \sum_{i=0}^{0.9} \sum_{\omega \in \Omega} \frac{0.1 f_{\omega}^i L(w, x, y, \omega)}{\sum f_{\omega}^i} \quad (17)$$

2.5.4 Other loss functions

Downtime It may be possible to extract the total system downtime and use it as a loss function. A preliminary attempt suggests that the size of the model may blow up.

Probability of Success It would be desirable to include an objective that maximized the probability that at least one attack succeeded, but I am not sure how to model it given the current structure.

3 Multi-period Robust Network Fortification Problem with Adaptive Adversary

This is the fully expanded version of the high-level model above. Besides linearizing many of the constraints, this model uses a Conditional-Value-at-Risk (CVaR) constraint to capture membership in the uncertainty set.

3.1 Parameters

- $G = (N, A)$: A directed graph. Nodes represent locks or dams and arcs represent pools.
- T : The set of time periods in the model, indexed by t or τ .
- Ω : The set of all possible successful attacks, which corresponds to the feasible region of the outer optimization problem. If y_0 is a feasible attack that has $y_{jt} = 1$ for some $j \in N$ and $t \in T$, y_1 which has the same components as y_0 except that $y_{jt} = 0$ is also feasible.
- $\Omega(y)$: All possible successful attacks resulting from a feasible attack y . $|\Omega(y)| = 2 \sum \sum y_{jt}$ possible successful attacks.
- $\omega \in \Omega$: An element of Ω or $\Omega(y)$ is called a scenario. ω is a matrix with binary coefficients. ω_j is the row vector of successful attacks on node $j \in N$. $\omega_{jt} = 1$ if node j is successfully attacked in period t , and 0 otherwise.
- a_j : The cost to attack node $j \in N$.
- b_j : The cost to open an IMTF at node $j \in N$.

- c_j : The cost to fortify node $j \in N$.
- B_0 : The attacker's budget.
- B_1 : The defender's budget.
- $\beta \in (0, 1)$: What percentage of the least probable feasible scenarios to ignore.
- δ_{1jt} : The percent increase in cost as a result of switching to land transportation at node $j \in N$ periods $t \in T$ in the absence of an IMTF.
- λ_{jt} : The monetary cost of grain shipped through node $j \in N$ in period $t \in T$ in the absence of failures. Suppose x^* is the solution to the deterministic capacitated min-cost network flow model over a time expanded network. Each time period is represented by a set of nodes $N(t)$ which form a layer in the network. The minimum time to transit each arc $(ij) \in A$ in the original network is given by t_{min}^{ij} . Each outgoing arc (ji) from j in the original network is transformed into a set of arcs $(ij\tau) \in \{t + t_{min}^{ij} \dots t_{max}\}$ connecting node $j \in N(t)$ to $i \in N(\tau)$, representing the flow departing node i during period t and arriving at node j in a later period τ . The cost of arc $(ij\tau)$ is $C_{ij} = c_{ij} + f(\tau - t)$, where c_{ij} is the transportation cost for arc $(ij) \in A$ and $f(\tau - t)$ gives the spoilage costs during a delay of $\tau - t$. So $\lambda_{jt} = \sum_{(ij\tau)} C_{ij} x^*_{ij\tau}$.
- p_j : Before reinforcement, the probability that node $j \in N$ fails when attacked.
- r_j : After reinforcement, the probability that node $j \in N$ fails when attacked.
- ω_{jt} : 1 if node $j \in N$ is successfully attacked in scenario $\omega \in \Omega$, and 0 if it survives or is not attacked.
- H_j : The number of periods that an unreinforced node $j \in N$ is closed after a successful attack.
- $h_j < H_j$: The number of periods that a reinforced node $j \in N$ is closed after a successful attack.

3.2 Decision Variables

- w_{jt} : For each node $j \in N$, $w_{jt} = 1$ if a fortification action is applied to node j in period $t \in T$, and 0 otherwise.

- W_{jt} : For each node $j \in N$, $W_{jt} = 1$ if node j is protected by fortification in period $\{1, \dots, t\}$, and 0 otherwise. In other words, $W_{jt} = \sum_{t \in T} w_{jt}$.
- x_{jt} : For each node $j \in N$, $x_{jt} = 1$ if an IMTF is constructed during period $t \in T$, and 0 otherwise.
- X_{jt} : For each node $j \in N$, $X_{jt} = 1$ if an IMTF is open in period $t \in T$, and 0 otherwise. In other words, $X_{jt} = \sum_{t \in T} x_{jt}$.
- y_{jt} : For each node $j \in N$, $y_{jt} = 1$ if node j is attacked in period $t \in T$, and 0 otherwise.
- z_{jt} : For each node $j \in N$, z_{jt} linearizes the product $w_{jt}y_{jt}$. $z_{jt} = 1$ if node i is fortified and attacked.
- L : The maximum loss over the most likely $1 - \beta\%$ of the feasible failure scenarios $\omega \in \Omega(y)$.
- l^ω : The loss in each scenario $\omega \in \Omega$. For feasible scenarios $\omega \in \Omega(y)$, $l^\omega = L(w, x, y, \omega)$ as defined in Section C.3. For infeasible scenarios $\omega \notin \Omega(y)$, $l^\omega = 0$.
- f_ω : For each scenario $\omega \in \Omega$, $f_\omega = 0$ if $\omega \in \Omega(y)$ and 1 if $\omega \notin \Omega(y)$.
- $p_\omega = \ln(P(\omega))$ for all $\omega \in \Omega$.
- ξ : At optimality, $\xi = p_{\omega\beta}$, where $\sum_{\omega | P(\omega) < P(\omega\beta)} P(\omega) \leq \beta$.
- ζ_ω : For infeasible scenarios $\omega \notin \Omega(y)$ and for the least probable $\beta\%$ of the feasible scenarios, $\zeta_\omega = 0$. Otherwise, $\zeta_\omega = P(\omega) - \xi$.
- z_ω : Linearizes the product ξf_ω for each scenario $\omega \in \Omega$.

3.3 Outer Problem: Attacker

$$\text{Maximize } H(w, x, z) \tag{18}$$

Subject to:

$$\sum_{j \in N} \sum_{t \in T} a_j y_{jt} \leq B_0 \tag{19}$$

$$y_{jt} \in \{0, 1\} \quad \forall j \in N \tag{20}$$

3.4 Inner Problem: Defender

$$H(w, x, z) = \text{Minimize } L \tag{21}$$

Subject to:

$$\sum_{j \in N} c_j w_{jt} + b_j x_{jt} \leq B_1 \quad (22)$$

$$f_\omega \geq \omega_{jt} - y_{jt} \quad \forall \omega \in \Omega, j \in N, t \in T \quad (23)$$

$$L \geq L_1^{0.9} \quad (24)$$

$$L \geq L_1^{0.9} - L_1^{0.1} \quad (25)$$

$$L \geq \sum_{i=0}^{0.9} \sum_{\omega \in \Omega} L_{3\omega}^i \quad (26)$$

$$L_{1,\omega}^i \geq \sum_{j \in N} \sum_{t \in T} l_{jt}^\omega - M(F_\omega^i - \zeta_\omega^i + 1) \quad \forall \omega \in \Omega, i = 0, 0.1, \dots, 0.9 \quad (27)$$

$$l_{jt}^\omega \geq \lambda_{jt} \omega_{jt} (1 - x_{j\tau}) \quad \forall \tau \in \{1, \dots, t\} \quad (28)$$

$$l_{jt}^\omega \geq \lambda_{jt} \omega_{j\tau} (\delta_{1jt} - X_{j\tau} \delta_{2jt}) \quad \forall t - h_j \leq \tau \leq t - 1 \quad (29)$$

$$l_{jt}^\omega \geq \lambda_{jt} \omega_{j\tau} (1 - W_{j\tau}) (\delta_{1jt} - X_{j\tau} \delta_{2jt}) \quad \forall t - H_j \leq \tau \leq t - h_j - 1 \quad (30)$$

$$\sum_{i=0}^{0.9} \sum_{\omega \in \Omega} L_{3\omega}^i \geq \sum_{i=0}^{0.9} \sum_{\omega \in \Omega} 0.1 L_{1,\omega}^i \quad (31)$$

$$W_{jt} \geq w_{j\tau} \quad \forall \tau \in \{1, \dots, t\}, t \in T \quad (32)$$

$$X_{jt} \geq x_{j\tau} \quad \forall \tau \in \{1, \dots, t\}, t \in T \quad (33)$$

$$z_{jt} \geq w_{jt} + y_{jt} - 1 \quad (34)$$

$$\sum_{\omega \in \Omega} z_\omega^i + \frac{1}{(1 - \beta_i)} \sum_{\omega \in \Omega} \zeta_\omega^i \leq 0 \quad \forall i \in \{0, 0.1, \dots, 0.9\} \quad (35)$$

$$\zeta_\omega^i \geq p_\omega - \xi^i - M f_\omega \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (36)$$

$$p_\omega \geq \sum_{j \in N} z_{jt} (\ln r_j - \ln p_j) + y_j \ln p_j \quad \forall \omega \in \Omega \quad (37)$$

$$z_\omega^i \geq -M F_\omega^i \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (38)$$

$$z_\omega^i \geq \xi^i \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (39)$$

$$z_\omega^i \geq \xi^i - M(1 - F_\omega^i) \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (40)$$

$$F_\omega^i \geq \frac{z_\omega^i}{k} \quad \forall i \in \{0, 0.1, \dots, 0.9\} \quad (41)$$

$$F_\omega^i = F_\omega^i - F_\omega^{i+1} \quad \forall i \in \{0, 0.1, \dots, 0.8\} \quad (42)$$

$$L_{3\omega}^i \leq -M f_\omega^i \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (43)$$

$$L_{3\omega}^i \leq L_3 \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (44)$$

$$L_{3\omega}^i \geq L_3 - M(1 - f_\omega^i) \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (45)$$

$$w_{jt} \in \{0, 1\} \quad \forall j \in N, t \in T \quad (46)$$

$$x_{jt} \in \{0, 1\} \quad \forall j \in N, t \in T \quad (47)$$

$$w_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (48)$$

$$x_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (49)$$

$$z_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (50)$$

$$L \geq 0 \quad (51)$$

$$l_{jt}^\omega \geq 0 \quad \forall \omega \in \Omega, j \in N, t \in T \quad (52)$$

$$\zeta_\omega^i \geq 0 \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (53)$$

$$f_\omega^i \geq 0 \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (54)$$

$$p_\omega \in \mathbb{R} \quad \forall \omega \in \Omega \quad (55)$$

$$\xi^i \in \mathbb{R} \quad \forall i \in \{0, 0.1, \dots, 0.9\} \quad (56)$$

$$z_\omega^i \leq 0 \quad \forall \omega \in \Omega, i \in \{0, 0.1, \dots, 0.9\} \quad (57)$$

In the outer problem, constraint (19) enforces the attacker's budget, and constraint (20) defines attacks as binary.

In the inner problem, constraint 23 enforces the defender's budget. The next constraint, (24), works with constraint (56) to indicate the feasibility of scenario $\omega \in \Omega$ by setting f_ω to 1 if any node $j \in N$ fails without being attacked in period $t \in T$. The next three constraints, (25), (26) and (27) form the toggle between the three loss functions. The following constraint (28) forces L_ω^i to be the maximum loss among the scenarios in the uncertainty set corresponding to percentile i . (M is some large number). Constraints (29) - (31) and (54) calculates the loss for each scenario $\omega \in \Omega$, regardless of feasibility. Constraint (32) is the fully-linearized version of the estimate of the expected loss and uses the auxiliary variables defined in constraints (110) – (114). Constraints (33) and (34) indicate whether node j is protected by fortification or an IMTF in period t . Constraint (35) enforces the definition of z_{jt} .

This model uses the outer linearization in constraint (36) to discard the least probable $\beta\%$ of node failure scenarios. The “probability” of each scenario is $\frac{1}{\sum f_\omega^i}$, and the “loss” is $\ln P(\omega)$ in the outer linearization of a CVaR constraint. The constraint is scaled by $\sum f_\omega^i$, which results in a

term $\xi^i \cdot \sum f_\omega^i$. This term is linearized by constraints (39) – (41) and (59). At optimality, ξ^i will be the natural log of the cutoff probability for the i th percentile.

Less probable scenarios will have $p_\omega = \ln P(\omega) < \xi^i$. As a result, constraint (37) will be 0 for scenarios $\omega \in \Omega(y)$ with $p_\omega < \xi^i$ or for scenarios $\omega \notin \Omega(y)$. The remaining constraints define the bounds for the decision variables.

4 Constructive Heuristic for Initial Solution

Since both the attacker and defender problems are resource allocation problems, it makes sense to try a greedy approach to the knapsack problems to create an initial solution.

Initialization

1. For each $j \in N$ and $t \in T$, calculate the expected unreinforced loss, $\hat{l}_{jt} = p_j \sum_{\tau=t}^{t+H_j} \delta_{1j\tau} \lambda_{j\tau}$.
2. Create an index set $S := N$ and empty $|N| \times |T|$ matrices w , x , and y .
3. Set the objective value f , the attacker's cost A , the defender's fortification cost D to 0.

Construct Initial Fortifications

1. For each $j \in N$ and $t \in T$, calculate the expected post-fortification losses for each of the three possibilities:
 - $\hat{l}_{jt}^w = r_j \sum_{\tau=t}^{t+h_j} \delta_{1j\tau} \lambda_{j\tau}$
 - $\hat{l}_{jt}^x = p_j \sum_{\tau=t}^{t+H_j} \lambda_{j\tau} \delta_{2j\tau}$
 - $\hat{l}_{jt}^{wx} = r_j \sum_{\tau=t}^{t+h_j} \lambda_{j\tau} \delta_{2j\tau}$
2. Find $(j^*, t^*, \hat{w}_{j^*t^*}, \hat{x}_{j^*t^*})$ that maximizes $\hat{l} = \max_{j \in N, t \in T} \left(\frac{\hat{l}_{jt} - \hat{l}_{jt}^w}{c_j}, \frac{\hat{l}_{jt} - \hat{l}_{jt}^x}{b_j}, \frac{\hat{l}_{jt} - \hat{l}_{jt}^{wx}}{c_j + b_j} \right) \cdot \hat{w}_{j^*t^*}$ and $\hat{x}_{j^*t^*}$ record the reinforcement action(s) that resulted in \hat{l} .
3. If $D + c_{j^*} + b_{j^*} \leq B_1$, set
 - $N := N \setminus \{j^*\}$
 - $D := D + c_{j^*} + b_{j^*}$
 - $w_{j^*,t^*} := \hat{w}_{j^*t^*}$
 - $x_{j^*,t^*} := \hat{x}_{j^*t^*}$
 - $\hat{l}_{j^*,t^*} := \hat{l}_{j^*,t^*} - \hat{l}$ (Updating expected loss).

4. Repeat previous two steps until $B_1 - D < \max_{j \in N} (c_j, b_j)$.

Construct Initial Attacks

1. Create an index set $S := N$.

2. Find $(j^*, t^*) = \arg \max_{j \in N, t \in T} \frac{\hat{i}_{j,t}}{a_j}$.

3. If $A + a_j^* \leq B_0$, set

- $N := N \setminus \{j^*\}$
- $A := A + a_j^*$
- $y_{j^*, t^*} := 1$
- $f :=$

$$f + \sum_{\tau=t}^{t+h_j} \lambda_{j\tau} (\delta_{1j\tau} - \delta_{2j\tau}) + \sum_{\tau=t}^{t+h_j} \lambda_{j\tau} \delta_{2j\tau} + (1 - w_{jt}) \sum_{\tau=t+h_j+1}^{t+H_j} \lambda_{j\tau} (\delta_{1j\tau} - x_{jt} \delta_{2j\tau}).$$

4. Repeat Steps 2-3 until $B_0 - A < \min_{j \in N} a_j$

5.0 RNIFP for Inland Waterways

This model is a bi-level attacker-defender model. The inner optimization problem is a Reliable Network Fortification Problem (RNFP) model, and the outer model is a capital budgeting model. The model is currently a single period model. The model does not currently take into account the probability of each scenario of node failures occurring, merely the losses overall the possible sets of node failures.

As currently formulated, the inner problem is a robust optimization model with an uncertainty set of all possible vectors of node failures for the attack decision y . The model does not consider the probability of each scenario, so the fortification decisions are not included in this iteration. A model that does use probability information to construct an uncertainty set is set out below.

5.1 Parameters

- $G = (N, A)$: A directed graph. Nodes represent locks or dams and arcs represent pools.
- Ω : The set of possible node failures. Each element, called a scenario, is a binary vector of length $2^{|N|}$.

- $\Omega(y) \subseteq \Omega$: The set of possible node failures resulting from an attack decision y .
- a_j : The cost to attack node $j \in N$.
- b_j : The cost to open an IMTF at node $j \in N$.
- B_0 : The attacker's budget.
- B_1 : The defender's budget.
- δ_j : The marginal cost of switching to land transportation at node $j \in N$.
- g : The cost or profit of one unit of grain.
- λ_j : The flow of grain through node $j \in N$ in the absence of failures; may be the solution to a min-cost network flow model.
- $s_j^\omega = 1$ if node $j \in N$ fails in scenario $\omega \in \Omega$, and 0 if it survives.

5.2 Decision Variables

- x_j : For each node $j \in N$, $x_j = 1$ if an intermodal transfer facility (IMTF) has been opened, and 0 otherwise.
- y_j : For each node $j \in N$, $y_j = 1$ if node j is attacked, and 0 otherwise.
- L : The maximum loss over the most likely $1 - \beta\%$ of the feasible failure scenarios $\omega \in \Omega(y)$.
- l^ω : The loss in each scenario $\omega \in \{0, 1\}^{|N|}$. For feasible scenarios $\omega \in \Omega(y)$, $l^\omega = L(y, \omega)$ as defined above. For infeasible scenarios $\omega \notin \Omega(y)$, $l^\omega = 0$.
- f_ω : For each scenario $\omega \in \Omega$, $f_\omega = 0$ if $\omega \in \Omega(y)$ and 1 if $\omega \notin \Omega(y)$.

5.3 Measuring Losses

In this model, the effect of a successful attack is modeled as causing a loss. The losses are defined in terms of cost. For each node $j \in N$ the loss is defined to be:

$$L^j(x, y, s_\omega) = \begin{cases} 0 & s_j^\omega = 0 \\ \lambda_{jg} & s_j^\omega = 1, x_j = 0 \text{ Cost of destroyed grain at } j \\ \lambda_j \delta_{jg} & s_j^\omega = 1, x_j = 0 \text{ Increase in cost to switch modes at } j \end{cases} \quad (58)$$

In terms of the formulation, the loss for each scenario is:

$$L(x, y, s_\omega) = \sum_{j \in N} s_j^\omega \lambda_{jg} (1 - x_j (1 - \delta_j)) \quad (59)$$

The loss (or damage) from attacks may be calculated in many ways. In this loss function, the purpose of the λ_{jg} term is to weight the nodes by importance. Any one of a number of measures of criticality or centrality may be substituted. Similarly, there may be better ways to calculate the loss reduction from opening an IMTF.

5.4 Outer Problem: Attacker

$$\text{Maximize } H(x) \quad (60)$$

Subject to:

$$\sum_{j \in N} a_j y_j \leq B_0 \quad (61)$$

$$y_j \in \{0, 1\} \quad \forall j \in N \quad (62)$$

5.5 Inner Problem: Defender

$$H(x) = \text{Minimize } L \quad (63)$$

Subject to:

$$\sum_{j \in N} b_j x_j \leq B_1 \quad (64)$$

$$f_\omega \geq s_j^\omega - y_j \quad \forall \omega \in \Omega, j \in N \quad (65)$$

$$L \geq l^\omega - M f_\omega \quad \forall \omega \in \Omega \quad (66)$$

$$l^\omega \geq \sum_{j \in N} s_j^\omega \lambda_{jg} (1 - x_j (1 - \delta_j)) \quad \forall \omega \in \Omega \quad (67)$$

$$x_j \in \{0, 1\} \quad \forall j \in N \quad (68)$$

$$L \geq 0 \quad (69)$$

$$l^\omega \geq 0 \quad \forall \omega \in \Omega \quad (70)$$

$$f_\omega \geq 0 \quad \forall \omega \in \Omega \quad (71)$$

In the outer problem, constraint (64) enforces the attacker's budget, and constraint (65) defines attacks as binary. In the inner problem, constraint (68) enforces the defender's budget. The next constraint, (69), works with constraint (75) to indicate the feasibility of scenario $\omega \in \Omega$ by setting f^ω to 1 if any node $j \in N$ fails without being attacked. The following constraint (70) forces L to be the maximum loss among the feasible scenarios (M is some large number). Constraint (71) calculates the loss for each scenario $\omega \in \Omega$, regardless of feasibility. The remaining constraints define the bounds for the decision variables.

6 RNIFP with Uncertainty Sets

This model is a bi-level attacker-defender model. The inner optimization problem is a Reliable Network Fortification Problem (RNFP) model, and the outer model is a capital budgeting model. The model is currently a single period model. As currently formulated, the inner problem is a robust optimization model. This model uses probability information to relax the uncertainty set by discarding the least probable $\beta\%$ of scenarios. This model still does not calculate the expected value of the losses.

6.1 Parameters

- a_j : The cost to attack node $j \in N$.
- b_j : The cost to open an IMTF at node $j \in N$.
- c_j : The cost to fortify node $j \in N$.
- B_0 : The attacker's budget.
- B_1 : The defender's budget.
- $\beta \in (0, 1)$: What percentage of the least probable feasible scenarios to ignore.
- δ_j : The marginal cost of switching to land transportation at node $j \in N$.
- g : The cost or profit of one unit of grain.
- λ_j : The flow of grain through node $j \in N$ in the absence of failures.
- p_j : Before reinforcement, the probability that node $j \in N$ fails when attacked.
- r_j : After reinforcement, the probability that node $j \in N$ fails when attacked.
- $s_j^\omega = 0$ if node $j \in N$ fails in scenario $\omega \in \Omega$, and 1 if it survives.

6.2 Decision Variables

- w_j : For each node $j \in N$, $w_j = 1$ if node j has been fortified, and 0 otherwise.
- x_j : For each node $j \in N$, $x_j = 1$ if an IMTF has been opened, and 0 otherwise.
- y_j : For each node $j \in N$, $y_j = 1$ if node j is attacked, and 0 otherwise.
- z_j : For each node $j \in N$, z_j linearizes the product $w_j y_j$. $z_j = 1$ if node i is fortified and attacked.
- L : The maximum loss over the most likely $1 - \beta\%$ of the feasible failure scenarios $\omega \in \Omega(y)$.

- l^ω : The loss in each scenario $\omega \in \{0, 1\}^{|\Omega|}$. For feasible scenarios $\omega \in \Omega(y)$, $l^\omega = L(y, \omega)$ as defined above. For infeasible scenarios $\omega \notin \Omega(y)$, $l^\omega = 0$.
- f_ω : For each scenario $\omega \in \Omega$, $f_\omega = 0$ if $\omega \in \Omega(y)$ and 1 if $\omega \notin \Omega(y)$.
- $p_\omega = \ln(P(\omega))$ for all $\omega \in \Omega$.
- ζ_ω : For infeasible scenarios $\omega \notin \Omega(y)$ and for the least probable $\beta\%$ of the feasible scenarios, $\zeta_\omega = 0$. Otherwise, $\zeta_\omega = p_\omega - \xi$.

6.3 Outer Problem: Attacker

$$\text{Maximize } H(w, x, z) \quad (72)$$

Subject to:

$$\sum_{j \in N} a_j y_j \leq B_0 \quad (73)$$

$$y_j \in \{0, 1\} \quad \forall j \in N \quad (74)$$

6.4 Inner Problem: Defender

$$H(w, x, z) = \text{Minimize } L \quad (75)$$

Subject to:

$$\sum_{j \in N} c_j w_j + b_j x_j \leq B_1 \quad (76)$$

$$f_\omega \geq s_j^\omega - y_j \quad \forall \omega \in \Omega, j \in N \quad (77)$$

$$L \geq l^\omega - M(f_\omega - \zeta_\omega + 1) \quad \forall \omega \in \Omega \quad (78)$$

$$l^\omega \geq \sum_{j \in N} s_j^\omega \lambda_{jg} (1 - x_j(1 - \delta_j)) \quad \forall \omega \in \Omega \quad (79)$$

$$z_j \geq w_j + y_j - 1 \quad \forall j \in N \quad (80)$$

$$\xi + \frac{1}{(1 - \beta) \sum_{\omega \in \Omega} 1 - f_\omega} \sum_{\omega \in \Omega} \zeta_\omega \leq 0 \quad (81)$$

$$\zeta_\omega \geq p_\omega - \xi - M f_\omega \quad \forall \omega \in \Omega \quad (82)$$

$$p_\omega \geq \sum_{j \in N} z_j (\ln r_j - \ln p_j) + y_j \ln p_j \quad \forall \omega \in \Omega \quad (83)$$

$$w_j \in \{0, 1\} \quad \forall j \in N \quad (84)$$

$$x_j \in \{0, 1\} \quad \forall j \in N \quad (85)$$

$$z_j \geq 0 \quad \forall j \in N \quad (86)$$

$$L \geq 0 \quad (87)$$

$$l^\omega \geq 0 \quad \forall \omega \in \Omega \quad (88)$$

$$\zeta_\omega \geq 0 \quad \forall \omega \in \Omega \quad (89)$$

$$f_\omega \geq 0 \quad \forall \omega \in \Omega \quad (90)$$

$$p_\omega \in \mathbb{R} \quad \forall \omega \in \Omega \quad (91)$$

$$\xi \in \mathbb{R} \quad (92)$$

In the outer problem, constraint (78) enforces the attacker's budget, and constraint (79) defines attacks as binary.

In the inner problem, constraint (82) enforces the defender's budget. The next constraint, (83), works with constraint (96) to indicate the feasibility of scenario $\omega \in \Omega$ by setting f_ω to 1 if any node $j \in N$ fails without being attacked. The following constraint (84) forces L to be the maximum loss among the scenarios in the uncertainty set (M is some large number). Constraint (85) calculates the loss for each scenario $\omega \in \Omega$, regardless of feasibility. Constraint 86 enforces the definition of z_j .

This model uses the outer linearization in constraint (87) to discard the least probable $\beta\%$ of node failure scenarios. The “probability” of each scenario is $\frac{1}{\sum 1-f_\omega}$, and the “loss” is $\ln P(\omega)$ in the outer linearization of a conditional value-at-risk (CVaR) constraint. At optimality, ξ will be the natural log of the cutoff probability. Less probable scenarios will have $p_\omega = \ln P(\omega) < \xi$. As a result, constraint (88) will be 0 for scenarios $\omega \in \Omega(y)$ with $p_\omega < \xi$ or for scenarios $\omega \notin \Omega(y)$. The remaining constraints define the bounds for the decision variables.

7 Multi-period RNIFP with Uncertainty Sets

This model is a bi-level attacker-defender model. The inner optimization problem is a Multi-period Reliable Network Fortification Problem (RNFP) model, and the outer model is a capital budgeting model. As currently formulated, the inner problem is a robust optimization model. This model uses probability information to relax the uncertainty set by discarding the least probable $\beta\%$ of scenarios. This model still does not calculate the expected value of the losses.

7.1 Parameters

- $G = (N, A)$: A directed graph. Nodes represent locks or dams and arcs represent pools.
- T : The set of time periods in the model, indexed by t or τ .
- Ω : The set of all possible successful attacks, which corresponds to the feasible region of the outer optimization problem. If y_0 is a feasible attacks that has $y_{jt} = 1$ for some $j \in N$ and $t \in T$, y_1 which has the same components as y_0 except that $y_{jt} = 0$ is also feasible.
- $\Omega(y)$: All possible successful attacks resulting from a feasible attack y . $|\Omega(y)| = 2^{\sum \sum y_{jt}}$ possible successful attacks.
- $\omega \in \Omega(y)$: An element of Ω or $\Omega(y)$ is called a scenario. ω is a $|N| \times |T|$ matrix with binary coefficients. ω_j is the row vector of successful attacks on node $j \in N$. $\omega_{jt} = 1$ if node j is successfully attacked in period t , and 0 otherwise.
- a_j : The cost to attack node $j \in N$.
- b_j : The cost to open an IMTF at node $j \in N$.
- c_j : The cost to fortify node $j \in N$.
- B_0 : The attacker's budget.
- B_1 : The defender's budget.
- $\beta \in (0, 1)$: What percentage of the least probable feasible scenarios to ignore.
- δ_{1jt} : The percent increase in cost as a result of switching to land transportation at node $j \in N$ periods $t \in T$ in the absence of an IMTF.
- δ_{2jt} : The percent cost reduction when switching to land transportation if an IMTF is open at node $j \in N$. $\delta_{2jt} > \delta_{1jt}$. For clarification, see the loss function in Subsection 2.5.1.
- λ_{jt} : The monetary cost of grain shipped through node $j \in N$ in period $t \in T$ in the absence of failures. Suppose x^* is the solution to the deterministic capacitated min-cost network flow model over a time expanded network. Each time period is represented by a set of nodes $N(t)$ which form a layer in the network. The minimum time to transit each arc $(ij) \in A$ in the original network is given by t_{min}^{ij} . Each outgoing arc (ji) from j in the original network is transformed into a set of arcs $(ijt\tau) \in \{t + t_{min}^{ij} \dots t_{max}\}$ connecting node $j \in N(t)$ to $i \in N(\tau)$, representing the flow departing node i during period t and arriving at node j in a later period τ . The cost of arc $(ijt\tau)$ is $C_{ij} = c_{ij} + f(\tau - t)$, where

c_{ij} is the transportation cost for arc $(ij) \in A$ and $f(\tau - t)$ gives the spoilage costs during a delay of $\tau - t$. So $\lambda_{jt} = \sum_{(ij \in A)} c_{ij} x^*_{ijt} \tau$.

- p_j : Before reinforcement, the probability that node $j \in N$ fails when attacked.
- r_j : After reinforcement, the probability that node $j \in N$ fails when attacked.
- ω_{jt} : 1 if node $j \in N$ is successfully attacked in scenario $\omega \in \Omega$, and 0 if it survives or is not attacked.
- H_j : The number of periods that an unreinforced node $j \in N$ is closed after a successful attack.
- $h_j < H_j$: The number of periods that a reinforced node $j \in N$ is closed after a successful attack.

7.2 Decision Variables

- w_{jt} : For each node $j \in N$, $w_{jt} = 1$ if a fortification action is applied to node j in period $t \in T$, and 0 otherwise.
- W_{jt} : For each node $j \in N$, $W_{jt} = 1$ if node j is protected by fortification in period $\{1, \dots, t\}$, and 0 otherwise. In other words, $W_{jt} = \sum_{t \in T} w_{jt}$.
- x_{jt} : For each node $j \in N$, $x_{jt} = 1$ if an IMTF is constructed during period $t \in T$, and 0 otherwise.
- X_{jt} : For each node $j \in N$, $X_{jt} = 1$ if an IMTF is open in period $t \in T$, and 0 otherwise. In other words, $X_{jt} = \sum_{t \in T} x_{jt}$.
- y_{jt} : For each node $j \in N$, $y_{jt} = 1$ if node j is attacked in period $t \in T$, and 0 otherwise.
- z_{jt} : For each node $j \in N$, z_{jt} linearizes the product $w_{jt}y_{jt}$. $z_{jt} = 1$ if node i is fortified and attacked.
- L : The maximum loss over the most likely $1 - \beta\%$ of the feasible failure scenarios $\omega \in \Omega(y)$.
- l^ω : The loss in each scenario $\omega \in \Omega$. For feasible scenarios $\omega \in \Omega(y)$, $l^\omega = L(w, x, y, \omega)$ as defined in Section C.3. For infeasible scenarios $\omega \notin \Omega(y)$, $l^\omega = 0$.
- f_ω : For each scenario $\omega \in \Omega$, $f_\omega = 0$ if $\omega \in \Omega(y)$ and 1 if $\omega \notin \Omega(y)$.
- $p_\omega = \ln(P(\omega))$ for all $\omega \in \Omega$.

- ξ : At optimality, $\xi = p_{\omega\beta}$, where $\sum_{\omega|P(\omega)<P(\omega\beta)} P(\omega) \leq \beta$.
- ζ_{ω} : For infeasible scenarios $\omega \notin \Omega(y)$ and for the least probable $\beta\%$ of the feasible scenarios, $\zeta_{\omega} = 0$. Otherwise, $\zeta_{\omega} = P(\omega) - \xi$.
- z_{ω} : Linearizes the product ξf_{ω} for each scenario $\omega \in \Omega$.

7.3 Loss Function

In this model a successful attack closes a node for several periods. The value of flow through a node during the period t is denoted by λ_{jt} and includes spoilage cost as well as transportation. During a successful attack on an unreinforced node without an IMTF, all flow is assumed to be destroyed - i.e. the loss is λ_{jt} . In subsequent periods the flow must be offloaded at expensive private riverside docks, resulting in a $\delta_{1jt}\%$ increase in total cost. A second successful attack on a closed node extends the closure period.

Constructing an IMTF reduces the cost to offload product onto rail and trucks by $\delta_{2jt}\%$; that is, the marginal cost increase is $\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$. The cost increases are indexed by time because transportation rates vary by season and because during the high season capacity restrictions may result in spoilage costs while waiting to offload. Reinforcement shortens the time to reopen a node from H_j to h_j . Table 2 summarizes the losses for each cases.

	No IMTF	Open IMTF
Unreinforced	<ul style="list-style-type: none"> • λ_{jt} in period of attack • $\delta_{1jt}\lambda_{jt}$ in next $H_j - 1$ 	$\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$ for H_j periods
Reinforced	<ul style="list-style-type: none"> • λ_{jt} in period of attack • $\delta_{1jt}\lambda_{jt}$ in next $h_j - 1$ 	$\lambda_{jt}(\delta_{1jt} - \delta_{2jt})$ for h_j periods

Note that $H_j > h_j$.

Turning this around, for a given node $j \in N$ in time period $t \in T$, the reinforcement, IMTF, and attack actions of the last H_j periods must be considered. It is important not to double count the losses due to a successful attack on a closed node.

Definition 7.1.

$$L_{jt}(w, x, y, \omega) = \max\{\lambda_{jt}\omega_{jt}(1 - X_{jt}) \quad (93)$$

$$\lambda_{jt}\omega_{j\tau}(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad t - h_j \leq \tau \leq t - 1 \quad (94)$$

$$\lambda_{jt}\omega_{j\tau}(1 - W_{j\tau})(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad (95)$$

$$t - H_j \leq \tau \leq t - h_j - 1\}$$

Linearizing this gives:

$$l_{jt}^\omega \geq \omega_{jt}(1 - X_{jt}) \quad (96)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad \forall t - h_j \leq \tau \leq t - 1 \quad (97)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(1 - W_{j\tau})(\delta_{1jt} - X_{jt}\delta_{2jt}) \quad \forall t - H_j \leq \tau \leq t - h_j - 1 \quad (98)$$

$$l_{jt}^\omega \geq 0 \quad (99)$$

7.4 Outer Problem: Attacker

$$\text{Maximize } H(w, x, z) \quad (100)$$

Subject to:

$$\sum_{j \in N} \sum_{t \in T} a_j y_{jt} \leq B_0 \quad (101)$$

$$y_{jt} \in \{0, 1\} \quad \forall j \in N \quad (102)$$

7.5 Inner Problem: Defender

$$H(w, x, z) = \text{Minimize } L \quad (103)$$

Subject to:

$$\sum_{j \in N} c_j w_{jt} + b_j x_{jt} \leq B_1 \quad (104)$$

$$f_\omega \geq \omega_{jt} - y_{jt} \quad \forall \omega \in \Omega, j \in N, t \in T \quad (105)$$

$$L \geq \sum_{j \in N} \sum_{t \in T} l_{jt}^\omega - M(f_\omega - \zeta_\omega + 1) \quad \forall \omega \in \Omega \quad (106)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(1 - x_{jt}) \quad \forall \tau \in \{1, \dots, t\} \quad (107)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(\delta_{1j\tau} - X_{jt}\delta_{2j\tau}) \quad \forall t - h_j \leq \tau \leq t - 1 \quad (108)$$

$$l_{jt}^\omega \geq \lambda_{jt}\omega_{j\tau}(1 - W_{j\tau})(\delta_{1j\tau} - X_{jt}\delta_{2j\tau}) \quad \forall t - H_j \leq \tau \leq t - h_j - 1 \quad (109)$$

$$W_{jt} \geq w_{j\tau} \quad \forall \tau \in \{1, \dots, t\}, t \in T \quad (110)$$

$$X_{jt} \geq x_{j\tau} \quad \forall \tau \in \{1, \dots, t\}, t \in T \quad (111)$$

$$z_{jt} \geq w_{jt} + y_{jt} - 1 \quad (112)$$

$$\sum_{\omega \in \Omega} z_{\omega} + \frac{1}{(1-\beta)} \sum_{\omega \in \Omega} \zeta_{\omega} \leq 0 \quad (113)$$

$$\zeta_{\omega} \geq p_{\omega} - \xi - M f_{\omega} \quad \forall \omega \in \Omega \quad (114)$$

$$p_{\omega} \geq \sum_{j \in N} z_{jt} (\ln r_j - \ln p_j) + y_j \ln p_j \quad \forall \omega \in \Omega \quad (115)$$

$$z_{\omega} \geq -M(1 - f_{\omega}) \quad \forall \omega \in \Omega \quad (116)$$

$$z_{\omega} \geq \xi \quad \forall \omega \in \Omega \quad (117)$$

$$z_{\omega} \geq \xi - M(f_{\omega}) \quad \forall \omega \in \Omega \quad (118)$$

$$w_{jt} \in \{0, 1\} \quad \forall j \in N, t \in T \quad (119)$$

$$x_{jt} \in \{0, 1\} \quad \forall j \in N, t \in T \quad (120)$$

$$w_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (121)$$

$$x_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (122)$$

$$z_{jt} \geq 0 \quad \forall j \in N, t \in T \quad (123)$$

$$L \geq 0 \quad (124)$$

$$l_{jt}^{\omega} \geq 0 \quad \forall \omega \in \Omega, j \in N, t \in T \quad (125)$$

$$\zeta_{\omega} \geq 0 \quad \forall \omega \in \Omega \quad (126)$$

$$f_{\omega} \geq 0 \quad \forall \omega \in \Omega \quad (127)$$

$$p_{\omega} \in \mathbb{R} \quad \forall \omega \in \Omega \quad (128)$$

$$\xi \in \mathbb{R} \quad (129)$$


$$z_{\omega} \leq 0 \quad \forall \omega \in \Omega \quad (130)$$

In the outer problem, constraint (108) enforces the attacker's budget, and constraint (109) defines attacks as binary.

In the inner problem, constraint (112) enforces the defender's budget. The next constraint, (113), works with constraint 135 to indicate the feasibility of scenario $\omega \in \Omega$ by setting f_{ω} to 1 if any node $j \in N$ fails without being attacked in period $t \in T$. The following constraint (114) forces L to be the maximum loss among the scenarios in the uncertainty set (M is some large number). Constraints (115) - (117) and (133) calculates the loss for each scenario $\omega \in \Omega$, regardless of feasibility. Constraints (118) and (119) indicate whether node j is protected by fortification or an IMTF in period t . Constraint (120) enforces the definition of z_{jt} .

This model uses the outer linearization in constraint (121) to discard the least probable $\beta\%$ of node failure scenarios. The “probability” of each scenario is $\frac{1}{\sum(1-f_\omega)}$, and the “loss” is $\ln P(\omega)$ in the outer linearization of a conditional value-at-risk CVaR constraint. The constraint is scaled by $\sum(1 - f_\omega)$, which results in a term $\xi \cdot \sum f_\omega$. This term is linearized by constraints (124) – (126) and (138). At optimality, ξ will be the natural log of the cutoff probability. Less probable scenarios will have $p_\omega = \ln P(\omega) < \xi$. As a result, constraint (122) will be 0 for scenarios $\omega \in \Omega(y)$ with $p_\omega < \xi$ or for scenarios $\omega \notin \Omega(y)$. The remaining constraints define the bounds for the decision variables.

Appendix B.
Student Poster Presentations



UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

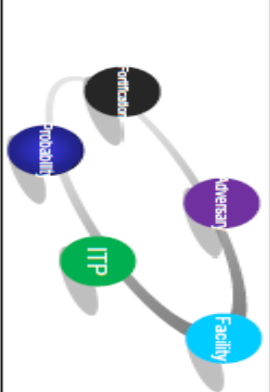
Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks

N. Oktun Bayek
University of Arkansas, Department of Industrial Engineering

INTRODUCTION

- More than 80% of the farm exports move on the Inland Waterways.¹⁾
- 90% of U.S. corn destined for export travels on the Mississippi and one-half of the total freight tonnage carried on the Upper Mississippi is corn.²⁾
- Supply chain infrastructure (locks, dams, bridges) is very old and subject to failure.
- Disruptions to multi-modal perishable commodity supply chains due to natural or intentional resulting in economic losses and delays in deliveries.

KEY ELEMENTS



RESEARCH QUESTION

- How to allocate the scarce fortification resources so that the supply chain resiliency is maximized?

DEFENDER DECISIONS

- Determine which nodes to fortify depending on adversary scenarios that are subject to budgetary constraints.
- Determine which intermodal transfer points to open depending on the node failures in each period.

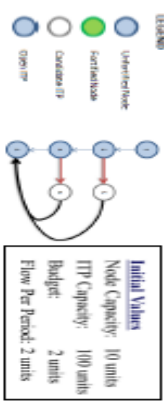
ADVERSARY SCENARIOS

- All realistic combinations of attack scenarios
- All possible node failure combinations

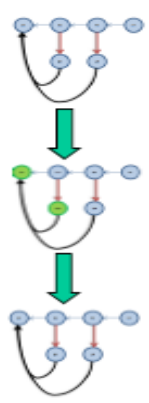
RESULTS

LEGEND

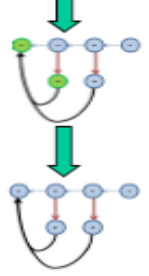
- User/inter-Node
- Scenario
- Candidate
- Open



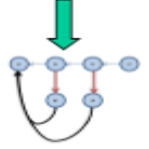
PERIOD 1



PERIOD 2



PERIOD 3



INITIAL VALUES

BUDGET: 10 units

SCENARIO PROBABILITIES ARE DOUBLED

BUDGET: 10 units

SCENARIO PROBABILITIES ARE DOUBLED and

BUDGET: 10 units

CONTRIBUTION

- Adaptive behavior of the adversary.
- Perishability concerns on a time-expanded network.
- Focus on inland waterway/ infrastructure components.
- Post-fortification failility.

SOLUTION METHODOLOGY

- Supply chain disruption model with fortification, resiliency, and budget constraints including nonlinear inequalities.
- Probability of node failure in each period updated according to fortification actions of previous period.
- Utilization of MINLP solver Couenne for exact solution.

CONCLUSION

- The effect of the probabilities on the fortification actions are observed.
- Behavior of the adversary is considered.
- Different instances are solved by using Couenne and the capability of solving bigger instances are analyzed.

REFERENCES

1. http://www.usace.army.mil/doss/OTNV/OTNhandbook_10es.pdf
2. Fretell, J.F. 2005. CRS Report for Congress, Grain Transport: Modal Trends and Infrastructure Implications. January 5, 2005

ACKNOWLEDGEMENTS

I thank my supervisors Chase Rainwater, Edward Poni, Ashlea Milburn, and Scott Mason for their support for my study.

4/30/2014

Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks

MBTC DHS-1109 – Department of Industrial Engineering

Dr. Edward A. Pohl, Dr. Ashlea Milburn, Dr. Chase E. Rainwater, Dr. Scott J. Mason, Dia St. John, Juliana Bright

MACK-BLACKWELL
Rural Transportation Center



MOTIVATION

- Disruptions to multi-modal perishable commodity supply chains due to natural hazards or malicious adversaries result in spoilage and downstream delays
- These effects can be minimized through informed infrastructure fortification actions aimed at maximizing system resiliency
- Structural reinforcement
- Additional security measures
- Redundancy of critical components
- Add intermodal transfer facilities
- Bulk transportation of corn along the Upper Mississippi River via barge provides our motivating case study
- 80% of U.S. corn destined for export travels on the Mississippi and one-half of the total freight tonnage carried on the Upper Mississippi is corn.^[1]



UNIQUE CONTRIBUTIONS

- Adaptive adversarial objective
- Multi-modal risk mitigation strategies
- Focus on inland waterways
- Perishability concerns
- Post-fortification failility
- Fortification lowers the failure probability of a facility, without removing the possibility of failure altogether



IMPACT

- Resulting decision framework will guide the allocation of DHS resources for inland waterway infrastructure fortification
- Protection provided to important supply chains (bulk commodity export, agriculture, energy)
- Model can be extended to various supply chain risk scenarios

MODEL DEFINITIONS

- Fortification actions refer to investments that increase system resiliency, including structural reinforcement, added security measures, and component redundancy.
- Attacks refer to any adversarial action or natural hazard that attempts to disrupt the supply chain.
- The targets of fortifications and attacks are river infrastructure components, primarily locks and dams.

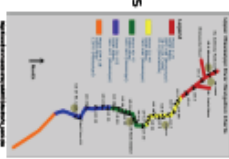


DEFENDER DECISIONS

- Determine which nodes to fortify
- Dependent on adversary decisions

ADVERSARY DECISIONS

- Subject to budgetary constraints
- Determine which nodes to attack
- Based on adaptive objective
- Chosen according to fortification decisions
- Subject to budgetary constraints



CURRENT DIRECTIONS

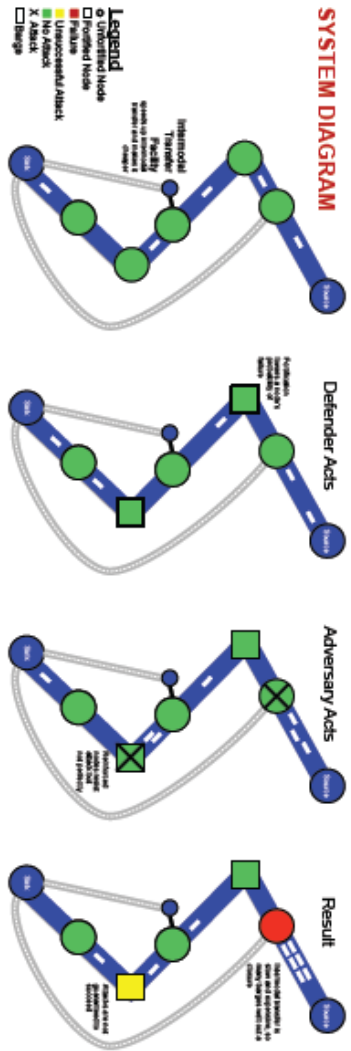
- Bi-level network flow model with nonlinear outer problem constraints
- Co-evolutionary bi-level heuristic solution method
- Bi-level robust network fortification model using Conditional Value-at-Risk constraints to determined the uncertain set
- Genetic algorithm heuristic solution method

REFERENCES

1. Fittell, J.F. 2005. CRS Report for Congress. Grain Transport: Modal Trends and Infrastructure Implications. January 5, 2005

Acknowledgment: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-SF-201-1-9303. Disclaimer: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official position, either expressed or implied, of the U.S. Department of Homeland Security.

SYSTEM DIAGRAM



Mitigating Dynamic Risk in Multi-Modal Perishable Commodity Supply Chain Networks

MBTC DHS-1109

Dr. Edward A. Pohl, Dr. Ashlea R. Bennett, Dr. Chase E. Rainwater, Dr. Scott J. Mason, Jessica Spicer, Dia St. John



MOTIVATION

- Supply chain disruptions caused by natural disasters and adversarial actions result in negative economic consequences.
- Fortification of infrastructure components can help reduce the cost of disruptions, but often requires expensive investments.
- At-risk components must be prioritized to maximize system resiliency.
- Our goal is to develop decision support models to maximize present and future resiliency of perishable commodity supply chain networks when allocating scarce fortification resources for multi-modal transportation infrastructure components, considering natural disasters and adversaries with unknown and adaptive objectives.

SPECIAL CONSIDERATIONS

- Prioritizing fortification investment alternatives requires knowledge of:
 - Likelihood and magnitude of potential disruptions
 - Resiliency resulting from alternate strategies
- Imprecise understanding of adversarial objectives will compound the difficulty of decision making.
- Perishability aspect of transported commodities introduces new component into economic consequence function.
- Consideration of multi-modal response plans increases number of investment alternatives.
 - Barge
 - Rail
 - Freight

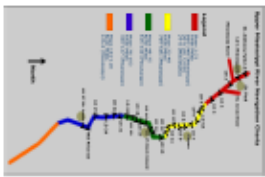
UNIQUE CONTRIBUTIONS

- Unknown and adaptive adversarial objective
- Multi-period interdiction/fortification model
- Integrated fortification and multi-modal risk mitigation strategies
- Focus on inland waterways
- Perishability concerns



MOTIVATING PROBLEM

- Our motivation stems from the bulk transportation of corn along upper Mississippi River via barge.
- 90% of U.S. corn destined for export travels on Mississippi and one-half of total freight tonnage carried on Upper Mississippi is corn.¹¹
- Economic consequences of disruption include spoilage and downstream delays.
- Inland waterway supply chain infrastructure components at risk include:
 - Bridges
 - Locks and Dams
 - Ports
- Fortification decisions include:
 - Reinforcement of Infrastructure components
 - Adding redundancy via multiple transportation modes



INSTANCE DEVELOPMENT

- Gathered data on Mississippi River infrastructure, including locks/dams, bridge crossings, and ports
- Gathered data regarding the flow of corn through the upper Mississippi River
- Began a natural disaster risk assessment for Mississippi River infrastructure
- Exploring multi-modal transportation opportunities along the Mississippi River



TIMELINE

- Phase I: July 2010—March 2011
 - Develop specific instance
 - Focus on supply chain disruptions caused by natural disasters.
- Phase II: February 2011—October 2011
 - Analyze disruptive actions caused by an adversary whose objective is known
- Phase III: September 2011—June 2012
 - Incorporate a dynamically evolving adversarial objective

REFERENCES

- Fittell, J.F. 2005. CRS Report for Congress. Grain Transport Modal Trends and Infrastructure Implications. January 5, 2005 http://www2.mvr.usace.army.mil/NIC2/mrcharts_omnl.cfm

Acknowledgement: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2008 ST 061 15303 October. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Appendix C.

ISERC Presentation


**Mitigating Dynamic Risk in Multi-Modal
Perishable Commodity Supply Chain
Networks**

ISERC 2011

Presenter: *Ola St. John*

Jessica Solcar, Dr. Edward A. Pohl, Dr. Ashlee K. Bennett,
Dr. Chase E. Rainwater, Dr. Scott J. Mason

MACK-BLACKWELL
Rural Transportation Center



General Motivation

- ▶ Economic consequence of supply chain disruptions
 - ▶ Natural hazards
 - ▶ Adversaries
- ▶ Reducing risk through fortification of infrastructure components requires expensive investments
- ▶ Investment decisions should mitigate present and future risk



▶ 3 <http://www.mack-blackwell.com/wp-content/uploads/2010/05/MACK-BLACKWELL-2007-11-15.pdf>
<http://www.rtpg.org/rtg/rtg.html>

Project Specific Motivation

- ▶ Prioritizing fortification investment alternatives requires knowledge of:
 - ▶ Likelihood and magnitude of potential disruptions
 - ▶ Resiliency resulting from alternate strategies
- ▶ Imprecise understanding of adversary compounds difficulty of decision making
 - ▶ Unknown objective
 - ▶ Adaptive objective
- ▶ Consideration of multi-modal response plans increases number of investment alternatives
- ▶ Perishability aspect of transported commodities introduces new component into economic consequence function

▶ 3

Research Focus

- ▶ Develop decision support models to maximize present and future resiliency of perishable commodity supply chain networks when allocating scarce fortification resources for multi-modal transportation infrastructure components
- ▶ Assess supply chain risk via all-hazards perspective:
 - ▶ Natural hazards
 - ▶ Adversaries with unknown and adaptive objectives

▶ 4

Motivating Problem



Bulk transportation of corn along upper Mississippi River via barge

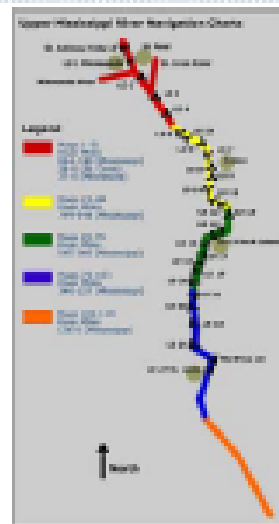
- ▶ 90% of U.S. corn destined for export travels on Mississippi*
- ▶ 1/4 of total freight tonnage carried on Upper Mississippi is corn*
- ▶ Economic consequence of disruption includes spoilage and delays

▶ 5 [Hesselt, J.F. 2009. OIG Report for Congress: Grain Transport: Modal Trends and Infrastructure Implications. January 1, 2009. <http://www.congress.gov/records/committees/transportation-and-infrastructure/legislation/january-1-2009>](http://www.congress.gov/records/committees/transportation-and-infrastructure/legislation/january-1-2009)

Motivating Problem

Inland waterway supply chain components at risk:

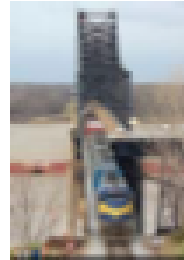
- ▶ Locks and dams
- ▶ Bridges
- ▶ Ports



▶ 6 <http://www.congress.gov/records/committees/transportation-and-infrastructure/legislation/january-1-2009>

Progress to Date

- ▶ Gathered instance data for case study
 - ▶ Focus on Upper Mississippi River
 - ▶ 31 locks and dams
 - ▶ 85 bridge crossings
 - ▶ Natural disaster risk assessment
- ▶ Developed mathematical model
 - ▶ Fallible post-fortification infrastructure components
 - ▶ Budgetary concerns
 - ▶ Rolling time horizon



▶ 7

P-median Fortification Problem (PMFP)

- ▶ Chooses Q facilities to fortify from a set of P existing facilities
- ▶ Facilities fail randomly with probability q
- ▶ Fortified facilities cannot fail
- ▶ Limitations
 - ▶ single time-period
 - ▶ post-fortification infallibility
 - ▶ no budget considerations
 - ▶ lacking network flow structure
 - ▶ no account for perishability

▶ 8

Post-fortification Fallibility Problem (PFFP)

Notation

J = set of existing facilities

I = set of customers served by J facilities

T = set of time periods in the planning horizon

k_{ij} = demand of customer i in time period t

d_i^k = distance from customer i to its k^{th} closest facility

c_{jt} = cost to fortify facility j in time period t

b_t = budget available in period t

r_t = amount of unused budget available for use in time period t

p_j = initial failure probability of facility j

q_{ij}^k = post fortification failure probability of the k^{th} closest facility to customer i at the end of period t

m = factor of fortification

$$w_{ij}^k = \begin{cases} 1 & \text{if facility } j \text{ is the } k^{\text{th}} \text{ closest facility to customer } i \\ 0 & \text{otherwise} \end{cases}$$

$$z_{jt} = \begin{cases} 1 & \text{if facility } j \text{ is fortified at time } t \\ 0 & \text{otherwise} \end{cases}$$

► 9

Budget Allowance Extension

- Total fortification costs in each time period are bounded by the sum of the budget and budget remainder for that period

$$\sum_{j \in J} c_{jt} z_{jt} \leq b_t + r_t \quad \forall t \in T \quad (1)$$

- Budget remainders include unused budget from all previous periods

$$r_t = b_{t+1} + c_{t+1} - \sum_{j \in J} c_{j,t+1} z_{j,t+1} \quad \forall t = 2, \dots, |T| \quad (2)$$

► 10

Post-fortification Fallibility Extension

- ▶ Fortification decreases failure probability by a factor of $1-m$ for each time period
- ▶ Failure probabilities for unfortified facilities remain unchanged

$$q_{i,t}^k = \sum_{j \in J} \alpha_{ij}^k (q_{i,t-1}^j (1 - m_{i,t})) \quad \forall i \in I, k \in J, t = 2, \dots, T \quad (3)$$

- ▶ Period 1 probabilities are based on initial probabilities of failure, p_j

$$q_{i,1}^k = \sum_{j \in J} \alpha_{ij}^k (p_j (1 - m_{i,1})) \quad \forall i \in I, k \in J \quad (4)$$

- ▶ A facility can be fortified in more than one time period

▶ 11

PFFP Objective

- ▶ Minimize total expected demand weighted distance traveled from customers to their closest operational facility over all time periods.

$$\min \sum_{i \in I} \sum_{k \in J} \sum_{t=1}^T h_i d_i^k (1 - q_{i,t}^k) - q_{i,t}^k \prod_{s=1}^{k-1} q_{i,t}^s$$

▶ 12

PFFP Model

$$\min \sum_{w \in T} \sum_{k \in J} \sum_{j \in J} h_{kj} d_{kj}^w (1 - q_k^w) \prod_{l=2, \dots, |T|} q_l^w$$

$$\text{s.t. } \sum_{j \in J} c_j z_j \leq b + \tau \quad \forall w \in T \quad (1)$$

$$\tau = h_{k_1} + c_{k_1} - \sum_{j \in J} c_j p_{k_1 j} \quad \forall w = 2, \dots, |T| \quad (2)$$

$$q_k^w = \sum_{j \in J} v_j^w (p_{kj} (1 - m_{kj})) \quad \forall w \in T, k \in J \quad (3)$$

$$q_l^w = \sum_{j \in J} v_j^w (q_{k_{l-1} j}^w (1 - m_{kj})) \quad \forall w \in T, k \in J, l = 2, \dots, |T| \quad (4)$$

$$v_j = 0 \quad (5)$$

$$z_j \in \{0,1\} \quad \forall j \in J, l \in T \quad (6)$$

▶ 13

PFFP Experimentation

- ▶ Customer and facility locations uniformly generated on a 50 by 50 grid
- ▶ Initial failure probabilities, p_j , uniformly generated between 0.1 and 0.3
- ▶ Demand, h_{kj} , uniformly generated integer between 0 and 20
- ▶ Fortification factor, $m = 0.25$
- ▶ Stop at 0.5% optimality gap
- ▶ Problem Classes
 - ▶ B100_C50 \equiv budget, $b_j = 100$ and fortification cost, $c_j = 50$ for all facilities and time periods, no remainders
 - ▶ B100_Cunif \equiv budget, $b_j = 100$ and fortification cost, c_j , uniformly generated between 25 and 75 for all facilities and time periods, no remainders
 - ▶ B100_Cunif_R \equiv budget, $b_j = 100$ and fortification cost, c_j , uniformly generated between 25 and 75 for all facilities and time periods, remainders

▶ 14

Computational Time Analysis

► 7 facilities, 15 customers

	B100_C50	B100_Cunif	B100_Cunif_R
Replication 1	19	312	383
Replication 2	43	83	117
Replication 3	20	2733	10800 (0.75%)
Replication 4	19	24	137
Replication 5	40	506	74
Average	28.2	731.6	2302.2
Range	148.7	1288485	22581000

► All times given in seconds

► Replication 3 of B100_Cunif_R stopped at 0.75% optimality gap

► 13

Solution Comparison

► 7 facilities, 15 customers

	B100_C50	B100_Cunif	B100_Cunif_R
Replication 1	6346.03	6385.66	6381.31
Replication 2	6046.37	6061.79	6053.96
Replication 3	4803.64	4957.21	4947.54 (0.75%)
Replication 4	5985.68	5999.06	5999.06
Replication 5	5288.59	5315.72	5300.4

► Including budget remainders decreased objective value by a maximum of 0.2882% while runtime increased by a maximum of 407%

► 14

Planning Horizon Effect

↳ 7 facilities, 15 customers

↳ B100_C50

	T=3	T=6	T=9	T=12
Replication 1	19	147	461	1199
Replication 2	43	238	493	1151
Replication 3	20	148	474	1160
Replication 4	19	150	530	1141
Replication 5	40	199	567	1119
Average	28.2	176.4	505	1154

↳ 17

Planning Horizon Effect

↳ 7 facilities, 20 customers

↳ B100_C50

	T=3	T=6	T=9
Replication 1	88	266	846
Replication 2	36	280	802
Replication 3	37	320	1116
Replication 4	35	300	897
Replication 5	36	348	939
Average	46.4	302.8	938

↳ 18

Future Work

- ▶ Continue instance data collection

- ▶ Extend current model
 - ▶ Network flow
 - ▶ Perishability

- ▶ Consider other disruption sources
 - ▶ Unknown adversarial objective
 - ▶ Dynamic adversarial objective

▶ 19

Unique Contributions

- ▶ Integrated fortification and multi-modal risk mitigation strategies
- ▶ Post-fortification fallibility
- ▶ Unknown and adaptive adversarial objective
- ▶ Perishability concerns



▶ 20 <http://www.berkeley.edu>