GAME THEORY BASED IDENTIFICATION OF FACILITY USE PROHIBITIONS FOR THE MOVEMENT OF HAZARDOUS MATERIALS UNDER TERRORIST THREAT

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

In Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Allison Coffey Reilly

January 2011

GAME THEORY BASED IDENTIFICATION OF FACILITY USE PROHIBITIONS FOR THE MOVEMENT OF HAZARDOUS MATERIALS UNDER TERRORIST THREAT

Allison Coffey Reilly, Ph.D.

Cornell University 2011

The modeling tools that have been developed over the last 25 years for the identification of routes for hazmat shipments emphasize the tradeoffs between cost minimization to the shipper/carrier and controlling the "natural" consequences that would stem from an accident. As the terrorist threat has grown, it has become clear that a new perspective, which allows for the representation of the goals and activities of terrorists, must be incorporated into these routing models. Government agencies can determine which specific facilities to restrict for each class of material and for which times of the day and/or week. This paper develops a mathematical model of a three-player game to represent the interactions among government agencies a shipper and terrorists as a framework for the analysis. It also develops an effective solution procedure for this game and illustrates the use of that procedure on a realistic case study.

BIOGRAPHICAL SKETCH

Allison Coffey Reilly was born August 28, 1983 to Edna Mae and John Reilly in Albany, New York. Raised in Latham, New York, along with sister, Kristen and brother, Brendan, Allison attended Shaker High School. She received her B.S in Civil Engineering from The Johns Hopkins University in 2005, followed by her M.S in Civil and Environmental Engineering from Cornell University in 2008. For her doctorate, Allison worked with Linda Nozick as her thesis advisor in the newly-formed concentration of Civil Infrastructure Systems in the School of Civil and Environmental Engineering at Cornell University. In her free time, Allison enjoys cooking, canoeing, and hikes with her partner, Rob, and dog, Harper.

To Dad, for the pep talks

To Mom, for believing in me

To Kristen and Brendan, for keeping me grounded

To Harper, for the reality checks

To Rob, for holding my hand

ACKNOWLEDGMENTS

The first and most important acknowledgement goes to my thesis advisor, Linda Nozick. It's been a pleasure working with you. Your guidance and support always reminds me of the light at the end of the tunnel.

To my Ph.D. committee (Oliver Gao and Thomas O'Rourke) and other equally important professors (Rachel Davidson, Mary Sansalone, and Ken Hover), thank you for offering your expertise, care, and patience.

I couldn't have gone through this process without Meredith Legg. You are always there for me, and for that I am forever grateful.

I thank my fellow graduate students in the transportation and civil infrastructure systems concentrations - Brian Levine, Anna Li, Natalia Romero, Darrell Sonntag, Timon Stasko, and Yohannes Kesete - for your insights and discussions, and of course, Yashoda Dadkar for helping me to get started on this project.

Thank you to Cornell Engineering Learning Initiatives, its dedicated staff – Linda Tompkins, Alice Rockey, and Lisa Schneider – and to all the TA Trainers with whom I have worked. You have provided me with balance and a safe community to grow and learn.

I also thank Sandia National Laboratories for the data which greatly enriched the case study.

This work was supported by the National Science Foundation Graduate Research Fellowship Program, Sandia National Laboratories, and Cornell Engineering Learning Initiatives. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation, Sandia National Laboratories, or Cornell Engineering Learning Initiatives.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BEA	Bureau of Economic Analysis
DHS	Department of Homeland Security
hazmats	Hazardous materials
TAZs	Transportation Analysis Zones

LIST OF SYMBOLS

α	A scalar variable
A	Shipper's/Carrier's payoff matrix
β	A scalar variable
B	Terrorist's payoff matrix
Γ	A set of non-dominated links
C	Incidence matrix
e	mx1 vector of 1s
K	Number of origin-destination pairs
l	nx1 vector of 1s
m	Number of routing schemes
n	Number of links
$P(z)$	The payoff to the shipper/carrier
p	Probability of an attack
$Q(z)$	The payoff to the terrorist
q	Number of routing options for an individual shipper/carrier
x	Frequency with which the shipper/carrier uses each routing scheme
x^0	A strategy for the shipper/carrier, that along with y^0, defines a Nash equilibrium
y	Frequency with which the terrorist attacks each link
y^0	A strategy for the terrorist, that along with x^0, defines a Nash equilibrium
z	nx1 vector with 0 representing a closed link and 1 representing an open link
ζ	A vector variable
η	A scalar variable

CHAPTER 1

INTRODUCTION

Approximately 800,000 shipments of hazardous materials (hazmat) move daily through the U.S. transportation system (U.S. Department of Transportation, 1998) and approximately one truck in five on the U.S. highways is carrying some form of hazardous material (U.S. Department of Commerce, 1994). In general, the safety record is excellent, but public sensitivity to the risks associated with hazmat shipments is substantial. The public sector plays a direct role in managing the level of risk through the regulation of the transportation network. Government agencies can determine which specific facilities to restrict (or allow) for each class (or classes) of material and for which times of the day and/or week. Further these regulations may take the form of designations (for e.g.: "preferred highway routes" for radioactive materials – U.S. Department of Transportation, 1992) or prohibitions (for e.g.: the State of New York prohibits movements of explosives across the Verrazano Narrows Bridge – U.S. Department of Transportation, 2004).

The development of a model to provide guidance to federal, state and local governments regarding which highway facilities might be restricted (for which materials and under which conditions) is a challenging but important activity. This is particularly important in the context of the U.S. Department of Homeland Security's Advisory System (color-coded "threat levels"). If threat level "Orange" or "Red" is declared, DHS suggests that government agencies consider constraining the transportation system "as appropriate", but there is little specific guidance on how to determine what actions might be "appropriate" (U.S. Department of Homeland

Security, 2004). The goal of the model developed in this research is to lead to a better understanding of how to make such determinations.

This research develops a game–theoretic model of the interactions among a government agency, a shipper/carrier and a terrorist as a framework for the analysis. Each of the relevant actors makes choices over time and has only partial control over the outcome realized as a result of their choices. For example, the government agency can make decisions to restrict the use of some parts of the transportation network, but the results of those choices are dependent on the actions of the shipper/carrier and the terrorist and conversely these decisions also cause consequences for the shipper/carrier and the terrorist. The shipper/carrier selects routes given the rules established by government agency. Beyond honoring government restrictions, the shipper/carrier is concerned about what the terrorist might do and this concern affects the choice of which routes to use. However since the probability of an attack against any single shipment is likely to be very small, the goals of the shipper/carrier are still to move the materials between locations economically while controlling the level of risk, but now the risks include both "natural" risks, including the probability of an accident and the effects should an accident occur and "induced" risks generated by potential terrorist activities. As for the terrorist, we can assume that their interest is in maximizing the damage they can inflict by targeting specific facilities. The choice of the facility is influenced by the routes chosen by the shipper/carrier and the regulations adopted by the government.

Figure 1 portrays the overall interactions among the actors in this game–theoretic framework. The inner box describes the relationship between the terrorist and the shipper/carrier. For this relationship, it is assumed that the regulations which indicate

when (and for which materials) the shipper/carrier is allowed to use each facility are already specified. The analysis that links these two boxes together is normative. That is, given: (1) the shipper's/carrier's perception about the likelihood of an attack; (2) the choices available to the shipper/carrier and the terrorist; (3) the payoff to each, given their decisions and those made by their opponent and (4) the terrorist's perception about what material is in a given shipment, the analysis in this work identifies first, which routes should the shipper/carrier use (and with what frequency) and second, where should the terrorist attack (and with what frequency). The interactions between the shipper/carrier and the terrorist is modeled as a non-cooperative two-person non-zero sum game with the shipper/carrier wishing to maximize the value of the routes used when there is a known probability of an attack and the terrorist wanting to inflict as much damage as possible in an attack.

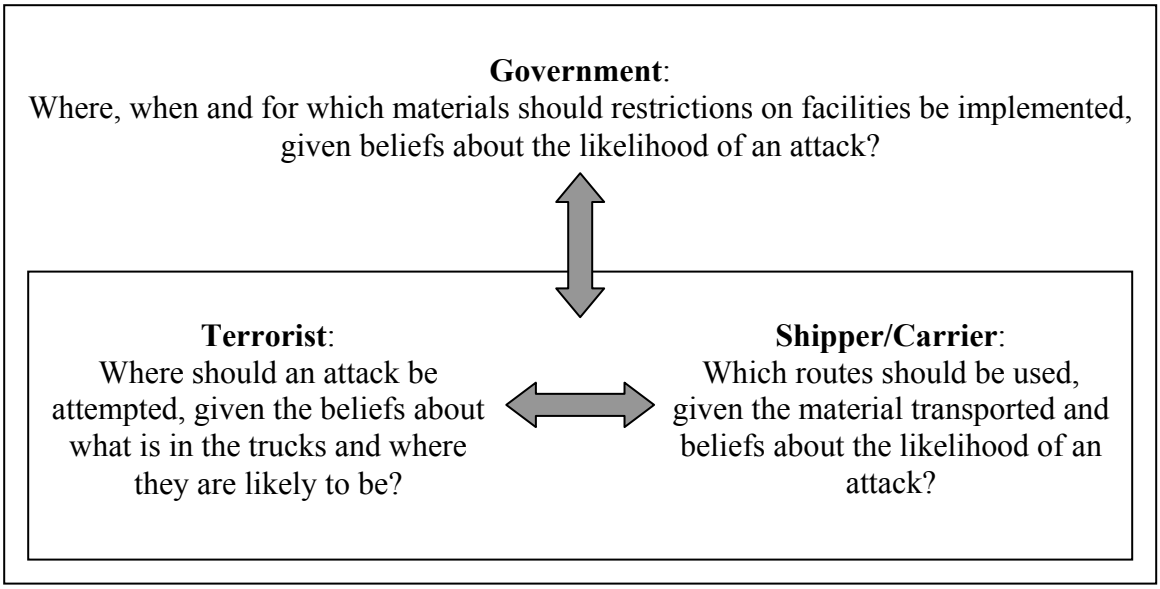

Figure 1. Game-theoretic Problem Structure

The outer box represents the influence of the government on those decisions. The government has the opportunity to control the severity of an attack (should one occur)

through the use of facility prohibitions. These prohibitions can be sufficiently detailed so as to prohibit specific types of hazmat from certain facilities during specific time periods and to have those prohibitions change based on the perceived likelihood of an attack. These prohibitions bound the consequences of an attack and constrain the choices that the shipper/carrier can make. These recommendations are based on the identification of Nash equilibrium strategies in the inner game between the terrorist and the shipper/carrier, given the prohibitions.

This paper makes three key contributions. First, a game is developed among the government, shipper/carrier and a terrorist using a commodity based origin-destination table. Second, we show how that game can be used to (1) determine the regulations that the government should consider adopting; (2) how those regulations should change as the probability of an attack increases; (3) the routes the shipper/carrier should consider along with the probability of use and (4) the facilities the terrorist should target along with the probabilities. Finally these ideas are applied to a realistic case study.

The next section of this work describes the key literature on which this paper is developed. The third section describes the formulation. The forth sections shows how to select route schemes and provides a solution procedure. The fifth section applies the formulation to realistic case study – transport of a hazardous substance on the United States rail network. A tradeoff curve is developed in this section which enables government agencies to assess how link closures affect the risk associated with a terrorist attack and shipper's/carrier's payoff. The last section provides key conclusions and opportunities for future research.

CHAPTER 2

LITERATURE REVIEW

This paper draws on literature in three key areas. The first key area is routing of hazardous materials. While there is extensive literature in this area, we focus on common routing attributes and path finding in stochastic dynamic networks for brevity. The second area is transportation and terrorism. The third area is the game theory literature of direct relevance to this research, including the use of game theory to model terrorist activities and the application of game theory models to the modeling of transportation problems. The remainder of this section describes key research in each area.

Shipper of hazardous materials is commonly concerned with minimizing the economic cost and the risk consequences of a release stemming from an accident when selecting a route or routes. Much of the economic cost to the carrier is proportional to the time taken for the shipment to travel from the origin to the destination. Thus cost minimization can be obtained through minimizing the total travel time. Defining public risk is more complex, but two characteristics – population exposure and accident rate – have gained wide acceptance. The population exposure, depending on the characteristics of the hazardous material to be transported, could be defined as the people in other vehicles that are within some distance of the shipment as it moves from its origin to its destination or it could be expanded to include the population residing within some distance of the shipment during its journey. The accident probability for a route is the probability of an accident happening along the route. Population exposure and accident rate can be combined into a single consequence measure for a route by summing across all links in the route the product of accident

rate and exposure. Erkut and Verter (1998), Erkut and Ingolfsson (2000) and Chang et al. (2005), among others, use the same measure in their hazmat routing studies.

Neither the travel time nor the consequence measure is deterministic since they both depend on the traffic volumes and activity patterns. Further they vary with the time of the day since characteristics like visibility, traffic volumes and activity patterns vary throughout the day. Using the expected values of the attributes ignores the variation resulting from these two causes and could lead to selection of routes that have acceptable expected values but perform ‘‘poorly” based on when they are actually used (Nozick et al., 1997). Hence, we represent the uncertainty for each attribute by a probability distribution which varies by the time-of-day.

Dadkar et al. (2008) and Nielsen et al. (2005) developed K shortest path algorithms for stochastic and dynamic networks. Dadkar et al. (2008) focused on problem instances where the distribution of each link attribute is continuous whereas Nielsen et al. (2005) focused on problem instances where the distribution of the link attributes is discrete with integer values. In the routing of hazardous materials, the objectives of interest produce continuous distributions for link performance. Hence Dadkar et al. (2008) is more relevant to this application. Also, Nielsen et al. (2005) focused on identifying the exact solution to the K shortest paths problem which leads to computational challenges in large networks whereas Dadkar et al. (2008) developed an algorithm that is computationally feasible for large networks. Hence for the purposes of this analysis we use the algorithm in Dadkar et al. (2008).

There is substantial interest in research related to transportation and terrorism. To date much of that research has focused on identifying what parts of the transportation

system are vulnerable to terrorism and initial ideas of what should be done about those vulnerabilities. For example, see Szyliowicz and Viotti (1997), Chatterjee et al. (2001), Frederickson and LaPorte (2002), and Haimes and Longstaff (2002).

Many game theory models have been developed to address a wide variety of problems. For a discussion of other game theory models see Fundenberg and Tirole (1995) or Kreps (1992). The seminal paper by Nash (1951) established the existence of equilibria for finite non-cooperative games but did not develop an algorithm for finding them. Among others, Mangasarian and Stone (1964) designed an algorithm for computing all the equilibria for finite, two-person, non-cooperative, non-zero sum games (also known as bimatrix games). They modeled a bimatrix game as a single integrated mathematical programming formulation and proved that each solution to this formulation is a Nash equilibrium point of that game.

There have been several studies that have used game theory to model terrorism. Sandler and Arce (2003) and Sandler and Enders (2003) provide excellent literature reviews. These studies focus on a variety of issues including the effectiveness of the no-negotiation strategy (Lapan and Sandler, 1988 and Selten, 1988), the accommodations which can be reached between a terrorist and a host government (Lee, 1988) and the strategic interdependence between nations as they attempt to combat terrorism (Sandler, 2003).

Most of the more involved games described by Hollander and Prashker (2006) follow the Stackelberg leadership model (von Stackelberg, 1934). Stackelberg games are played between two players – one of whom is a leader and the other is a follower. The leader makes a decision and the follower sees the outcome of the leader's move and

makes her move. Transportation situations adapt well to Stackelberg games since the government/transportation authorities can be considered the leader because they provide the infrastructure and dictate the rules under which it may be used. Travelers then make use of this infrastructure given the rules in place for its use. Stackelberg games are often expressed as bilevel optimizations for formulation and solution.

Bell (2000), Bell and Cassir (2002), and Bell (2004) used a two-person zero-sum non-cooperative game to measure the performance reliability of transport networks in case of single user, multiple users and freight vehicle routing problems, respectively. Bell (2003) sought to identify the most crucial links or nodes with an aim to defining the network's vulnerability. In each game, the user(s) seeks a least-cost path with a virtual network tester or an ''evil demon" trying to maximize trip cost. To calculate the equilibria of these games, they are solved as maximin problems with the Method of Successive Averages (MSA).

Biaonco et al. (2009) presented a bilevel formulation focused on risk equity. Both levels corresponded to government agencies – the meta-local authority that aims to minimize the maximum link risk in the whole network and the regional area authority that aims to minimize the total risk over their network. While the focus on equity is significantly different than our focus, the core concepts explored in the modeling are related.

Kara and Verter (2004) proposed a bilevel formulation where the government imposes restrictions on the network and the shipper/carrier then choose the routes. Erkut and Gzara (2008) extended this research. They proposed incorporating the transport costs in the government objective along with risk considerations, so that the government can

represent a trade off between cost and risk. A key difference in the core problem examined in these papers and the one considered in the presented research is the character of the policy adopted by the government and the shipper/carrier. In case of Kara and Verter (2004) and Erkut and Gzara (2008), the policies adopted by both the government and the shipper/carrier should be static. The only uncertainty represented in these papers is that associated with natural risks (which are independent of the actions of either player). Our analysis focuses on situations for which there is a third player in the form of a malicious terrorist attacker and therefore an analysis that admits randomized policies is likely to be more beneficial to the shipper/carrier. This, in turn, will force a randomized policy to be more advantageous to the terrorist. Since the policy must be implementable it is likely important that the prohibitions enacted by the government be static (or vary only with threat level).

Szeto and Sumalee (2008) propose similar goals to the ones of this paper – use a game theoretic model to identify routing and scheduling decisions for multiple hazmat shippers/carriers interested in moving material between specific locations. However, the proposed formulation is a zero-sum game which is not computational feasible for large networks. Additionally, the role of a government entity, controlling terrorist gains, is absent.

Dadkar et al. (2009) develop a non-zero sum game-theoretic model of the interactions among government agencies, a single repetitive hazmat shipment for a single origin to a single destination, and terrorists. A heuristic is used to find optimal sets of government imposed facility restrictions that produce a Nash equilibria where the shipper's/carrier's expected payoff is as high as possible given that the terrorist's expected payoff is below a prescribed threshold. This work assumes only one hazmat

shipment made repetitively from a single origin to a single destination. However, it does provide an excellent point of departure for this analysis. This analysis focuses on how to identify these facility restrictions when there is a full origin-destination table for the commodity of interest.

CHAPTER 3
MODEL FORMULATION

The objectives of this model are twofold. The first is to identify the strategies of the shipper/carrier and the terrorist given government imposed prohibitions. We assume that the shipper/carrier and the terrorist would pursue Nash equilibrium strategies for the non-cooperative two-person non-zero sum game. The second is for the government to identify link prohibitions that maximize the shipper's/carrier's payoff while limiting the terrorist's payoff. We formulate this optimization problem as a Stackelberg game in which the government is the leader and the shipper/carrier and the terrorist are the followers.

We consider a shipper/carrier who repetitively wants to deliver an extremely hazardous substance between multiple origin–destination pairs. There are multiple routes that connect each origin–destination pair. We define a routing scheme to be a unique strategy which identifies the route to deliver the substance for each origin–destination pair. Let us assume that there are m routing schemes. A terrorist can choose from n links to attack. These n links are all the links that appear on at least one route that the shipper/carrier considers. A procedure for developing the routing schemes is given in the next subsection.

We assume that the government, the shipper/carrier and the terrorist have common knowledge on the network structure, the payoffs for both the shipper/carrier and the terrorist. We assume that in case of an attack, only one link is targeted each time an attack is mounted and every attack is successful. We also assume that the probability of an attack (p) is known. The probability p can be interpreted as indirectly

reflecting a rate at which attacks are mounted or as a subjective estimate of likelihood at a given time. The estimation of p is likely to be based on intelligence information. Therefore, it will be important to perform an analysis to understand the sensitivity of the recommendations to changes in the estimate for p. This type of analysis is illustrated in Section 5.

Let A and B be the $m \times n$ payoff matrices for the shipper/carrier and the terrorist, respectively. The payoffs to both the players depend on whether the route chosen by the shipper/carrier traverses the link targeted by the terrorist. The payoff matrix for the shipper/carrier, A, can be formulated using probability of attack (p), the utility of each route to the shipper/carrier as well as the consequences of a successful attack to the shipper/carrier. The utility of a routing scheme is simply the sum of the utilities of the routes selected for each shipment. The matrix entry $A(i, j)$ is the payoff to the shipper/carrier when he uses routing scheme i and link j is targeted to attack. If link j is not on routing scheme i, $A(i, j)$ is assumed to be the utility of that routing scheme. However, if route i traverses link j, $A(i, j)$ is assumed to be the expected value of the utility of routing scheme i in case of no attack and the representative value of damage caused by a successful attack (in this case, the population exposure on the link j when the route i traverses it).

The payoff matrix for the terrorist, B, can be formulated using probability of attack (p) and the utility of a successful attack to the terrorist. The matrix entry $B(i, j)$ is the payoff to the terrorist when he targets link j and routing scheme i is used. $B(i, j)$ is assumed to be p times the population exposure on link j if the shipper/carrier uses routing scheme i that contains that link and 0 otherwise.

The government can influence the decisions of the shipper/carrier by prohibiting the use of certain facilities during certain time periods. Thus, the shipper/carrier may not use routes which would violate those prohibitions. Also, terrorists will know of these prohibitions and therefore they will not stage attacks on facilities when these prohibitions are in effect. The objective of the government is to establish rules for the use of certain facilities that maximize the shipper's/carrier's payoff while limiting the terrorist's payoff. In the next subsection we present the mathematical programs for the bi-level optimization problem.

3.1 Shipper/Carrier and Terrorist Optimization Problem

We assume that both the shipper/carrier and the terrorist would pursue Nash equilibrium strategies for the game after observing the government's regulation. We first model the government's decision. Let $z = \left(z_j \right)$ be a $n \times 1$ binary decision vector to indicate the prohibitions enacted by the government. If $z_j = 0$, then link j is prohibited from use and $z_j = 1$ otherwise.

We then formulate the shipper's/carrier's and the terrorist's optimization problem. Let c_{ij} be 1 if link j is included in the routing scheme i used by the shipper/carrier and 0 otherwise and let $C = \left(c_{ij} \right)$. We next define the decision variables for the shipper/carrier and the terrorist. Let x be a $m \times 1$ decision vector to indicate the frequency with which the shipper/carrier uses each of the m routing schemes. Let y be a $n \times 1$ decision vector to indicate the frequency with which each of the n links are targeted by the terrorist. The shipper/carrier's optimization problem is to choose the shipping frequency vector x that maximizes his expected payoff

$$x'Ay \tag{1}$$

$$\text{subject to } e'x = 1, \tag{2}$$

$$C'x \le z, \tag{3}$$

$$x \ge 0, \tag{4}$$

and the terrorist's optimization problem is to choose the attack frequency vector y that maximizes his expected payoff

$$x'By \tag{5}$$

$$\text{subject to } l'y = 1, \tag{6}$$

$$y \le z, \tag{7}$$

$$y \ge 0, \tag{8}$$

where e and l are $m \times 1$ and $n \times 1$ vectors of 1s, respectively.

Recall that a Nash equilibrium point is defined by the pair of strategies $\left(x^0, y^0\right)$ that solves both the mathematical programs simultaneously (Nash, 1951). Note that the game defined by these two mathematical programs may not have a pair of Nash equilibrium strategies for some government decision z. For example, $z = \vec{0}$, the feasible decision set of the game is empty. To simplify our notation, we assume that both the carrier/shipper's and terrorist's objective values are negative infinity if the game is infeasible. Thus, we can focus on the case in which there exists a Nash equilibrium solution.

Since a Nash equilibrium solution is defined by two separate mathematical programs, it is useful to convert the two mathematical programs into a single mathematical

program. To this end, we need to define additional variables. Let α and β be scalar variables and let ζ and η be the $n \times 1$ vector variables. Consider the following quadratic program that chooses $(x, y, \alpha, \beta, \zeta, \eta)$ to maximize the quadratic function

$$x'(A+B)y - \alpha - \beta - (\zeta' + \eta')z \tag{9}$$

$$\text{subject to } Ay \le \alpha e + C\zeta, \tag{10}$$

$$B'x \le \beta l + \eta, \tag{11}$$

$$e'x = 1, \tag{12}$$

$$l'y = 1, \tag{13}$$

$$z \ge C'x, \tag{14}$$

$$z \ge y, \tag{15}$$

$$x \ge 0, \tag{16}$$

$$y \ge 0, \tag{17}$$

$$\zeta \ge 0, \tag{18}$$

$$\eta \ge 0. \tag{19}$$

The following proposition shows that the Nash equilibrium strategies for the two-person game can be characterized by the solutions of the quadratic program.

Proposition 1. Suppose that the game defined by mathematical programs (1) – (8) is feasible. Then a pair of strategies (x^0, y^0) is a pair of Nash equilibrium strategies for the game defined by mathematical programs (1) – (8) if and only if there exist $(\alpha^0, \beta^0, \zeta^0, \eta^0)$ such that $(x^0, y^0, \alpha^0, \beta^0, \zeta^0, \eta^0)$ solves the quadratic program (9) – (19) and the maximum objective value is 0.

Proof. We first claim that (x^0, y^0) solve mathematical program (1) – (4) and mathematical program (5) – (8) simultaneously if and only if there exist two scalars

α^0 and β^0 and two $n \times 1$ vectors ζ^0 and η^0 such that $\left(x^0, y^0, \alpha^0, \beta^0, \zeta^0, \eta^0\right)$ satisfies constraints (10) – (19) and

$$\left(x^0\right)' C\zeta^0 - \left(\zeta^0\right)' z = 0, \tag{20}$$

$$\left(x^0\right)' Ay^0 - \alpha^0 - \left(\zeta^0\right)' z = 0, \tag{21}$$

$$\left(y^0\right)' \eta^0 - \left(\eta^0\right)' z = 0, \tag{22}$$

$$\left(x^0\right)' By^0 - \beta^0 - \left(y^0\right)' \eta^0 = 0. \tag{23}$$

To see this, note that for the given $y = y^0$, mathematical program (1) – (4) is a linear program. Since this linear program is feasible by assumption and the feasible set is bounded, then the corresponding dual program has a finite optimal solution. Let $\left(\alpha^0, \zeta^0\right)$ be a finite optimal dual solution for the linear program, where α^0 is the dual value that corresponds to constraint (2) and ζ^0 is the $n \times 1$ vector of the dual values that correspond to constraint (3). Then x^0 is an optimal solution for linear program (1) – (4) for the given $y = y^0$ and $\left(\alpha^0, \zeta^0\right)$ is an optimal dual solution if an only if

$$\left(\left(x^0\right)' C - z'\right)\zeta^0 = 0,$$
$$\left(x^0\right)'\left(Ay^0 - \alpha^0 e - C\zeta^0\right) = 0,$$

and constraints (10), (12), (14), (16) and (18) hold. This is because constraints (10), (12), (14), (16) and (18) are the feasibility constraints for both the primal and the dual programs and the other two equations follow from the complementary slackness theorem for linear programming. These two equations and constraint (12) ensure that constraints (20) and (21) hold.

Consider the linear program (5) – (8) for the given $x = x^0$ and its corresponding dual program. Let $\left(\beta^0, \eta^0\right)$ be a finite optimal dual solution. It follows from the previous

argument that y^0 is an optimal solution for linear program (5) – (8) for the given x^0 and $\left(\beta^0, \eta^0\right)$ is a finite optimal dual solution if an only if

$$\left(\left(y^0\right)' - z'\right)\eta^0 = 0,$$
$$\left(y^0\right)'\left(B'x^0 - \beta^0 l - \eta^0\right) = 0,$$

and constraints (11), (13), (15), (17) and (19) hold. These two equations and constraint (13) ensure that constraints (22) and (23) hold. This proves the claim.

Now we can use the claim to prove the proposition. Suppose that $\left(x^0, y^0\right)$ is a pair of Nash equilibrium strategies. Then it follows from the claim that there exist two scalars α^0 and β^0 and two $n \times 1$ vectors ζ^0 and η^0 such that $\left(x^0, y^0, \alpha^0, \beta^0, \zeta^0, \eta^0\right)$ is a feasible solution of the quadratic program (9) – (19). Also note that

$$\left(x^0\right)'(A+B)y^0 - \alpha^0 - \beta^0 - \left(\left(\zeta^0\right)' + \left(\eta^0\right)'\right)z$$
$$= \left(x^0\right)'Ay^0 - \alpha^0 - \left(\zeta^0\right)'z + \left(x^0\right)'By^0 - \beta^0 - \left(\eta^0\right)'z = 0,$$

where the second equation follows from constraints (21) and (23). Also note that for each feasible solution $\left(x, y, \alpha, \beta, \zeta, \eta\right)$ for the quadratic program (9) – (19),

$$x'Ay \le \alpha x'e + x'C\zeta \le \alpha + z'\zeta \text{ and } x'By \le \beta l'y + \eta'y \le \beta + \eta'z.$$

Then

$$x'(A+B)y - \alpha - \beta - \left(\zeta' + \eta'\right)z \le 0.$$

This implies that $\left(x^0, y^0, \alpha^0, \beta^0, \zeta^0, \eta^0\right)$ solves the quadratic program.

Conversely, if $\left(x^0, y^0, \alpha^0, \beta^0, \zeta^0, \eta^0\right)$ solves the quadratic program, then the previous argument implies that

$$\left(x^0\right)'(A+B)y^0 - \alpha^0 - \beta^0 - \left(\left(\zeta^0\right)' + \left(\eta^0\right)'\right)z \le 0 .$$

We assume that there exists a pair of Nash equilibrium strategies. It follows from the claim that there exist a feasible solution of the quadratic program (9) – (19) $\left(x, y, \alpha, \beta, \zeta, \eta\right)$ such that

$$x'(A+B)y - \alpha - \beta - \left(\zeta' + \eta'\right)z = 0 .$$

Then

$$\left(x^0\right)'(A+B)y^0 - \alpha^0 - \beta^0 - \left(\left(\zeta^0\right)' + \left(\eta^0\right)'\right)z = 0 .$$

Constraints (10) – (19) and the above equation imply that

$$\left(x^0\right)' Ay^0 = \alpha\left(x^0\right)'e + \left(x^0\right)'C\zeta = \alpha + z'\zeta ,$$
$$\left(x^0\right)' By^0 = \beta l' y^0 + \eta' y^0 = \beta + \eta' z .$$

This implies that constraints (20) – (23) hold and this proves the proposition. Q.E.D.

It is useful to know that if $z_j = 1$ for all j, the quadratic program would reduce to the quadratic program by Magnasain and Stone (1964). To see this, recall that Magnasain and Stone (1964) show that there exist $\left(x, y, \alpha, \beta\right)$ such that constrains (12), (13), (15), and (16) hold and also $Ay \le \alpha e$, $B'x \le \beta l$, and $x'(A+B)y - \alpha - \beta = 0$. Let $\zeta = \vec{0}_{m\times 1}$ and $\eta = \vec{0}_{n\times 1}$. Note that $\left(x, y, \alpha, \beta, \zeta, \eta\right)$ is an optimal solution. Therefore, the

quadratic program (9) – (19) is an extension of the quadratic program established by Magnasain and Stone (1964).

Note that the quadratic program (9) – (19) may not have a unique solution. Then we need secondary criteria to choose a Nash equilibrium strategy. It is reasonable to assume that the shipper/carrier would play the Nash equilibrium strategy that maximizes his payoff. Also note that a Nash equilibrium solution depends on the government's decision z. Let $\Lambda(z)$ be the set of $(\alpha,\beta,\zeta,\eta)$ such that there exist (x,y) for which $(x,y,\alpha,\beta,\zeta,\eta)$ is a solution to the quadratic program for the given z. Based on the previous proof, we conclude that the payoffs to the shipper/carrier and the terrorist at the solutions are respectively $\alpha+\zeta'z$ and $\beta+\eta'z$ for all $(\alpha,\beta,\zeta,\eta)\in\Lambda(z)$. Let $\alpha(z)+(\zeta(z))'z$ be the maximum payoff to the shipper/carrier over $\Lambda(z)$ for the given z and $\beta(z)+(\eta(z))'z$ be the corresponding payoff to the terrorist.

3.2 Government Optimization Problem

Recall that the objective of the government is to maximize the shipper/carrier's payoff while limiting the terrorist's payoff. To model this problem, let γ be the government's tolerance of the terrorist's payoff. Then the government chooses the prohibition vector z that maximizes

$$\alpha(z)+(\zeta(z))'z \tag{24}$$

$$\text{such that } \beta(z)+(\eta(z))'z\le\gamma, \tag{25}$$

$$z_j\in\{0,1\} \text{ for } j=1,\ldots,n. \tag{26}$$

The objective function (24) is to maximize the expected payoff of the shipper/carrier. Constraint (25) limits the payoff of the terrorist and constraints (26) impose binary constraints on the decision variables.

Observe that the maximization problem (24) – (26) may not feasible. We assume that the objective value of the maximization program is negative infinity in this case.

CHAPTER4

SOLUTION PROCEDURE

Since transportation networks are typically large, there can be (1) many possible routes for each shipment, leading to an exorbitant number of routing schemes, and (2) there are many distinct sets of link prohibitions which need to be considered. Therefore, quadratic maximization problem (9) – (19) for each set of link prohibitions will be large making the identification of its solution challenging. Also, as the number of sets of link prohibitions increases, the number of the non-concave quadratic maximization problems which must be solved increases. Thus, it becomes important to control the number of routing schemes and the number of link prohibitions examined. To this end, we first show how to identify "good" route choices for each shipment and how to assemble them into a routing scheme. We then describe a heuristic which identifies reasonable sets of links to prohibit in order to identify the trade-off frontier for p.

4.1. Formulation of Routing Schemes

Recall that a routing scheme identifies for each origin-destination pair the route to use. Note that the optimal strategies for the shipper/carrier and the terrorist are pareto-efficient and therefore, only those routing schemes need to be explicitly identified. This greatly reduces the number of routing schemes which must be generated. Recall that a routing scheme is non-dominated for the shipper/carrier if there are no other routing schemes that have an equal or better expected payoff for each link that might be attacked with at least one link being strictly better.

We estimate the non-dominated routing schemes using the following four steps. In the first three steps routing schemes, based on the shipper/carrier' strategies, which are likely to be pareto-efficient are identified. In the fourth step, based on dominance applied to the shipper and terrorist's strategies, the non-dominated set of routing schemes from those routing schemes identified in Steps 1 through 3 is identified.

The first step is based on the observation that the routing scheme that gives the best expected payoff for the shipper/carrier when a specific link is attacked often creates useful strategies for consideration. Hence, Step 1 identifies routing schemes by choosing the route for each shipment which maximizes the expected payoff for the shipper/carrier for each link attacked. Based on these routing schemes, we can then estimate a set of the non-dominated links.

Step 2 identifies routing schemes focused on the estimated set of non-dominated strategies for the terrorist. This is done as follows. For each shipment, identify the route that maximizes the minimum return they would receive if the terrorist attacks one of the estimated non-dominated links. That decision is then augmented with an assumption that the remaining shipments use the route with the highest utility yielding a complete routing scheme. Note that this process will generate at most, the same number of routing schemes as there are unique origin-destination pairs. If the routing schemes identified leads to additional strategies for the terrorist that are non-dominated this step must be repeated with the set of non-dominated strategies for the terrorist expanded.

In Step 3 we explore changes to the routing schemes identified in the first two steps with the goal of identifying strategies that are better. This is done as follows. For each

routing scheme and origin-destination pair, see if by using a different route for that origin-destination pair, an improvement can be identified, where an improvement is defined as an increase in the expected payoff to the shipper/carrier for an estimated non-dominated strategy for the terrorist. The key element of this step is that for each routing scheme and origin-destination pair we consider each link in the estimated non-dominated set to search for improvements in the routing scheme. Note that this is an iterative process. Each time a new routing scheme is identified, this type of change is explored. If the routing schemes identified leads to additional strategies for the terrorist that are non-dominated, Step 2 and Step 3 must be repeated with the additional set of non-dominated strategies for the terrorist expanded.

In Step 4 we apply the dominance criteria iteratively to the shipper's/carrier's and the terrorist's payoff matrices until no strategies can be removed.

4.2. Solution Strategies

Based on the expected payoff matrices for both the shipper/carrier and the terrorist generated in the previous section, the following heuristic can be used to estimate the trade-off frontier between the expected payoffs for the shipper/carrier and the terrorist.

1. Let Γ be the set of non-dominated links identified in Step 4 (in the algorithm used to generate routing schemes assuming no link restrictions).
2. Enumerate all combinations links in Γ to obtain 2^{Γ} possible subsets of Γ. Initialize our estimate of the efficient frontier for the payoff to the shipper and the terrorist to null.
3. For each subset of Γ, determined the shipper's/carrier's set of non-dominated routing schemes and solve the quadratic program (9) – (19). For each nonlinear optimization record the payoff to the shipper and the terrorist and the links

restricted. Update our estimate of the efficient frontier between the payoffs to the shipper and the terrorist. Note whether new point(s) have been added to the frontier. If no new points have been added, stop.

4. If the terrorist attacks any links not in the set Γ, add that link to Γ and go to Step 2.

It is important to remember that we generate the routing schemes assuming which links are available for use. As that set is restricted, some links which were previously dominated are no longer dominated (because some of those that dominated have been prohibited from use). Also, at a minimum, this algorithm will iterate through Step 2 twice because restricting all links identified in Step 1 will force the identification of more strategies for the terrorist. In the case study, the inclusion of these new strategies did not generate more points for our estimate of the efficient frontier.

CHAPTER 5

CASE STUDY

To illustrate the use of the formulation and solution procedure on a realistic problem, we consider the transportation of a single hazardous material over the US rail network between 55 unique origin-destination pairs. The origins and destinations for those hazardous material shipments are represented by a set of 84 Transportation Analysis Zones (TAZs), which are aggregations of BEA areas. The TAZs and US rail network are shown in Figure 2. For simplicity, we assume that all shipments depart from their origins at 12 AM. In practice, pure strategies for multiple departure times can easily be integrated into the payoff matrices. The key question investigated in this case study is the estimation of the tradeoff frontier between controlling the consequences of an attack and the economic effects on the Shipper/Carrier for specific values of the probability of an attack, p.

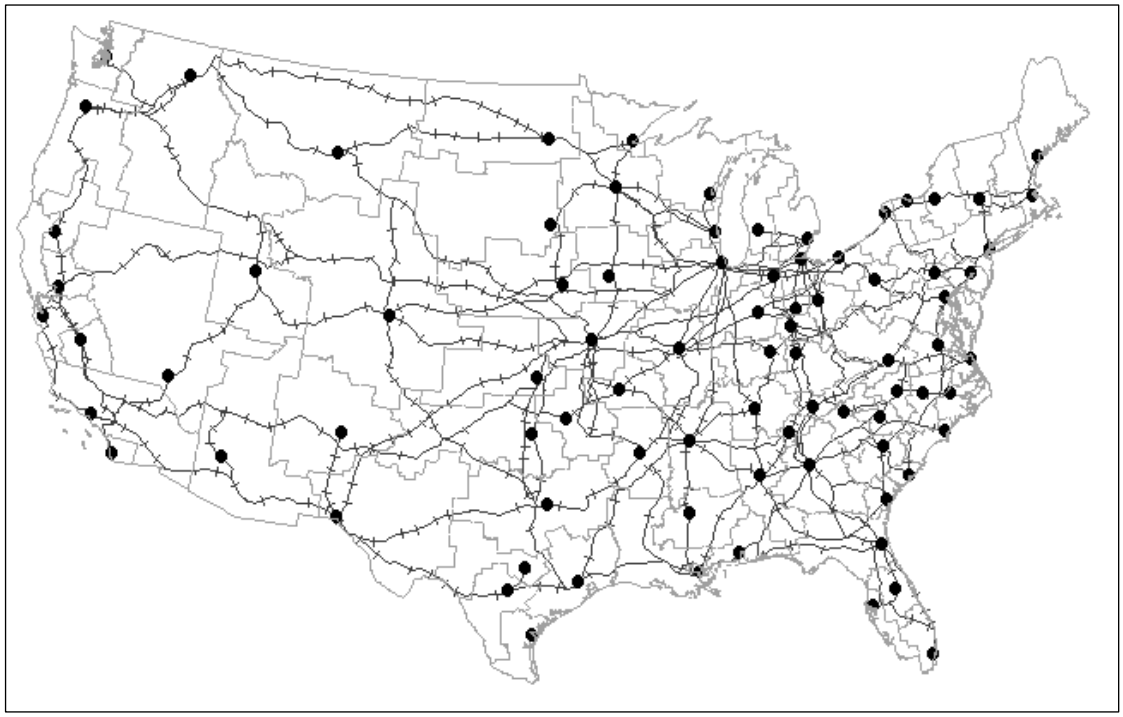

Figure 2. The case study network with TAZs shown

First, we need to identify the pure strategies available to the Shipper/Carrier, the Terrorist, and the Government, as well as the payoff matrices for both the Shipper/Carrier and the Terrorist that reflect their key motivations and assumed behaviors. The Shipper/Carrier chooses one route for each shipment (repetitive movements from the same origin to the same destination) to create a routing scheme and these routing schemes are thus the pure strategies available to the Shipper/Carrier. We use the *K* shortest path algorithm developed for stochastic dynamic networks by Dadkar *et al.* (2008a) to generate 200 paths for each specific shipment. This is done for all 55 shipments. Therefore, we assume that all paths of any interest to the Shipper/Carrier will be included in the "best" 200. We make the following assumptions for the purpose of this analysis.

For the purposes of this analysis the following is assumed:

1. Link travel time is modeled as a sum of free–flow time plus an exponentially distributed random delay with a mean of 10% of the free flow travel time. Even though the random delay on a link is modeled as a constant plus an exponential random delay we assume that the travel time across a path is approximately normal based on the Central Limit Theorem and as also assumed in Chang *et al*. (2005).
2. Accident probability varies according to a gamma distribution based on the work of Nembhard (1994) where the scale parameter is based on whether the link is urban or rural.
3. The major hazards are fire or vapor exposure, or both, in the event of an accident or an attack. The at–risk population is the community located within 2-miles of the link (U.S. Census 2000). Our focus is the US rail network, hence the on-link population is considered negligible.

For this analysis, it is important that there is one measure which summarizes the value of using each route in comparison to others for each shipment; hence we define a composite measure for each route as the equally weighted sum of travel time and consequence measure (a combination of population exposure and accident probability) across all links. An increase in this composite measure signifies that the Shipper/Carrier is worse off. Thus the negative value of the mean of this composite measure is taken as the utility of a route for a given shipment and the Shipper/Carrier will choose the routes with the lowest composite measure mean for higher utility. Note that the Shipper/Carrier achieves this utility only in case of no attack. To reflect each shipment's usage of the network, the utility of a route for a particular shipment is then scaled proportional to the carloads shipped per year.

This case study network has 282 bidirectional links. However, only 259 of which are on the 200 shortest paths for the 55 shipments on which we focus. Thus only 259 links are of interest to the Government. These are the pure strategies available to the Government since the Government will want to restrict the movement of hazmat on only these links. The Government has the option of closing none, some, or all links. Similarly these 259 links are also the pure strategies available to the Terrorist since the Terrorist will want to attack only those links that are utilized by the Shipper/Carrier. The expected payoffs matrices are developed as described in Section 3.0.

The algorithm was run with an assumed p = 0.001% and 0.01%. The MATLAB Optimization Toolbox was used to solve the non-linear program and all experiments were run on a Xeon X5450 3.0 GHz PC. The remainder of this section is divided into three subsections. The first subsection demonstrates the four-step process of formulating routing schemes using the case study network. Subsection 2 develops link prohibitions based on a simple measure. The performance of these prohibitions serves as a point of comparison with method given in Section 4.2 and illustrated in Subsections 3 and 4. Subsections 3 and 4 focus on interpreting the efficient frontiers found for the two different assumed probabilities of attack (0.001% and 0.01%) in order to understand how the strategies change for the Shipper/Carrier, the Terrorist, and the Government.

5.1 Routing Schemes

When link prohibitions are imposed by the Government, some or all of each shipment's 200 routes may become infeasible. If all become infeasible we generate additional routes, if they exist. In this case study, if this occurs; there are no additional routes to add to the analysis. For each unique combination of link prohibitions, we

identify only feasible pure strategies for the Shipper/Carrier and the Terrorist. For the Shipper/Carrier, we enumerate likely routing schemes, and for the Terrorist, we identify all the links that are used by at least one of the enumerated routing schemes. One route is contributed for each shipment to create a routing scheme and we focus on developing routing schemes likely to be pareto-efficient as described in Section 4.1.

We evaluate the value of a routing scheme by the total path utility in the case of an attack. The 200 routes enumerated for each of the 55 shipments are assigned a path utility which reflects a successful trip, as discussed in Section 5.0. However, with some probability, $p \geq 0$, the trip is unsuccessful due to an attack on a specific link, and the Shipper/Carrier experiences losses to their path utility. We define an individual shipment's path utility be the expected utility received from successfully completing a trip on this path minus the expected losses from a successful terrorist attack on a specific link. We aggregate these utilities to create the total path utility of the routing scheme based on the link attacked. Note that this is the logic behind the entries of the Shipper's/Carrier's payoff matrix, A, as described in Section 3.0.

The goal of the first step for creating routing schemes is to maximize the Shipper's/Carrier's total path utility in the case of an attack on a specific link and this is done for each link in the network. We sequentially choose one link and assume it is this link that the Terrorist targets. Then, for each shipment, we select the route that maximizes the path utility in the case of an attack on this link. Loss of utility stems from either or both of the following two possibilities: (1) the shipment travels along a route different from its highest utility route in the case of no attack, and (2) the Terrorist targets a link on the path along which the shipment travels. Therefore, the Shipper/Carrier may find benefit using a route lower in utility in the case of no attack

for a particular shipment when it is known that the Terrorist will target a link not on this route. We then aggregate the chosen routes for each shipment into a routing scheme. This routing scheme is always non-dominated since there is no other routing scheme that has an equal or better total path utility in the case of an attack on the specific link and is a pareto-efficient row in the Shipper's/Carrier's payoff matrix, *A*.

To illustrate this concept, let us assume that Link S in Figure 3 will exclusively be targeted by the Terrorist. For the sake of this discussion, we are only interested in Shipment σ, which is departing Oakland, CA (for Houston, TX). We show Shipment σ's best and second best utility routes in the case of no attack in Figure 3. Note that these primary and secondary routes share the link traveling through Modesto. Shipment σ traverses Link S when traveling its primary route, but does not when traveling its secondary route. Table 1 shows the utility from using Shipment σ's primary and secondary routes in the case of no attack, the expected losses from an attack on Link S, and path utility from an attack on Link S, for $p = 0.001\%$. As Table 1 shows, even when the attack likelihood is relatively low ($p = 0.001\%$), there is benefit from having Shipment σ use its secondary route, since this path's utility in the case of an attack on Link S, -108.40, is greater than the primary route's utility in the case of an attack on Link S, -108.81. This directly implies that the losses in utility from using a worse utility route (the second route) in case of no attack are less than the losses to utility from a terrorist attack on Link S when the shipment is present. For the sake of this argument, no other shipments' primary routes in the case of no attack traverse Link S. Therefore, the Shipper/Carrier would decide that all remaining shipments use their best utility route in the case of no attack.

Table 1. Shipment σ's route utility in the case of an attack on Link S and p = 0.001%

Route preference in the case of no attack	Route utility in the case of no attack	Exposure on Link S	Expected losses from terrorism on Link S when $p = 0.001\%$	Route utility in the case of an attack on Link S and $p = 0.001\%$
First	-108.14	67,000	0.67	-108.81
Second	-108.40	0	0.00	-108.40

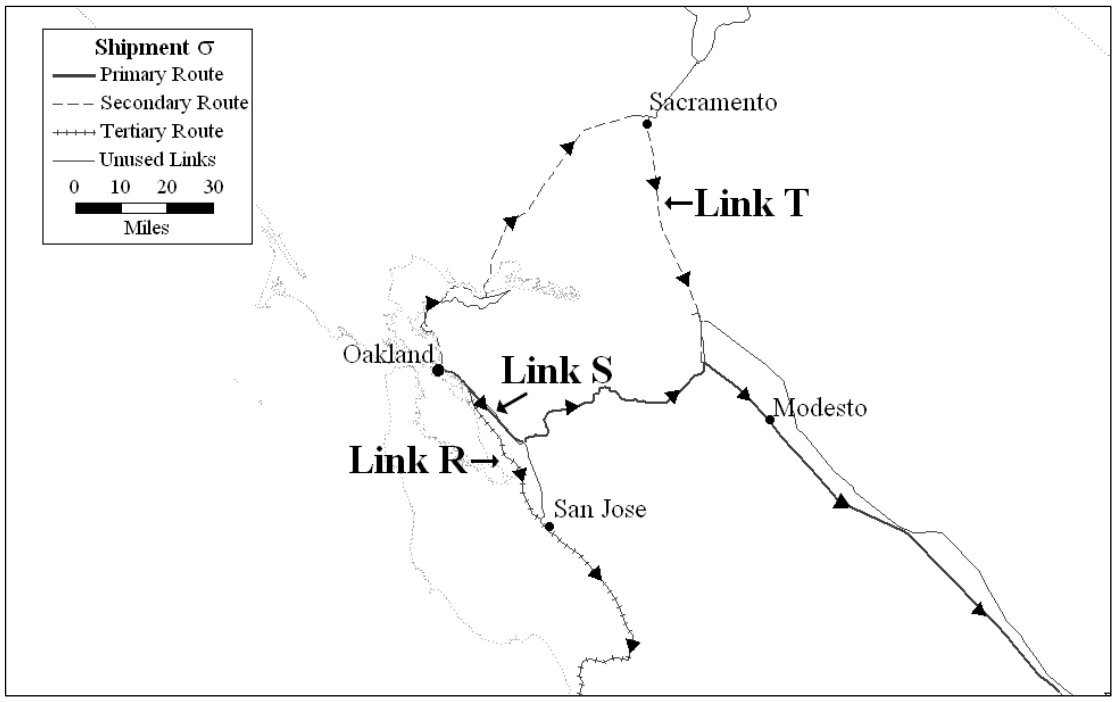

Figure 3. Shipment σ's strategies

We identify the current non-dominated links before proceeding to Step 2. Remember that in Step 1 we have identified a routing scheme for each link that might be attacked. That gives us 259 routing schemes. However, based the Shipper's/Carrier's defined strategies at this point, not all of the links will be of interest to the Terrorist. If we look at the return to the Terrorist for attacks on each link given the 259 routing schemes, some links might lead to returns that are always no better than other link. These links are dominated and can be removed from consideration.

In Step 1 of the routing scheme formulation, we used a link-based approach to maximize the Shipper's/Carrier's total path utility from an attack on a particular link. In Step 2, we focus on the individual shipments and choose for each shipment which route maximizes the shipment's path utility in the case of an attack. Since the Terrorist is a destruction maximizer, he targets the non-dominated link on a shipment's path that possesses the greatest vulnerability. If the path does not contain a non-dominated link, the Terrorist will not consider attacking any links along this path and the path utility is simply the utility given from completing the route. Using this logic, we develop a routing scheme in which the Shipper/Carrier decides that all shipments besides the selected shipment use the path that offers the greatest utility in the case of no attack and the chosen shipment uses the path that offers the greatest utility in the case of an attack. In Step 2, the number of routing schemes added is equal to the number of shipments, though the number of unique routing scheme may be less.

Let's examine Shipment σ from Step 1. We focus on this shipment's three best utility routes in the case of no attack, all shown in Figure 3. Also, say we know that Links R S, and T are non-dominated, in addition to other links on paths not utilized by Shipment σ from the dominance criterion applied to the routing schemes developed in Step 1.

If Shipment σ were to use its best route in the case of no attack, Link S will be attacked since it is the most vulnerable link on this route. Similarly, Link T will be attacked when the secondary route is used and Link R is attacked when the tertiary route is used.

Table 2 shows Shipment σ's path utilities for two different attack probabilities (p = 0.001% and 0.01%) for the three routes. From this we see that when the probability of attack is low (0.001%), the best strategy is to have Shipment σ use its primary route because it is the primary route which offers the best path utility in the case of an attack (-108.81). This infers that the loss from an attack on Link S when Shipment σ uses its primary route is less than the combined utility loss of using a non-primary route and having a link on this non-primary route being attacked. From this, we create a routing scheme where every shipment, including Shipment σ, uses their best route in the case of no attack. When the probability of an attack is 0.01%, on the other hand, there is an advantage to having Shipment σ use its tertiary route since it is this route that has the maximum path utility in the case of an attack on Link R (-111.87). The expected exposure on the third route's most vulnerable link - Link R - is less the expected exposure on the other two paths' most vulnerable links, making it advantageous despite a lower route utility in the case of no attack. For this p, a routing scheme is added that has Shipment σ using its third best route in the case of no attack, and all other shipments using their best route in the case of no attack.

Table 2. Shipment σ's route utilities in the case an attack on its most vulnerable links

Route preference in the case of no attack	Route utility in the case of no attack	Path's targeted link	Exposure on the Path's targeted link	Route utility in the case of an attack and p = 0.001%	Route utility in the case of an attack and p = 0.01%
First	-108.14	S	67,000	-108.81	-114.83
Second	-108.40	T	42,100	-108.82	-112.60
Third	-108.49	R	33,900	-108.83	-111.87

In Step 2, we select the path for each shipment that minimizes the route utility loss in the case of an attack, assuming the Terrorist will target the most vulnerable non-dominated link on a given path. However, all players may choose to and receive benefit from varying their strategy. Therefore, in Step 3, we consider the ability of the Terrorist to use mixed strategies and consider what the Shipper/Carrier might do in response.

This is done as follows: We consecutively select a previously developed routing scheme which gives us a defined strategy for each shipment. Given the Shipper's/Carrier's strategy for an individual shipment, we successively allow an attack to occur on each of the non-dominated links already defined and see if the Shipper/Carrier receives an improvement in route utility in the case of an attack on one of these non-dominated links from having a shipment use a different path. If so, a new routing scheme is added, which is identical to the routing scheme being examined, except for the new route for the given shipment. Notice that this doesn't yield a routing scheme with multiple routes for a single shipment. Rather it adds a new routing scheme with the new route assigned to a single shipment. This process is iterative, meaning each newly defined routing scheme is examined for attacks on multiple non-dominated links using the same logic. Step 3 is complete once every routing scheme has been examined for route utility improvements in the case of attacks on non-dominated links. The last iteration produces no new routing schemes. Occasionally, new non-dominated links are discovered. When this occurs, all routing scheme developed before this discovery are reexamined for a path utility improvement in the case of an attack on the newly discovered non-dominated link.

This is illustrated using the routing scheme developed in Step 1, from which we know that given an attack on Link S, Shipment σ uses its second highest utility route in the case of no attack and all other shipments use their highest utility routes in the case of no attack. Like Step 2, assume that Links R, S, and T, in addition to other links not in this region and of current interest, are non-dominated. We now introduce Shipment τ, which is also departing from Oakland (for Los Angeles, CA). Shipment τ's highest, second highest, and third highest utility routes in the case of no attack are shown in Figure 4. Note that Shipment τ's secondary and tertiary routes overlap on the link traveling through Modesto.

We know from Step 1, when an attack occurs only on Link S, Shipment τ uses its primary route, since this path does not traverse Link S and therefore does not pose a threat to this shipment. We are now concerned with Shipper's/Carrier's best response for Shipment τ in the case of an attack on Link R or S. Table 3 shows Shipment τ's path utility in the case of no attack for its three top routes, the expected losses from an attack on Links R and S, and the path utility in the case of an attack on Links R or S. The last column shows the worst possible expected path utility from a combination of attacks on Links R and S. For example, should the Shipper/Carrier decide that Shipment τ should use its primary route, the worst expected path utility results from an attack on Link R exclusively. Similarly, the worst expected path utility from Shipment τ using its secondary route comes from an exclusive attack on Link S. Should Shipment τ use its tertiary route, the expected path utility in the case of any combination of a frequency of attacks on Links R and S is the same as the case of no attack. Given the worst case scenario for attacks on Links R or S, the Shipper/Carrier is best served by having Shipment τ use its tertiary route since it has the highest worst case expected path utility in the case of an attack on Links R or S. From this, we create

a routing scheme where Shipment σ uses its secondary route, Shipment τ uses its tertiary route, and all other shipments on the network use their primary route in the case of no attack.

Table 3. Shipment τ's path utility in the case of an attack on Links R or S and p = 0.01%

Route preference in the case of no attack	Route utility in the case of no attack	Expected losses from an attack on Link R	Expected losses from an attack on Link S	Expected path utility from an attack on Link R	Expected path utility from an attack on Link S	Worst Case Scenario	Min-imum
First	-108.40	0.34	0	-111.78	-108.40	Link R is attacked	-111.78
Second	-108.52	0	0.67	-108.52	-115.20	Link S is attacked	-115.20
Third	-108.53	0	0	-108.53	-108.53	None	-108.53

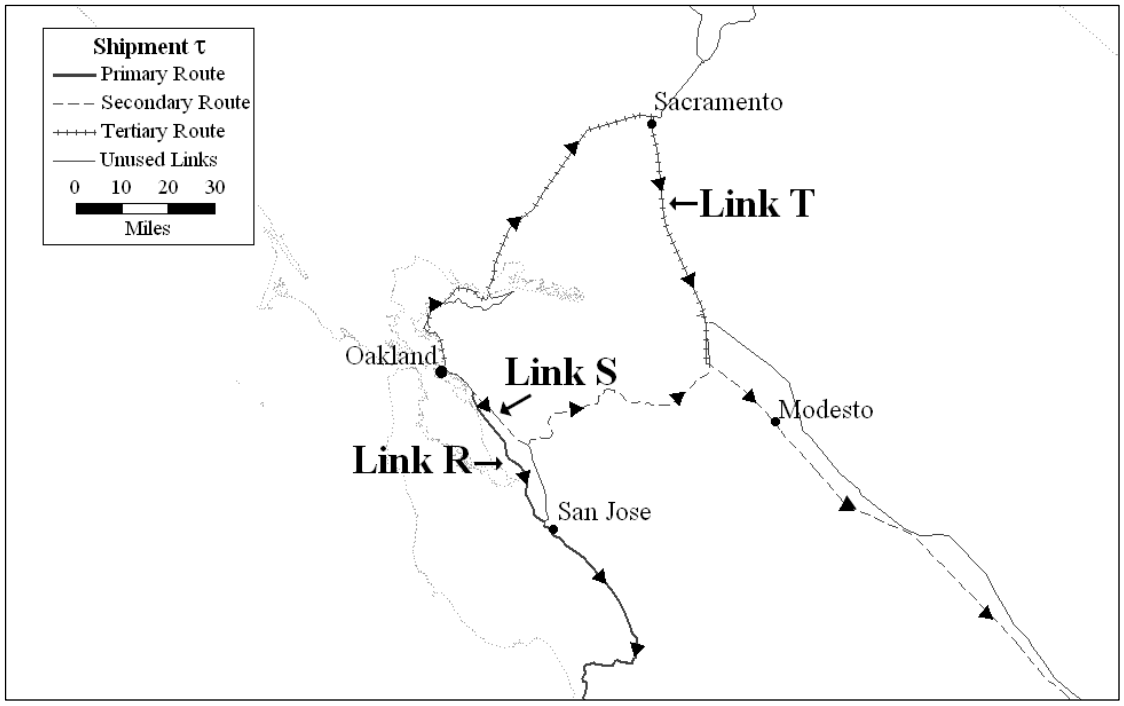

Figure 4. Shipment τ's strategies

In Step 4 we apply the dominance criteria iteratively to the Shipper's/Carrier's and Terrorist's payoff matrices, *A* and *B*, until no strategies can be removed.

Steps 1 through 4 provide a heuristic for generating routing schemes that are likely to be non-dominated strategies for both the Shipper/Carrier and the Terrorist. They are critical component for completing the solution procedure described in 4.2, where we evaluate the expected payoffs to the Shipper/Carrier and the terrorist for all combinations of non-dominated link closures and from this identify the efficient frontier.

Before identifying the set of non-dominated links and estimating the trade-off frontier (between the return to the Shipper/Carrier and the Terrorist) for a given value of *p*, via the process described in section 4.2, it is useful to examine the impact of adopting a "simple" rule to identify the prohibitions. This provides a mechanism to compare the restrictions developed via the process in Section 4.2. A reasonable simple rule might be to enact prohibitions on links with high exposure. The following subsection focuses on the performance of this type of rule. Subsections 5.3 and 5.4 apply the method described in Section 4.2 to estimate the efficient frontiers when $p = 0.001\%$ and $p = 0.01\%$, respectively.

5.2 Closing the N most populated links, probability of an attack = 0.001%

Before identifying the set of non-dominated links and estimating the trade-off frontier (between the return to the Shipper/Carrier and the Terrorist) for a given value of *p*, via the process described in Section 4.2, it is useful to examine the impact of adopting a "simple" rule to identify the prohibitions. This provides a mechanism to compare the restrictions developed via the process in Section 4.2. A reasonable simple rule might

be to enact prohibitions on links with high exposure. The following subsection focuses on the performance of this type of rule.

Figure 5 shows the expected payoffs to the Terrorist and the Shipper/Carrier when the links are ranked in order of their exposure levels and then successively closed (with all links having higher exposure levels being closed as well) when $p = 0.001\%$. As the figure shows, closing the five most populated links on the networks is no better (and albeit no worse) than closing no links. When the top six through the top 21 most populated links are restricted, the expected payoff to the Terrorist increases by approximately 50% to 0.30 - despite the best of intentions of the Government.

When the 22 most populated links are restricted, the expected payoff to the Terrorists drops to 0.2 - approximately the same exposure level as when no links are restricted. Here, the expected payoff to the Shipper/Carrier decreases (from about -108 to -120) since about 2% (840 out of 44,720) of total carloads is unable to be transported.

Closing the top 25 most populated links reduces the expected payoff to the Terrorist to 0.10. The Terrorist receives the same expected payoff whether the top 25 most populated links are restricted or the top 56 links are restricted. However, as more links are added, the expected payoff to the Shipper/Carrier continues to decrease as more desirable routes become unavailable and additional shipments are prohibited from transport (due to lack of available paths). When the top 25 populated links are restricted, 5.3% of total carloads cannot be transported. When the 30 most populated links are restricted, 6.4% of total carloads become infeasible though maintaining the expected return to the Terrorist.

In order to limit exposure to 8,000, the top 70 most populated links on the network must be restricted. This comes at significant expense to the Shipper/Carrier as 10.3% of total carloads are not able to be shipped.

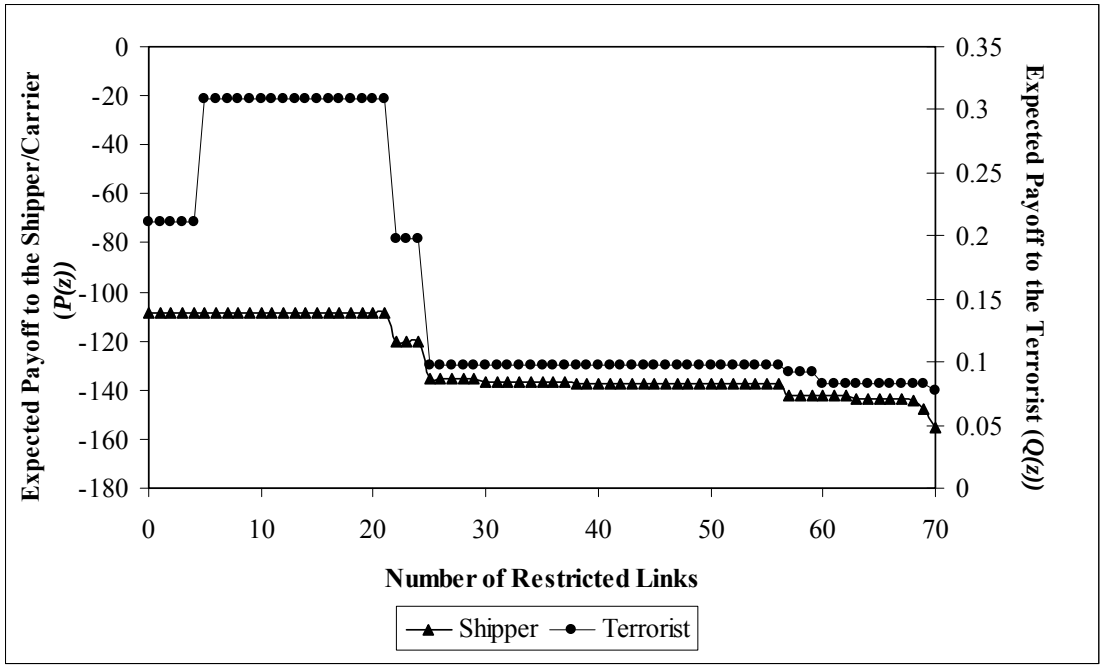

Figure 5. Expected payoff to the Shipper/Carrier and the Terrorist from closing the most populated links

5.3 Probability of an attack = 0.001%

Table 4 and Figure 6 show the efficient frontier from the solutions found for p = 0.001%. The four solutions (Points I, II, III, and IV) represent the Nash equilibria of four efficient sets of link restrictions. Point I represents the Nash equilibrium when no link restrictions are imposed on the network and the expected payoff to the Terrorist is allowed to be arbitrarily high. Points II through IV represent link restrictions that reflect the increasing interest in limiting the potential impacts of an attack. Figure 7Figures 7 and 8 show the key links.

Table 4. Efficient frontier for the case study (p = 0.001%)

Point	**Restrict-ions**	**Number of Links Restricted**	**Links Closed**	**Car-loads not shipped per year (% of total)**	***P(z)* (Expected payoff to Shipper/ Carrier)**	**Expected Utility for Shipper when no Attack occurs**	***Q(z)* (Expected payoff to Terrorist)**	**Strategy adopted by the Shipper**		**Strategy adopted by the Terrorist**	
								Routing Scheme Chosen	Probabil-ity with which the routing scheme is chosen (%)	Link Chosen	Probabil-ity with which the link is chosen (%)
I	None	None	None	0 (0%)	-108.43	-108.22	0.21	*a*	68	S	5
								b	32	T	95
II	$\beta \leq 0.2$	3	Q, R, S	840 (1.9%)	-120.08	-119.88	0.20	*c*	100	U	100
III	$\beta \leq 0.1$	7	L, Q, R, S, U, Y, Z	2400 (5.4%)	-135.20	-135.10	0.10	*d*	63	K	59
								e	37	W	41
IV	$\beta \leq 0.08$	8	K, N, Q, R S, U, W, Y	2880 (6.4%)	-140.90	-140.82	0.08	*f*	100	M	100

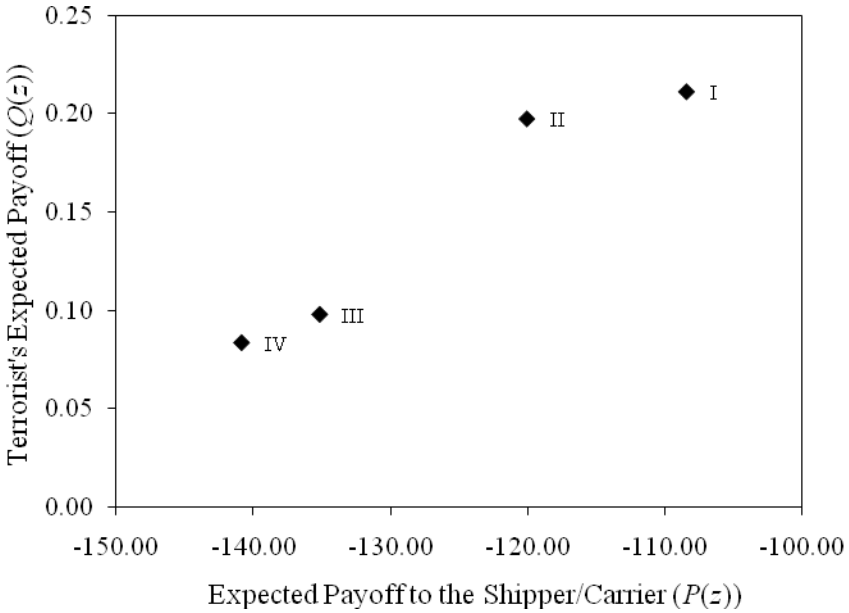

Figure 6. Efficient Frontier for the case study (p = 0.001%)

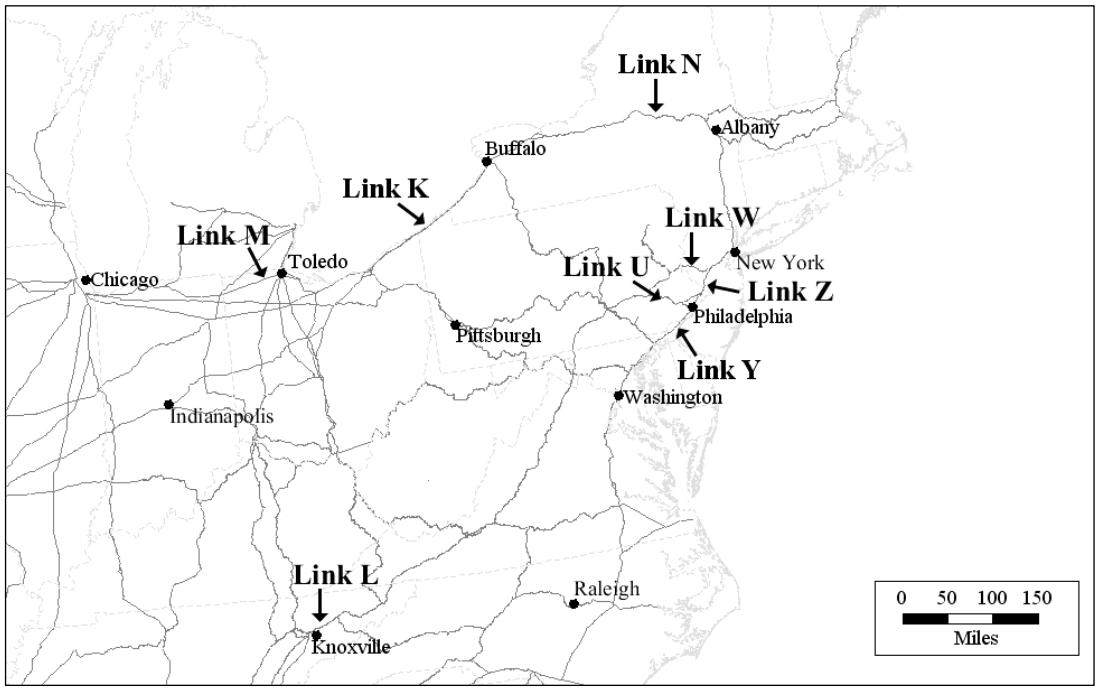

Figure 7. Key links in the Eastern US

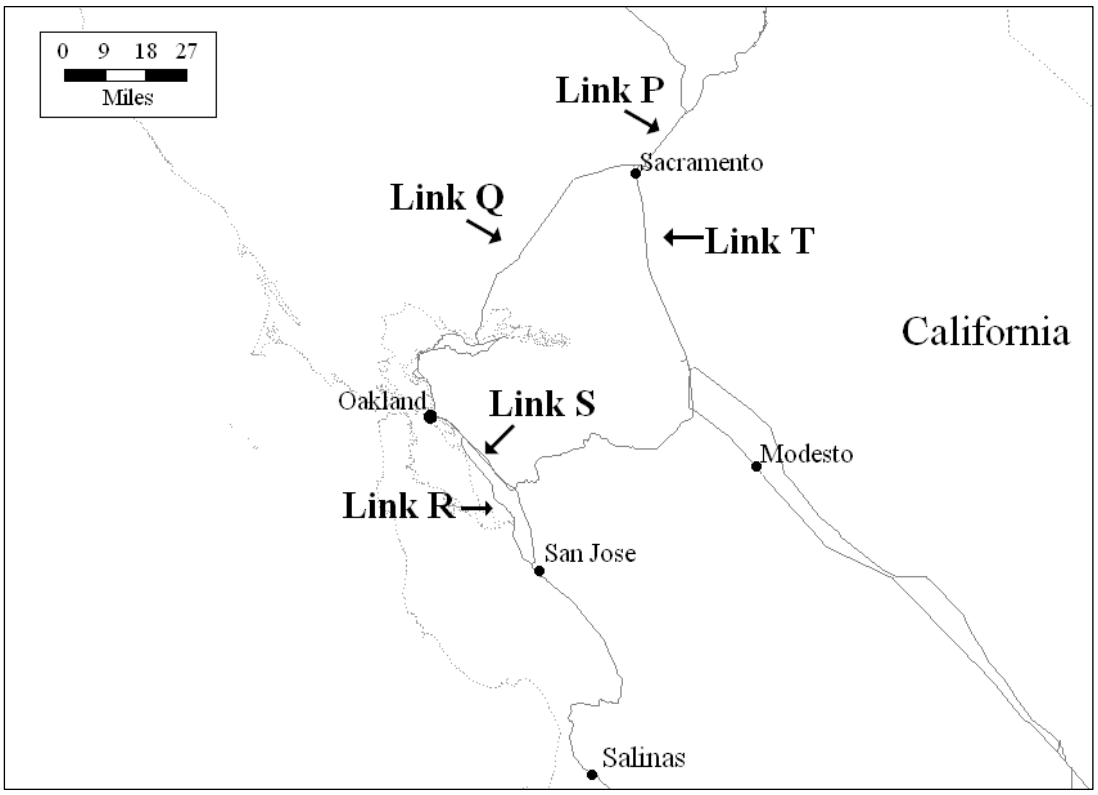

Figure 8. Key links in Northern California

At Point I, the likelihood of an attack is high enough to dissuade the Shipper/Carrier from having Shipment σ exclusively use its route with the highest utility in the case of no attack (shown in Figure 3) and to use Shipment σ's second highest utility route in the case of no attack with some frequency. These two routes traverse the network's most populous links, Links S and T. All other shipments use routes that offer the highest utility in the case of no attack since these routes do not use these links (S and T), including Shipment *τ*, as seen in Figure 4. As a result, the Shipper/Carrier chooses Routing Scheme *a* where all shipments use their utility maximizing route in the case of no attack, with a probability of 68% and Routing Scheme *b* where all shipments use their utility maximizing route in the case of no attack with the exception of Shipment σ, who is traveling from Oakland, CA to Houston, TX using his secondary route, with a probability of 32%.

Links S and T are attacked with a probability of 5% and 95% respectively. The severity of an attack is ameliorated by the fact that the Terrorist only knows with some probability when and where Shipment σ will be present, so some attempts will be unsuccessful. The attack rates on Links S and T reflect the Terrorist hedging their strategy to maximize their payoff. The expected payoff to the Terrorist is 0.21, which translates to a population exposure of 21,000 when the probability of an attack is 0.001%.

It is also worth noting that it is not necessarily a good strategy to simply close the links the Terrorist would target. Take Links S and T for example. They are the most populated links on the West Coast and the links that the Terrorist targets at the Nash Equilibrium represented by Point I. If the Government (say a local government) chooses to close Links S and T, as shown in Figure 9, all shipments have feasible routes available to them. Shipment τ has access to its primary route in the case of no attack and Shipment σ no longer has access to his primary and secondary routes, but has access to his tertiary route. (See Figures 3 and 4). Furthermore, the Shipper/Carrier can have Shipments σ and τ can use any route that enters Oakland via Link P to Link Q. (See Figure 9).

In this case, the Shipper/Carrier finds the maximum benefit from having each shipment use the highest utility route available to them with 100% probability and do not see any economic advantage from taking a route that uses Link Q. Shipment σ uses his tertiary route and Shipment τ uses his primary route. Link R has the largest population exposure at the time of truck crossing among all links in this routing scheme and will be attack with 100% probability. The expected payoff to the Terrorist

is 0.34, which is more than 50% greater than the Terrorist's expected payoff when no link restrictions are imposed. The Shipper's/Carrier's expected payoff is -108.91. The Nash equilibrium represented by Point I, where no links are restricted, is a better strategy from the Government and Shipper's/Carrier's perspective since it has a lower expected payoff to the Terrorist (0.21) and a higher expected payoff to the Shipper/Carrier (-108.43). Keeping Links S and T open allows Shipments σ and τ to use a mixed strategy that uses high utility routes. In this case, this reduces the expected payoff to the Terrorist and increases the expected payoff to the Shipper/Carrier.

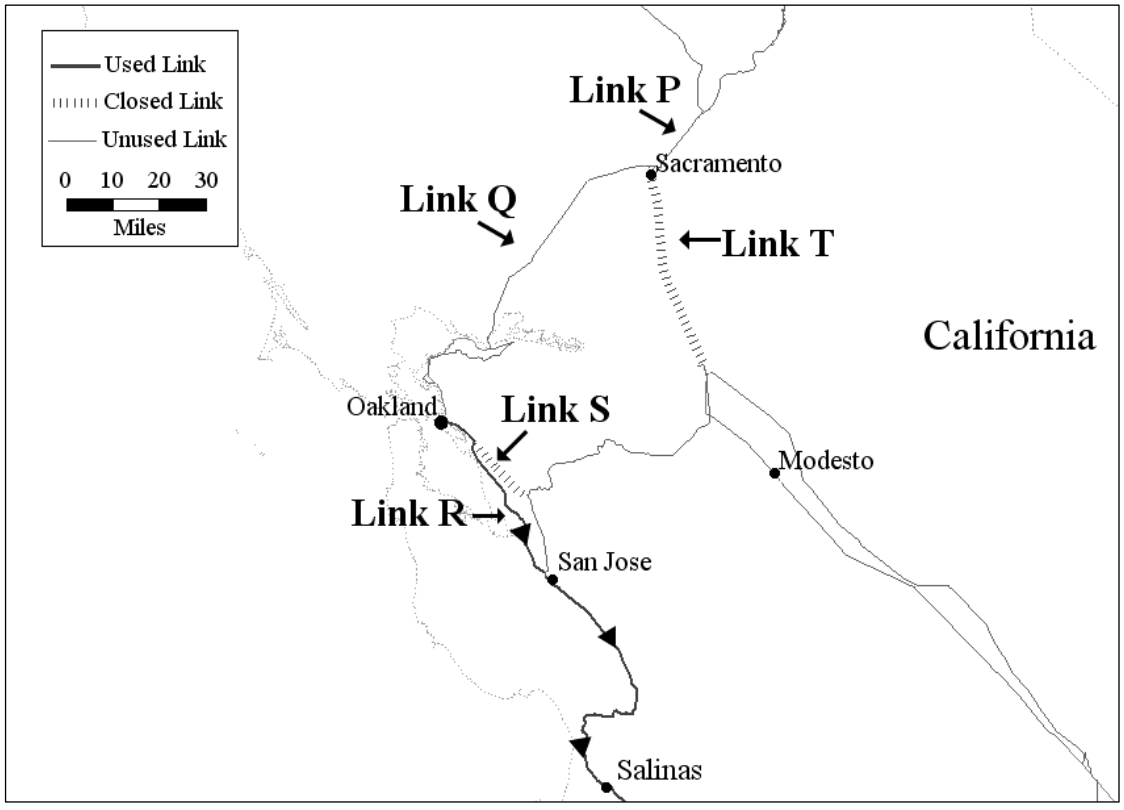

Figure 9. Nash Equilibrium when p = 0.001% and Links S and T are restricted (arrows indicate Shipment σ and τ's selected route)

Point II is the result of establishing the prohibitions in the Oakland, CA area, as illustrated in Figures 10 and 11. Links Q, R, and S are closed. This point has an equivalent expected payoff to the Terrorist to closing the top 22 most populated links as shown in Section 5.2. Shipments σ and τ are prevented from traveling since all of their possible paths use a closed link. All remaining shipments solely use their highest utility route in the case of no attack, creating Routing Scheme *c*. Exclusive use of this routing scheme leads to a 10.7% drop in the expected payoff to the Shipper/Carrier but only a slight decrease in the expected payoff to the Terrorist, as seen in Figure 6. Utility loss to the Shipper/Carrier stem from two causes: Shipments σ and τ not being able to travel and losses from an attack on Link U. By restricting these links, the Government creates a Nash equilibrium that reduces the Terrorist's expected payoff by 4.7% to 0.20 and keeps the expected exposure level of 20,000. There exist no combinations of link closures that has the Shipper/Carrier optimally reroute Shipments σ and τ in a way that allows these shipments to travel and keeps exposure levels to below 20,000. To get an expected exposure level of 20,000 and still allow travel from Oakland, additional links in the network around Oakland are necessary. This would provide for additional options for the Shipper/Carrier which are less attractive to the Terrorist.

Since the Shipper/Carrier always uses Routing Scheme *c*, the Terrorist always attacks the link (Link U) on that routing scheme with the largest value of exposure, as illustrated in Figure 10.

.

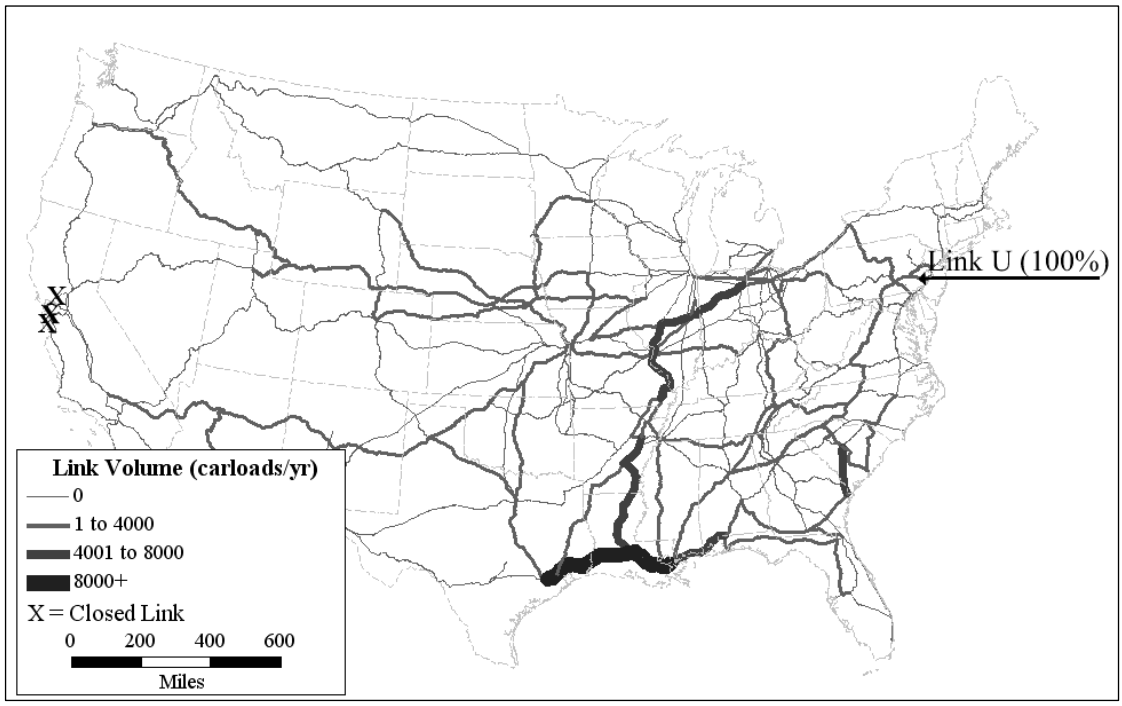

Figure 10. Nash Equilibrium for Point II, Routing Scheme *c* (p = 0.001% and 3 link restrictions)

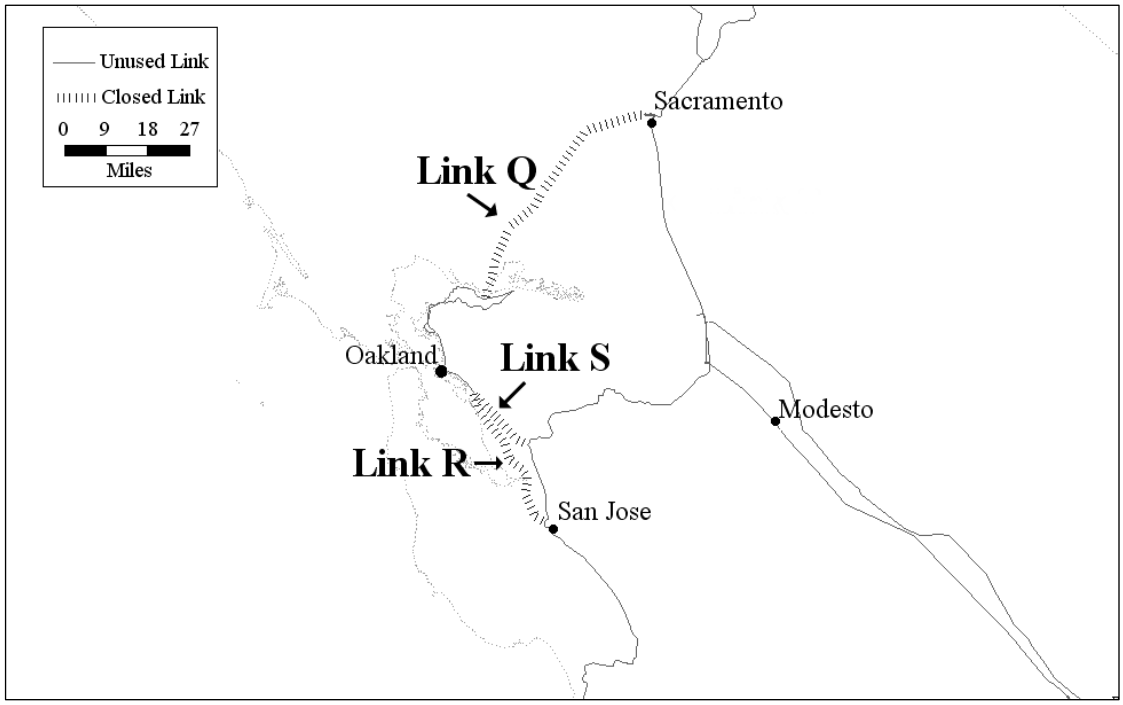

Figure 11. Link restrictions Q, R, and S

Point III in Figure 6 represents a decline of about 53% in the payoff to the terrorist when seven links are prohibited from use. Figure 12 and 13 give the two routing schemes associated with this Nash equilibrium. This set of seven link restrictions prohibits movements into and out of Philadelphia (U,Y and Z) and Oakland (via links Q,R and S) as well as access to one link near Knoxville, TN - Link L. Note that four of the restricted links are shown in Figures 12 and 13. The other three restricted links prohibit access to Oakland and are shown in Figure 11. 5.3% of total carloads are not shipped. The Terrorist attacks Link W with a frequency of 41% and Link K with a frequency of 59%.

The expected payoff to the Terrorist represented by Point III is equivalent to the expected payoff to the Terrorist when the top 25 most populated links through the top 56 most populated links are restricted in Section 5.2. The expected payoff to the Shipper/Carrier is slightly better in Point III compared to these restrictions from Section 5.2. For example, when the top 30 links are restricted, an additional 480 carloads are not shipped compared to Point III. This is due to inefficient link restrictions that do nothing to reduce the exposure levels but do prevent transport of hazmats, and hence reduce the expected payoff to the Shipper/Carrier.

Closing Link L is unintuitive since it does not border a densely populated US city. Simply closing the links providing access to Philadelphia and Oakland when p = 0.001% reduces the expected payoff to the Terrorist 0.19 – a nominal decrease from when only access to Oakland is restricted (Point II in Figure 11).

To understand why, we focus on Shipment ρ which is traveling from Baton Rouge, LA to New York City, NY. When Link L is opened, the Shipper/Carrier selects Shipment ρ's primary route in the case of no attack for use, shown in Figure 14. This route traverses Link W, the most populated, unrestricted link on the network and is the link the Terrorist will attack exclusively. Despite large potential losses from an attack, the Shipper/Carrier receives no economic incentive from varying Shipment ρ's strategy. The Terrorist receives an expected payoff of 0.19 from this strategy. Prohibiting Link L makes all of Shipment ρ's 50 highest utility routes in the case of no attack infeasible with the exception of Routes 11 and 33. Figure 14 also shows these 2 routes. When Link L is closed, the Shipper/Carrier selects Route 11 for Shipment ρ with 63% probability and Route 33 with 37% probability. All other shipments not barred from travel use their primary route in the case of no attack. This creates Routing Schemes *d* and *e*. Route 11 traverses Link W, though at a time of day when Link W is slightly less populated than when the primary route traverses Link W, further reducing the Terrorist's expected payoff. The Terrorist finds benefit in varying his strategy as well. He attacks Link W with 41% probability and Link K with 59% probability. However, the best expected payoff the Terrorist can receive is 0.10, equivalent to an exposure of 10,000.

So, by the Government closing Link L, the Shipper/Carrier is slightly worse off, only because Shipment ρ does not have access to its primary route. However, the Terrorist's expected payoff decreases dramatically. There is no other combination of non-dominated link restrictions that provide a greater expected payoff to the Shipper/Carrier while maintaining the Terrorist's expected payoff to this level, making Point III efficient.

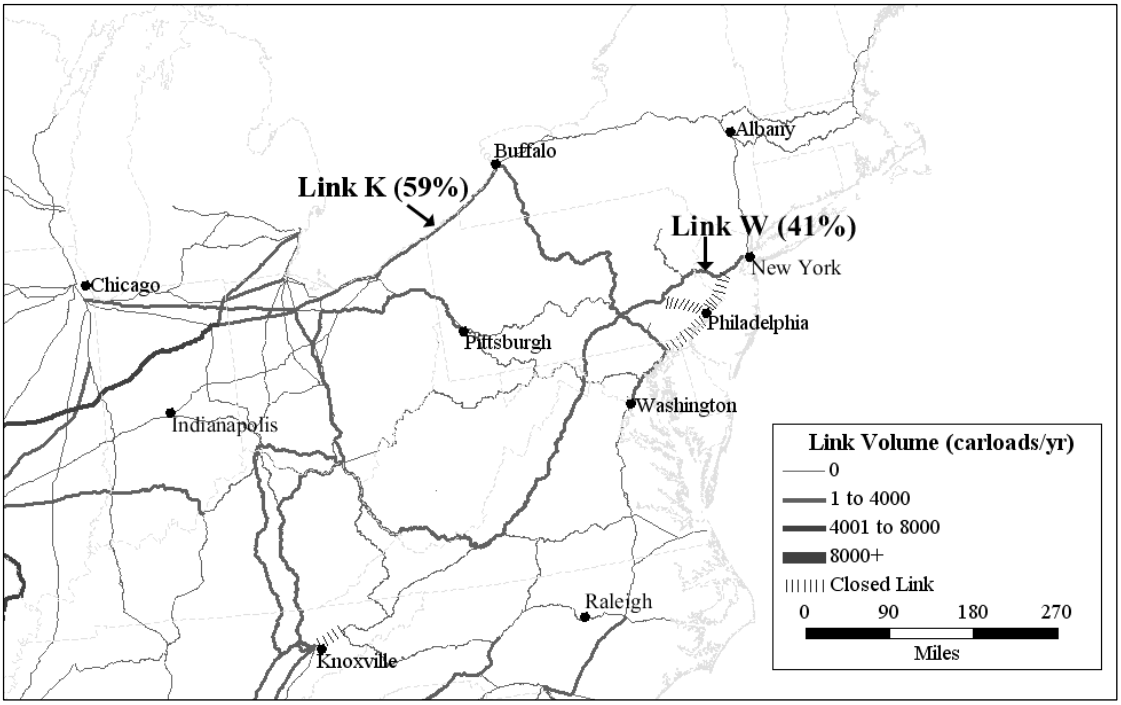

Figure 12. Nash equilibrium for Point III, Routing Scheme *d* (p = 0.001% and 7 link restrictions, 4 of which are shown)

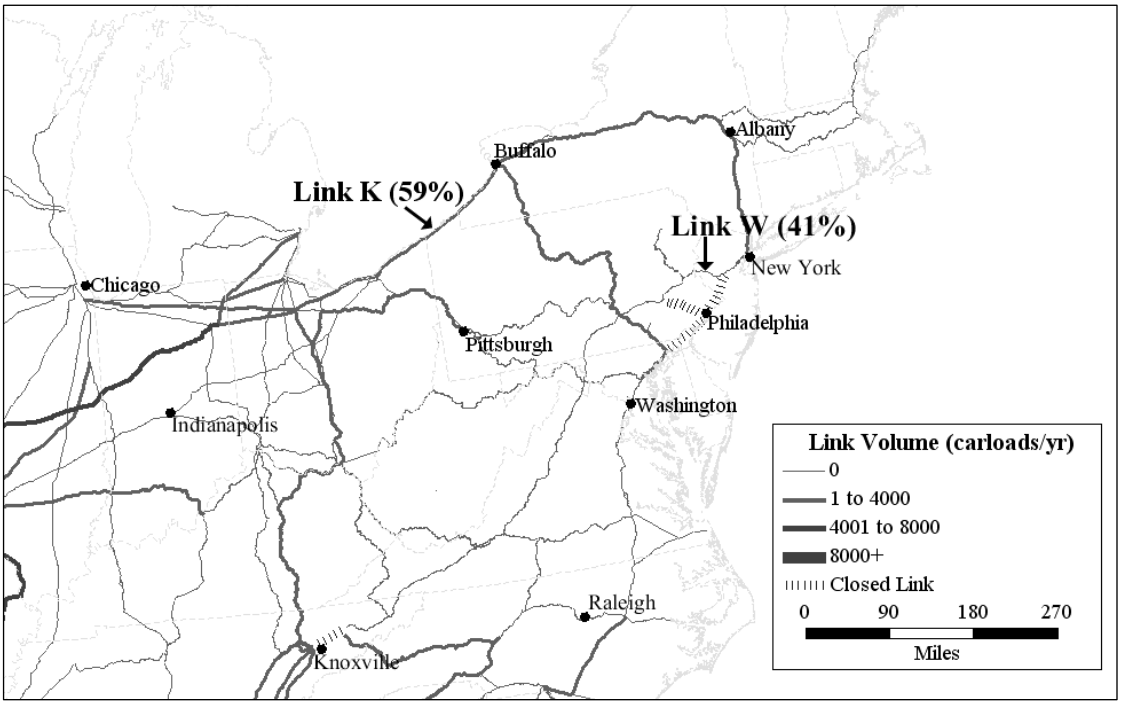

Figure 13. Nash equilibrium for Point III, Routing Scheme *e* (p = 0.001% and 7 link restrictions, 4 of which are shown)

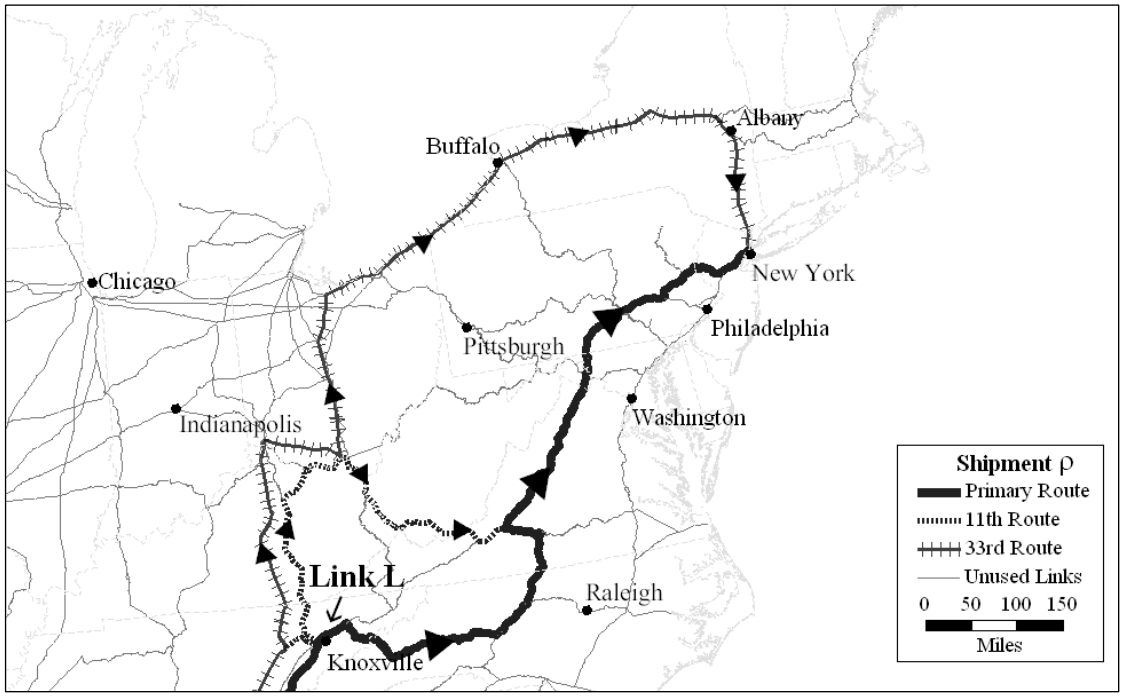

Figure 14. Shipment ρ's strategies

By using a mixed routing strategy, the Shipper/Carrier transfers some vulnerability onto other shipments. Figure 13Figures 12 and 13 show that there is always positive link volume on Link K, though we know Shipment ρ only traverses Link K when using Route 33. Therefore, there is at least one other shipment on the network which uses Link K and who will be present when Shipment ρ is not. This has two implications: there will always be a shipment present for an attack on Link K and this shipment may not be Shipment ρ. Therefore, other shipments become vulnerable to an attack when a mixed strategy is used.

Point IV represents the Nash equilibrium of the most restrictive network, with eight link restrictions. Five of the eight links restricted by the Government are shown in Figure 15. The three other restricted links block access to Oakland and are also

restricted by Points II and III, as shown in Figure 11. The expected payoff to the Terrorist is controlled to 0.08 – a 61.9% reduction from expected payoff to the Terrorist offered by Point I and the optimal solution when the government aims to restrict expected exposure to 8,000. The increased restrictions make some routes infeasible. The Shipper/Carrier is prevented from making shipments to and from Oakland, Philadelphia, and New York City. 6.4% of total carloads are not shipped.

The expected payoff to the Terrorist represented by Point IV is equivalent to the Terrorist's expected payoff when the top 70 most populated links are restricted, as seen in Section 5.2. However, the expected payoff to the Shipper/Carrier represented by Point IV, -140.9, is greater than the expected payoff to the Shipper/Carrier when the top 70 most populated links are restricted, -147.8. When the top 70 most populated links are restricted, 10.3% of total carloads are restricted from transport in contrast to 6.4% based on the restrictions associated with Point IV.

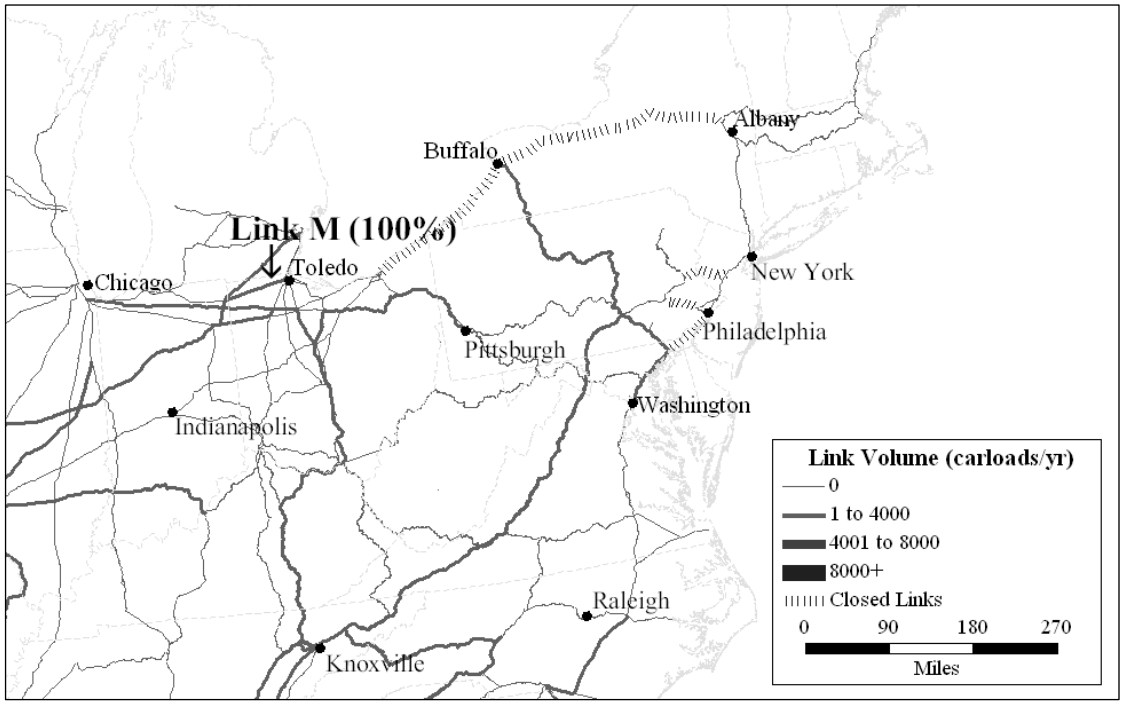

Figure 15. Nash Equilibrium for Point IV (p = 0.001% and 8 link restrictions, 5 of which are shown)

5.4 Probability of an Attack = 0.01%

Table 5 and Figure 16 show the efficient frontier from the solutions found for p = 0.01%. For a higher probability of an attack, the Shipper/Carrier chooses to be more conservative with their routing decisions and the Government does not need to apply as many restrictions. For example, to control the return to the terrorist below a threshold of 8,000, 8 link restrictions are needed with the probability of attack is 0.001% in contrast to 6 when the probability of attack is 0.01%.

Table 5. Efficient frontier for the case study (p = 0.01%)

Point	**Restrict-ions**	**Number of Links Restricted**	**Links Closed**	**Car-loads not shipped per year (% of total)**	***P(z)* (Expected payoff to Shipper/ Carrier)**	**Expected Utility for Shipper when no Attack occurs**	***Q(z)* (Expected payoff to Terrorist)**	**Strategy adopted by the Shipper at the Nash Equilibrium**		**Strategy adopted by the Terrorist at the Nash Equilibrium**	
								Routing Scheme Chosen	Probabil-ity with which the routing scheme is chosen (%)	Link Chosen	Probabil-ity with which the link is chosen (%)
V	None	None	None	0 (0%)	-110.23	-108.26	1.97	*a*	51	R	6
								b	29	S	3
								g	7	T	15
								h	13	U	76
VI	$\beta \leq 1.5$	3	U, Y, Z	1560 (3.5%)	-124.86	-123.46	1.41	*j*	46	R	12
								k	33	S	15
								l	12	T	28
								m	9	W	45
VII	$\beta \leq 0.8$	6	Q, R, S, U, Y, Z	2400 (5.4%)	-135.93	-135.11	0.80	*n*	39	K	11
								q	15	V	77
								s	46	W	12

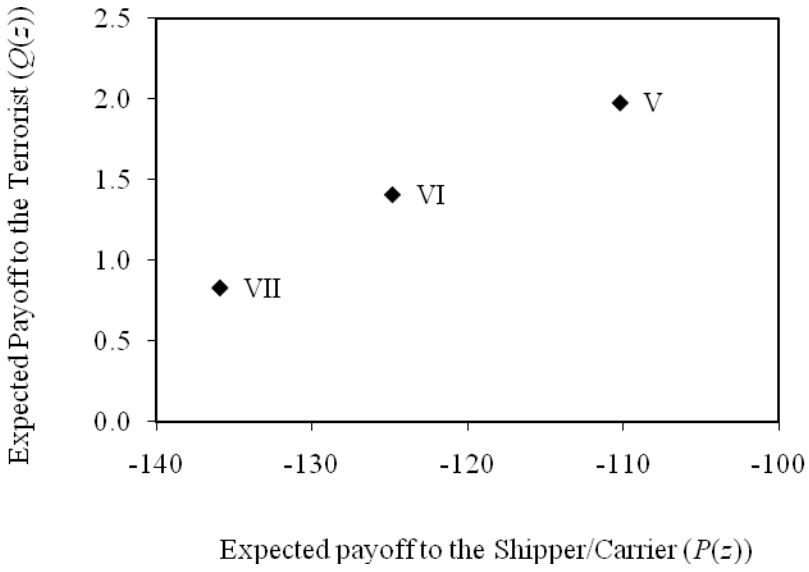

Figure 16. Efficient Frontier for the case study (p = 0.01%)

Point V on the efficient frontier represents the solution obtained when there is no limit on the expected payoff to the Terrorist and thus there are no restrictions on the network. In this case, the probability of an attack is high enough to dissuade the Shipper/Carrier from having Shipments σ and τ exclusively use the routes that offer the highest utility in the case of no attack, because it is links on these routes that the Terrorist primarily targets. Shipments σ's and τ's strategies combine to create four unique routing schemes. Routing Scheme *a* is used with 51% probability and has all shipment using their primary route. Routing Scheme *b* is used with 29% and has all shipments using their primary route except for Shipment σ, which uses its secondary route. Routing Schemes *a* and *b* are identical to Routing Schemes *a* and *b* when p = 0.001%. Routing Scheme *g* is used with 7% probability and is identical to Routing Scheme *b* except that Shipment σ uses its tertiary route. Routing Scheme *h* is used with 13% probability and Shipment τ uses his secondary route and all remaining

shipments use their primary route. Shipments σ's and τ's strategies can be seen in Figures 3 and 4.

Just as the Shipper/Carrier finds benefit in a mixed strategy, so does the Terrorist. He attacks Links R, S, T, and U with probabilities 3%, 15%, 76%, and 6% respectively. (Link U is shown in Figure 17 and is utilized by shipments entering and leaving Philadelphia.) Despite Links S and T having high exposure levels, they are infrequent targets of an attack. This is due to the diversified strategy in the Oakland area providing ambiguity as to the location of Shipments σ and τ. Link U is targeted with a reasonably high possibility (76%). Shipments transporting hazmats to and from Philadelphia do not attain economic benefit by varying their strategy at this risk level. The Terrorist's expected return when the probability of attack is 0.01% is 1.97, meaning the expected exposure is 19,700 – a 6.2% reduction from the Nash equilibrium strategy of Point I. As the probability of an attack increases, the Shipper/Carrier finds benefit in diversifying his strategy for Shipments σ and τ to offset his risk. This reduces the expected payoff to the Terrorist and shows that the Shipper's/Carrier's and the Government's goals are aligning.

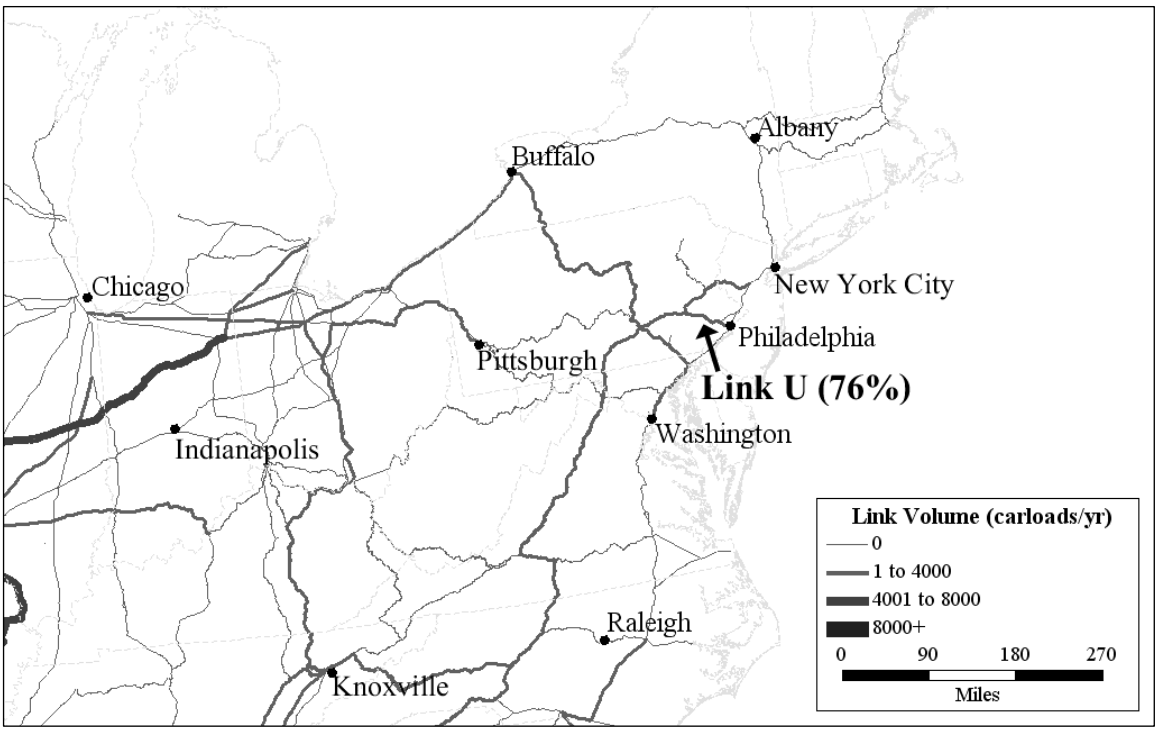

Figure 17. Nash Equilibrium for Point V near Philadelphia (p = 0.01% and no restrictions)

The Nash equilibrium represented by Point VI shows that restricting access to Philadelphia reduces the expected Terrorist's payoff to 1.41 and limits expected exposure to below 15,000 – a 28.4% reduction from the expected exposure levels of Point V. Akin to Point V, the Shipper/Carrier is persuaded to use a mixed strategy for Shipments σ and τ that decreases the expected payoff to the Terrorist. Shipment ρ, who is traveling to New York City, also finds economic benefit from a mixed strategy. Should access to Philadelphia remain, the Shipper/Carrier sees no advantage to varying the strategy of shipments whose origination and destination are Philadelphia and reducing the payoff to the terrorist at this p. Therefore, from the Government's perspective, it is best to first restrict access to Philadelphia, rather than Oakland (when p = 0.001%). Table 6 summarizes the paths selected by the Shipper/Carrier for

Shipments σ, τ, and ρ for Routing Scheme *j*-*m*. Figures 3, 4, and 14 show the paths the Shipper/Carrier selects for Shipments σ, τ, and *ρ*.

Table 6. Routing schemes for the Nash equilibria represented by Point VI

Routing Scheme	**Probability with which the routing scheme is chosen (%)**	**Route of Shipment σ**	**Route of Shipment τ**	**Route of Shipment ρ**	**Shipments Entering or Departing Philadelphia**	**All other Shipments**
j	46	Primary Route	Secondary Route	Primary Route	Do Not Travel	Primary Route
K	33	Tertiary Route	Primary Route	Primary Route	Do Not Travel	Primary Route
l	12	Secondary Route	Tertiary Route	Primary Route	Do Not Travel	Primary Route
m	9	Secondary Route	Tertiary Route	33rd Route	Do Not Travel	Primary Route

Links R, S, and T are attacked with likelihood 15%, 28%, and 12% respectively. Link W provides access to New York City and is attacked with likelihood 45%, as shown in Figure 18.

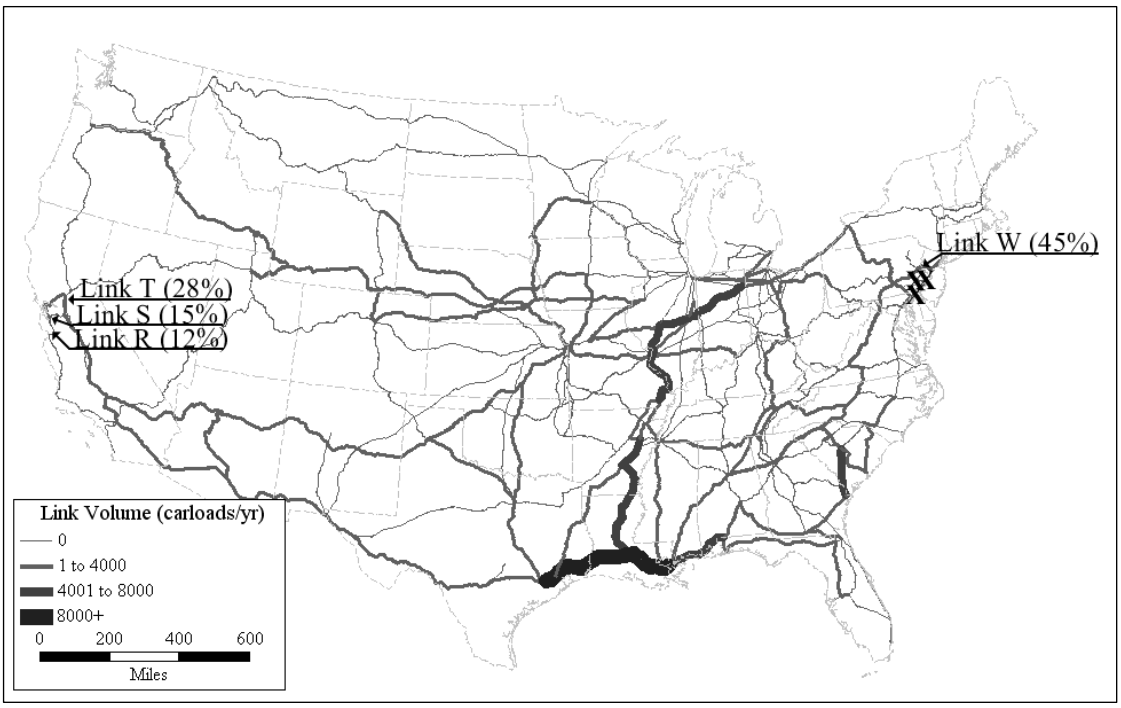

Figure 18. Nash Equilibrium for Point VI, Routing Scheme *j* (p = 0.01% and 3 link restrictions)

Point VII represents the Nash equilibria where the Government wishes to limit the expected exposure to 8,000. This exposure level is equivalent to the expected exposure of Points IV. Notice that in order to get the same expected exposure with a lower probability of an attack to that with a higher probability, the number of link restrictions needs to be greater. For example, Points IV and VII have the same expected exposure, but Point IV requires eight link restrictions while Point VII requires six. Some routes that offer high utility are no longer attractive to the Shipper/Carrier when the probability of attack is higher since they contain links with higher population exposure which leads to worse expected payoffs to the Shipper/Carriers when an attack occurs. Thus the Shipper/Carrier prefers to control the consequences of a successful attack, and therefore the Terrorist's expected payoff, by either avoiding such routes or utilizing a mixed strategy approach. At this point, the

Shipper's/Carrier's and the Government's goals begin to align, and the Government needs to enact fewer prohibitions.

CHAPTER 6

CONCLUSIONS

This paper develops a model of the interactions among a shipper/carrier of a hazardous material, a terrorist and the government using a full origin-destination table to understand: (1) how governments might set link prohibitions to cope with the threat of attack on a shipment of hazardous materials; (2) how the shipper/carrier might make decisions of which routes to use with what frequencies in response to these prohibitions and the underlying threat of terrorism and (3) what links terrorists might then target with what frequencies. In order to achieve this we construct a non-linear integer optimization which is an extension of a two-person, non-zero sum game given in Mangasarian and Stone (1964). In order to effectively solve the resultant optimization for realistic instances, a heuristic was developed to identify the shipper's/carrier's pareto-efficient routing schemes and from that, a heuristic was created to identify effective prohibitions.

The model was then applied to a realistic case study focused on the shipment of a hazardous material on the US rail network, using a full origin-destination table. These analyses illustrated that as the probability of an attack rises, the shipper/carrier should select more and more conservative routes which causes a decline in the expected payoff to the shipper/carrier but also controls the damages caused by an attack. This behavior is of particular importance because historically when considering routing decisions for hazardous material shipments, the emphasis has been on the identification of the single "best" route to use repetitively. This game shows the weakness in that strategy and that it is dominated when the probability of an attack is significant. These analyses also show that as the probability of an attack rise the goals

of the government and the shipper/carrier align. This results in the shipper/carrier making decisions that control the consequences of an attack. Therefore, the government does not need to enact quite as many prohibitions to control the consequences of an attack. The shipper/carrier now has sufficient incentives to avoid links that are particularly attractive targets for the terrorist. Third, this analysis illustrates the weaknesses of identifying prohibitions strictly based on simple metrics like population. In the case study, when link restrictions are placed on only two of the three links out Oakland (which have the highest exposure), there is a doubling of the return to the terrorist (from about 20,000 to 42,000). Also, when links are restricted based on exposure only, the return to the terrorist may actually increase and unnecessary negative impacts to the shipper/carrier may be imposed. Finally, this type of analysis can help identify non-intuitive locations for prohibitions. When the probability of attack is 0.001% when the links around Philadelphia and Oakland are restricted but not the link near Knoxville, the return to the terrorist is about 0.19 but when this additional link is restricted the return drops to about 0.1 (with a modest impact on the shippers; from -135.06 to -135.20).

This paper contributes to the literature by developing a non-cooperative non-zero sum game which represents the interactions between a shipper/carrier, terrorist and the government for the movement of hazardous materials for a single shipper/carrier for multiple origin-destination pairs. It creates reasonable rules to predict what the shipper/carrier and terrorist are likely to do in response to government prohibitions and their interactions with each other. This allows the identification of a single Nash equilibrium point for the interactions between a shipper/carrier and a terrorist for a given value of p and a maximum allowable expected payoff to the terrorist which can

then be used in for decision-making by all three parties. Finally a solution procedure that is effective for realistic problems is also developed.

There are three key areas for additional research. First, extend the formulation and solution procedure to address multiple shippers, each with several origins and destinations. Second extend the game to simultaneously consider a coordinated terrorist attack. These extensions would substantially enrich the decision-making included in the game by all players. Finally, there are other application areas for the tools developed in this analysis. For example, the same core question can be applied to truck weight enforcement. Given unlimited resources, governments would operate truck weigh stations continuously in order to catch all of the overweight vehicles on the US highway system. The methodology described in this paper could be used to optimally determine which weigh stations should be opened at what time to catch as many overweight trucks as possible.

APPENDIX

ILLUSTRATIVE EXAMPLE

To gain a better understanding of the model, we apply it to the example network illustrated in Figure 19. Three shippers are interested in making repetitive shipments between Node 1 and Node 2 (OD 1-2), Node 2 and Node 3 (OD 2-3), and Node 2 and Node 4 (OD 2-4), respectively. Figure 1 also shows the link length, and the off-link population exposure. The probability of attack is assumed to be 1%.

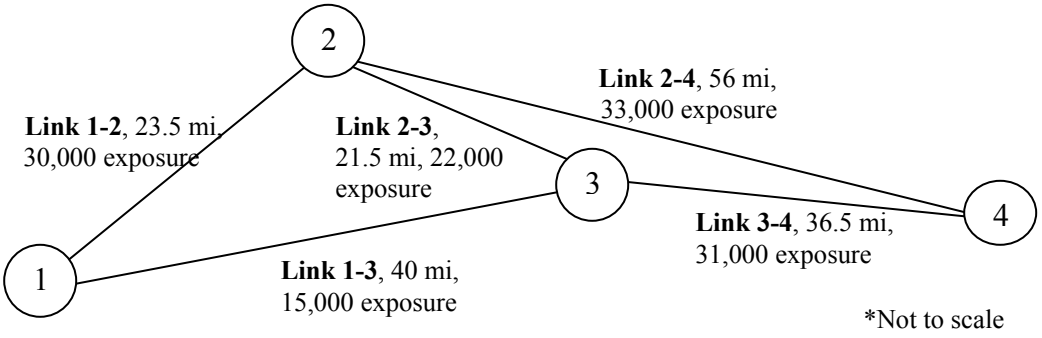

Figure 19. 4-Node, 5-Link Illustrative Network

Three routing alternatives exist for each OD pair and are given in Table 1. In this example, the shipper of each OD pair wishes to minimize cost which is assumed proportional to distance. Since an increase in distance signifies that the shipper is worse off, the negative of the normalized distance, with the minimum distance scaled to -100, is taken as the utility, U_{kq}, of shipper of OD Pair k's route q. Note that the shipper of OD Pair k achieves this utility only in case of no attack.

Table 7. Routing alternatives with utilities for the shippers of OD Pairs 1-2, 2-3, and 2-4

	OD Pair 1-2		**OD Pair 2-3**		**OD Pair 2-4**	
	Route	*Utility of Route*	*Route*	*Utility of Route*	*Route*	*Utility of Route*
OD Pair *k*'s Primary Route	1-2	-109.3	2-3	-100.0	2-4	-260.5
OD Pair *k*'s Secondary Route	1-3-2	-286.0	2-1-3	-295.3	2-3-4	-269.8
OD Pair *k*'s Tertiary Route	1-4-3-2	-616.3	2-4-3	-430.2	2-1-3-4	-465.1

Before we develop potential routing schemes, we examine (1) the expected exposure resulting from an attack on each link and (2) the expected utility of each route when a specific link is attacked. The expected exposure is developed first as this information is necessary for developing (2). The expected utility and expected exposure are necessary components for creating the shippers' routing schemes and computing the shippers' and terrorist's expected payoff matrices, *A* and *B*.

Table 2 shows the expected exposure from an attack on the shipper of OD Pair *k* on Link 1-2 for each of the three available routes. As Table 8 and Figure 19 show, the terrorist's expected payoff from attacking the shipper of OD Pair 1-2 on Link 1-2 when the shipper uses his primary route is 0.01*30,000 = 300. However, if this shipper decides to use his secondary route, the terrorist would expect to receive nothing if he attacks Link 1-2 since this shipper does not traverse Link 1-2. Using the information from Tables 7 and 8 and the probability of an attack, the shipper of OD Pair *k*'s expected utility in the case of an attack on Link 1-2 for each of its three available routes is evaluated.

Table 8. Terrorist's expected payoff from attacking the shipper OD Pair k on Link 1-2

	OD Pair 1-2	**OD Pair 2-3**	**OD Pair 2-4**
OD Pair *k*'s Primary Route	300	0	0
OD Pair *k*'s Secondary Route	0	300	0
OD Pair *k*'s Tertiary Route	0	0	300

Table 9. Shipper of OD Pair k's expected utility for each available route in the case of Link 1-2 being attacked

	O-D Pair 1-2	**O-D Pair 2-3**	**O-D Pair 2-4**
OD Pair *k*'s Primary Route	**-408.2**	-100.0	-260.5
OD Pair *k*'s Secondary Route	**-286.0**	-592.4	-269.8
OD Pair *k*'s Tertiary Route	-616.3	-430.2	-760.5

Table 9 shows the shipper of OD Pair *k*'s expected utility in the case of an attack on Link 1-2 for all three available routes. If the shipper of OD Pair *k* does not use Link 1-2 when traveling on a specified route, the expected utility is simply the utility of that route, given in Table 7. Otherwise, the expected utility is the expected utility of route *q* in case of no attack (from Table 7) minus the expected value of damage caused by a successful attack (from Table 8). For example, since the shippers of OD Pair 1-2's primary route uses Link 1-2, its expected payoff on Link 1-2 is 99% * -109.3 - 1% * 30,000 = -408.2. However, since the shipper of OD Pair 1-2 does not use Link 1-2 when traveling his secondary route, the expected payoff on Link 1-2 is -286.0, which is the utility of his secondary route.

The goal of the first step for creating routing schemes is to maximize the shippers' total path utility in the case of an attack on a specific link. We illustrate this assuming an attack on Link 1-2 and create a routing scheme that is non-dominated in case of an attack on this link. The shippers of OD Pairs 2-3 and 2-4 do not traverse Link 1-2

when traveling their primary route, so they contribute their primary, highest utility routes to the routing scheme. On the other hand, the expected utility of the shipper of OD Pair 1-2's primary route is less than the expected utility of his secondary route, as seen in Table 9. This is because his primary route traverses Link 1-2, where the risk level is high. Therefore, the shipper of OD pair 1-2 contributes his secondary route to this routing scheme. We add Routing Scheme Γ, where the shippers of OD Pairs 2-3 and 2-4 use their primary routes and the shipper of OD Pair 1-2 uses his secondary route, to the list of routing schemes. Routing Scheme Γ, like all routing schemes developed in Step 1, is non-dominated. The same logic is applied to the 4 remaining links to get 5 non-dominated routing schemes. From these non-dominated routing schemes, the expected payoff matrix for the terrorist can be calculated and the non-dominated links, 1-2, 1-3, 2-3, 2-4, and 3-4 are determined**.**

In Step 1, we used a link-based approach to maximize the shippers' combined path utility from an attack on a particular link. In Step 2, we focus on the shippers individually and choose for each shipper which of his available routes maximizes his path utility in the case of an attack. Since the terrorist is a destruction maximizer, he targets the non-dominated link on a shipper's selected path that possesses the greatest vulnerability. If the path does not contain a non-dominated link, the terrorist will not consider attacking any links along this path and the expected route utility is simply the utility given from completing the route. This is illustrated using OD Pair 2-4.

Columns 2 through 6 of Table 10 show the expected route utility for the shipper of OD Pair 2-4 in the case of an attack on Non-Dominated Links 1-2, 1-3, 2-3, 2-4, or 3-4. Knowing that the terrorist will attack the link on the path with the greatest expected exposure (Column 7), the expected route utility in the case of an attack on the link with the greatest exposure is calculated and shown in Column 8. For example, when

the shipper of OD pair 2-4 travels his primary route, the terrorist will attack Link 2-4 since this link has the greatest exposure (and the only link that the primary path uses). The shipper expects to receive 99%*-260.5 -1%*33,000 = -587.9 in this case. Likewise, when he travels his secondary route, the terrorist has the option of attacking Links 2-3 and 3-4. Link 3-4 has greater exposure levels (31,000 versus 22,000), and will be targeted. The shipper expects to receive 99%*-269.8 -1%*31,000 = -577.1 in this case.

Notice that this shipper's secondary route has a greater expected utility in the case of an attack than its primary route (as seen in Column 8), making the secondary route advantageous for the shipper of OD pair 2-4. Routing Scheme Λ is created where the shipper of OD Pair 2-4 take his secondary route and all other shippers use their primary route. This logic of maximizing the expected utility in the case of an attack on link with the greatest exposure is repeated for all OD pairs, creating up to an additional 3 routing schemes. There is no guarantee that these additional routing schemes will be non-dominated.

Table 10. Shipper of OD Pair 2-4 expected payoff in the case of an attack

	Shipper of OD Pair 2-4's expected utility in the case of an attack on Non-Dominated Links					**Link Targeted**	Shipper of OD Pair 2-4's expected utility in the case of an attack
	Link 1-2	**Link 1-3**	**Link 2-3**	**Link 2-4**	**Link 3-4**		
Primary Route	-260.5	-260.5	-260.5	-587.9	-260.5	Link 2-4	-587.9
Secondary Route	-269.8	-269.8	-487.1	-269.8	-577.1	Link 3-4	**-577.1**
Tertiary Route	-760.5	-610.5	-465.1	-465.1	-770.5	Link 3-4	-770.5

In Step 2, we select the path for each shipper that minimizes the route utility loss in the case of an attack, assuming the terrorist will target the most vulnerable non-dominated link on a given path. However, all players may choose to and receive benefit from varying their strategy. Therefore, in Step 3, we consider the ability of the terrorist to use mixed strategies and consider what the shippers might do in response.

Specifically, in Step 3 we determine for each of the routing schemes enumerated thus far if there is a different route that the shipper of an OD pair can take that increases the expected utility in case of an attack on any of the non-dominated links. This process is iterative – each new routing scheme that is generated is then reexamined for an attack on any of the non-dominated links. This process stops once no new routing schemes are generated.

Take Routing Scheme Λ developed in Step 2 as an example - all shippers take their primary route, except the shipper of OD Pair 2-4, who takes his secondary route. When we look at the impact on the shipper of OD Pair 1-2 from this routing scheme and a possible attack on Link 1-2, we see that he would fare better using his secondary route – see Column 2 of Table 11. Therefore, Routing Scheme Ξ is added to the list of feasible routing schemes and is identical to Routing Scheme Λ except that the shipper of OD Pair 1-2 use his secondary route. This process is continued by examining the impact on expected utility in the case of an attack on Non-Dominated Links 1-2, 1-3, 2-3, 2-4, or 3-4 for all remaining routing schemes and for all OD pairs. After Iteration 1, 4 new routing schemes are added and this process is repeated until no additional routing schemes are found. In this example, a total of 8 unique routing schemes are discovered in Steps 1 through 3.

Table 11. Shipper of OD Pair 1-2 expected utility in the case of an attack on non-dominated links

	Link 1-2	Link 1-3	Link 2-3	Link 2-4	Link 3-4
Primary Route	**-408.2**	-109.3	-109.3	-109.3	-109.3
Secondary Route	**-286.0**	-433.2	-503.2	-286.0	-286.0
Tertiary Route	-616.3	-760.1	-616.3	-940.1	-920.1

The shippers' and terrorist's expected payoff matrices are then computed. Any dominated routing schemes or link as determined from the shippers' and terrorist's payoff matrices are removed from both players payoff matrix. This results in 5 non-dominated links, Links 1-2, 1-3, 2-3, 2-4, and 3-4 and 5 non-dominated routing schemes shown in Column 3 of Tables 12 and 13. The first entry in Column 3 of these tables, (2,1,1), says that the shipper of OD Pair 1-2 uses his secondary route and shippers of OD Pairs 2-3 and 2-4, respectively, use their primary route. Three of the 5 non-dominated routing schemes, Γ Δ, and Θ, are derived in Step 1 and represent the shippers' best expected payoff in the case of an attack on each of the 5 non-dominated links. Steps 2 and 3 produce Routing Schemes Λ and Ξ, respectively. The payoff matrices, shown in Tables 12 and 13 are then used to solve equations (14) through (25).

Table 12. Shippers' Expected Payoff Matrix

		Routing Scheme Components	Link 1-2	Link 1-3	Link 2-3	Link 2-4	Link 3-4
Routing Scheme	**Γ**	**(2,1,1)**	-646.5	-793.7	-862.7	-973.9	-646.5
	Δ	**(1,1,1)**	-768.7	-469.8	-688.8	-797.2	-469.7
	Θ	**(1,2,1)**	-961.1	-812.2	-665.1	-992.5	-665.1
	Λ	**(1,1,2)**	-778.0	-479.1	-695.4	-479.1	-786.4
	Ξ	**(2,1,2)**	-655.8	-803.0	-869.3	-655.8	-963.1

Table 13. Terrorist's Expected Payoff Matrix

		Routing Scheme Components	Link 1-2	Link 1-3	Link 2-3	Link 2-4	Link 3-4
Routing Scheme	**Γ**	**(2,1,1)**	0	150	220	330	0
	Δ	**(1,1,1)**	300	0	220	330	0
	Θ	**(1,2,1)**	300	150	0	330	0
	Λ	**(1,1,2)**	300	0	220	0	310
	Ξ	**(2,1,2)**	0	150	220	0	310

The shippers' expected payoff for Routing Scheme Γ in the case of an attack on Link 2-4 is -973.9 and is calculated as follows. Routing Scheme Γ uses the following links: Link 1-3, 2-3, and 2-4. The link with the greatest exposure is Link 2-4, with an off-link population of 33,000. Therefore the expected system loss is 1% * 33,000 = 330. Only the shipper of OD pair 2-4 uses this link and is concerned with being targeted. Hence, the shippers of OD pairs 1-2 and 2-3 each contribute the utility of their selected routes, -286.0 and -100.0 respectively, and the shipper of OD pair 2-4 contributes the expected utility of a successful trip, 99% * -260.5 = -257.9 to the expected payoff calculation. The aggregation of the utilities, -257.0 + -286.0 + -100 − 330 = -973.9, creates the expected payoff to the shippers using Routing Scheme Γ in the case of an attack on Link 2-4.

REFERENCES

Bell, M. G. H., 2000. A game theory approach to measuring the performance reliability of transport networks. *Transportation Research Part B* 34(6), 533-545

Bell, M. G. H., 2003. The use of game theory to measure the vulnerability of stochastic networks. *IEEE Transactions on Reliability* 52(1), 63-68.

Bell, M. G. H., 2004. Games, heuristics, and risk averseness in vehicle routing problem. *Journal of Urban Planning and Development* 130(1), 37-41.

Bell, M. G. H., Cassir, C., 2002. Risk-averse user equilibrium traffic assignment: an application of game theory. *Transportation Research Part B* 36(8), 671-681.

Chang, T., Nozick, L. K., Turnquist, M. A., 2005. Multiobjective path finding in stochastic dynamic networks, with application to routing hazardous materials shipments. *Transportation Science* 39(3), 383-399.

Chatterjee, A., Wegmann, F. J., Fortey, N. J., Everett, J. D., 2001. Incorporating safety and security issues into urban transportation planning. *Transportation Research Record* 1777, 75-83.

Dadkar, Y., Jones, D., Nozick, L. K., 2008. Identifying geographically diverse routes for the transportation of hazardous materials. *Transportation Research Part E* 44(3), 333-349.

Dadkar, Y., Nozick, L. K., Jones, D., 2010. Optimizing facility use restrictions for the movement of hazardous materials. *Transportation Research Part B* 44(2), 267-281.

Erkut, E., Verter, V., 1998. Modeling of transport risk for hazardous materials. *Operations Research* 46(5), 625-642.

Erkut, E., Gzara, F., 2008. Solving the hazmat transport network design problem. *Computers and Operations Research* 35(7), 2234-2247.

Erkut, E., Ingolfsson, A., 2000. Catastrophe avoidance models for hazardous materials route planning. *Transportation Science* 34(2), 165-179.

Frederickson, H. G., LaPorte, T., 2002. Airport security, high reliability, and the problem of rationality. *Public Administration Review* 62(s1), 33-43.

Fundenberg, D., Tirole, J., 1995. *Game Theory*, MIT Press, Cambridge, MA.

Haimes, Y. Y., Longsta_, T., 2002. The role of risk analysis in the protection of critical infrastructures against terrorism. *Risk Analysis* 22(3), 439-444.

Hollander, Y., Prashker. J. N., 2006. The applicability of non-cooperative game theory in transport analysis. *Transportation* 33(5), 481-486.

Kreps, D. M., 1992. *Game Theory and Economic Modeling*, Oxford University Press, UK.

Kuhn, H. W., 1961. An algorithm for equilibrium points in bimatrix games. *Proceedings of the National Academy of Sciences* 47(10), 1657-1662.

Lapan, H. E., Sandler, T., 1988. To bargain or not to bargain: that is the question. *American Economic Review* 78(2), 16-20.

Lee, D.R., 1988. Free riding and paid riding in the fight against terrorism. *American Economic Review* 78(2), 22-26.

Mangasarian, O. L., Stone, H., 1964. Two-person non-zero sum games and quadratic programming. *Journal of Mathematical Analysis and Applications* 9(3), 348-355.

Nash, J. F., 1951. Non-cooperative games. *Annals of Mathematics* 54(2), 286-295.

Nembhard, D. A., 1994. Heuristic path selection in graphs with non-order preserving reward structure. Ph.D. The University of Michigan, Ann Arbor, MI.

Nielsen, L. R., Pretolani, D., Andersen K.A., 2005. *K* shortest paths in stochastic time-dependent networks [online]. Logistics/SCM Research Group Working Papers from Aarhus School of Business, Department of Business Studies.

Nozick L. K., List, G. F., Turnquist, M. A., 1997. Integrated routing and scheduling in hazardous materials transportation. *Transportation Science* 31(3), 200-215.

Sandler, T., 2003. Collective action and transnational terrorism. *The World Economy* 26(6), 779-802.

Sandler, T., Arce, D., 2003. Terrorism and game theory. *Simulation and Gaming* 34(3), 319-336.

Sandler, T., Enders,W., 2003. An economic perspective on transnational terrorism. *European Journal of Political Economy* 20(2), 301-316.

Selten, R., 1988. A simple game model of kidnappings. *Models of Strategic Rationality, Theory and Decision Library, Series C: Game Theory, Mathematical Programming and Operations Research*, Kluwer Academic Publishers, Boston, pp. 77-93.

Szeto, W.Y., Sumalee, A., 2009. A game theoretic approach to routing and scheduling hazardous materials in transport networks with multiple origin-destination pairs. Transportation Research Board Annual Meeting 2009 Paper #09-0937.

Szyliowicz, J., Viotti, P., 1997. Dilemmas of transportation security. *Transportation Quarterly* 51(2), 79-95.

US Census, 2000.

U.S. Department of Homeland Security, 2004. Threat Advisory System.

U.S. Department of Transportation, 1992. Guidelines for selecting preferred highway routes for highway route controlled quantity shipments of radioactive materials (Report RSPA-HMS-92-02). Office of Hazardous Materials Safety, Research and Special Programs Administration, Washington, D.C.

U.S. Department of Transportation, 2004. National hazardous materials registry. Federal Motor Carrier Safety Administration, Washington, D.C.

U.S. Department of Transportation, Surface Transportation Board, 2006. Carload Waybill.

von Stackelberg, H., 1934. *Marketform und Gleichgewicht*, Springer, Vienna: An English Translation, *The Theory of Market Economy*, Oxford University Press, Oxford.