PROTECTING ROAD NETWORK AGAINST INTENTIONAL ATTACKS BY NEAR-OPTIMAL INTERDICATION STRATEGY

A Thesis in
Industrial Engineering and Operation Research

by
Mengyao Gao

© 2014 Mengyao Gao

Submitted in Partial Fulfillment
of the Requirements
for the Degree of
Master of Science
August 2014
The thesis of Mengyao Gao was reviewed and approved* by the following:

Tao Yao  
Professor of Industrial Engineering  
Thesis Advisor

Venky Shankar  
Professor of Civil Engineering

Paul Griffin  
Professor of Industrial Engineering  
Peter and Angela Dal Pezzo Department Head Chair

*Signatures are on file in the Graduate School.
Abstract

In this study we investigate the vulnerability of road networks to interdictions. We consider that an intentional attacker wants to maximize the congestion level on the network by interdicting some links of the network. The behavior of the drivers traveling on the network is assumed to follow user equilibrium traffic assignment which is affected by the interdiction initiated by the attacker. In this problem, we propose a method, to reduce the damage to lowest level. An attack-to-protect (ATP for short) method is developed to solve for optimal interdiction strategies and to explore the effectiveness of protecting the identified vulnerable links of the network. Numerical experiments are conducted to examine factors that influence the effectiveness of this method. Specifically, we compare the efficiency of this method when applied on different Cartesian grids. Managerial insights into the vulnerability and protection of road networks are drawn from the analysis.
## Table of Contents

LIST OF FIGURES ........................................................................................................ VI

LIST OF TABLES ........................................................................................................ VII

ACKNOWLEDGEMENTS ......................................................................................... VIII

CHAPTER 1 INTRODUCTION .................................................................................. 1

CHAPTER 2 LITERATURE REVIEW ....................................................................... 3

2.1 CONGESTION MODEL .................................................................................... 3

2.2 INTERDICTION PROBLEM ............................................................................... 4

CHAPTER 3 MODEL DESCRIPTION ....................................................................... 7

3.1 NOTATION ........................................................................................................ 7

3.2 UE MODEL ....................................................................................................... 9

3.3 CONVEX COMBINATION ALGORITHM ........................................................ 10

CHAPTER 4 ALGORITHM DESCRIPTION .......................................................... 12

4.1 ATTACK-TO-PROTECT (ATP) METHOD ....................................................... 12

CHAPTER 5 ILLUSTRATIVE EXAMPLE .............................................................. 14

5.1 DATA DESCRIPTION ...................................................................................... 14

5.2 MEASUREMENT ............................................................................................ 16
5.3 Results ........................................................................................................................................ 16

CHAPTER 6 NUMERAL EXPERIMENTS ............................................................................. 18

6.1 External Factors ............................................................................................................ 18

6.2 Internal Factors ............................................................................................................. 21

CHAPTER 7 CONCLUSIONS ................................................................................................. 23

REFERENCES: ..................................................................................................................... 25
List of Figures

5.1A OVERVIEW OF MANHATTAN.................................................................15
5.1B STUDY AREA.........................................................................................15
5.1C SIMPLIFIED NETWORK MODEL............................................................15
6.1 SCATTERPLOT OF EFFECTIVENESS (%) VS EFFORT (%).......................22
List of Tables

3.1 NOTATION......................................................................................................................8

5.1 CRITICAL LINKS.............................................................................................................17

6.1 EXPERIMENTAL DESIGN FACTORS............................................................................19

6.2 EXPERIMENT DESIGN....................................................................................................19

6.3 ANALYSIS OF VARIANCE FOR RESPONSE (%)..............................................................20

6.4 NUMERAL RESULT OF EFFECTIVENESS SUBJECT TO PROTECTION EFFORT.........................................................................................................................21

6.5 REGRESSION ANALYSIS OF PROTECTION EFFORT AND EFFECTIVENESS.........................................................................................................................22
Acknowledgements

I want to express my gratitude first to my advisor Dr. Tao Yao. He strongly supported my research, guided me patiently and evolved me to think creatively. His insight into transportation research always enlightened me when in trouble.

Also thank the rest of my thesis committee: Dr. Shankar and Dr. Griffin, for their careful review and helpful comments.

Besides, I truly appreciate Dr. Bo Zhang’s assistance throughout the research period and advices for my study and career.

At the end of master period, I have completed my campus life. Thanks go to every person I met and every dream I had.
Chapter 1

Introduction

In recent decades, terrorists have preferred to target traffic in big cities, not only endangering human beings’ lives, but also destroying infrastructure systems such as food supply, telecommunication, economics and electric power. For example, 56 people were killed and over 700 people injured in the London bombings in 2005. In that case, the Financial Times and Stock Exchange 100 Index (FTSE 100) fell by about 200 points during the first two hours. The need for a reasonable policy to improve the security of urban transportation, raising researchers’ thinking about the vulnerability of the urban transportation networks therefore remains. Matisziw et al. [8] developed a model that was able to determine upper and lower bounds on the loss of connectivity for interdiction of arcs in the network. Murray and Mahmassani [9] gave a bi-level formulation to identify vulnerable links of a transportation network in four cases: defender has no information; defender has some information; defender and attacker interact once; and these two players interact multiple times.

Most researchers used the shortest path theory to set up their models. This model claims that if some link in a driver’s route is interdicted, the driver will select another route with
the second shortest distance or time. However, congestion effects are ignored in their assumptions. Therefore, this thesis is going to address network analysis under both intentional attack and congestion, and to develop an attack-to-protect (ATP) method to protect it. This is an innovative attempt to examine both problems of congestion and interdiction. We have also proved that our method can be applied to Cartesian grids.

Bier and Hausken [2] analyze congestion and interdiction effects on a network of two arcs. They assumed a driver would refuse to travel if the travel time exceeded their reservation time, which produces penalty time. They considered two cases with the two arcs being subjected to traffic congestion and intentional attack. One was when both arcs worked, and the other one was when one of the arcs was blocked. By comparing total travel time and penalty time in these two cases, they suggested that more effort should be assigned to the defense of less congested arcs and to routes with larger capacity. This thesis is the first attempt to apply the method successfully to more complex networks.
Chapter 2

Literature Review

In order to analyze the interdiction problem in traffic with congestion, we have to consider two points. One is how to set up the congestion model and the other one is how to reduce the loss from attacks (defined as “time added to normal driving time”). “A literature review regarding these two points follows.

2.1 Congestion model

To solve the congestion problem in a traffic network, the user-equilibrium (UE) model is commonly applied, which stems from Wardrop’s first principle, published in 1952. This assumes that the driver will choose the route from origin to destination with the shortest travel time among available routes, neglecting his or her effect on other drivers. Wardrop’s second principle [15] developed the system optimum (SO) model. This assumes that the driver’s choice aims at efficient use of the whole system such that system travel time is minimized. When the transportation network is safe, the driver will choose the routes to arrive at the destination as soon as possible. At the very beginning of attacks when the government cannot respond immediately, the driver will still decide the
route with the shortest travel time by himself or herself. Therefore, the UE model is more suitable to describe our problem.

To assign vehicle flow in the UE model, researchers have proposed various methods. Scarf [11], Todd [14] and Garcia [7] developed the fixed point method and explored its application. Pang and Chan [10] offered the generalized linear method, as well as successive linearization with Lemke’s method. Frank and Wolfe [6] first provided the convex combination method, and Florian and Nguyen [5] tried to develop it. Considering computing burden and accuracy, we selected Frank and Wolfe’s convex combination method to solve the flow assignment in this thesis. We will describe the model and algorithm in chapter 3.

2.2 Interdiction problem

There is a considerable amount of literature on interdiction problems with flow assignment in certain types of networks, such as power and security systems (provide some example citations here other than Church/Scaparra, Bier). These studies have provide us an approach to reducing system loss from attacks in terms of a) identifying the critical links in a traffic network and b) to protect them or allocate fortification resources nearby.

In the field of security, Church and Scaparra [4] applied the p-median model to select the assets whose interdictions would result in the maximum loss of the system and prevent them from attacks indefinitely. In the power system area, Bier [3] identified the transit
lines with the maximum electrical flow as the critical lines in the power system and hardened them from interdictions. In that paper, the author nested three algorithms. One is to assign the electric flow; another one is to interdict the lines with maximum flow; and the last one is to harden the interdicted lines by restoration and protection from future attacks indefinitely.

Our research is also based on this basic idea of protecting critical links. We prefer to utilize a simple and direct method to protect traffic and analyze system performance. We incorporate Bier’s method of protecting the links with maximum flow using the convex combinations technique.

In our research, we define three players–drivers, a defender and an attacker, and two simulating periods–attacking and protecting. The attacker, such as a terrorist, plans several intentional attacks simultaneously, interdicting some links of the transportation network, with the objective of maximizing system loss. The defender protects the critical links, in order to minimize the loss. The drivers in the network are assumed to know real-time information (at all times and on all available routes) and choose the route with the shortest travel time. We, from the view of the defender, set up a scenario that is simulated as an updated process of attacking and protecting. In the attacking period, we select the links with maximum flows that are identified by the convex combination method and then interdict them. In the protecting period, we restore the links that are interdicted in the attacking period and protect them from attacks indefinitely. We test, the
application range of this approach is tested by calculating its effectiveness in different traffic networks.

The rest part of this thesis is organized as follows. In Section 3, we construct the UE model and introduce the convex combination method to solve the model. We propose an ATP method in Section 4 and give a simple example of its application in Section 5. Section 6 presents two sets of numeral experiments to explore the factors that influence our method. In Section 7, we present conclusions from the thesis.
Chapter 3
Model Description

Wardrop’s first principle states: “The journey time in all routes actually used are equal and less than those which would be experienced by a single vehicle on any unused routes.” This is the original definition of the user equilibrium (UE). Under equilibrium conditions, no driver can lower their travel time by choosing an alternate route.

To solve the UE model in a large traffic network, we often construct a mathematical program with a minimization formulation and solve the program iteratively. In Section 3.1, we first introduce some preliminary notations. Then we construct the UE model in Section 3.2. In Section 3.3, we describe the solution finding convex combination algorithm.

3.1 Notation

The network can be represented by a set of nodes $\Theta$ and a set of links $\Lambda$. Let $x_{rs}$ be the travel rate of O-D pairs, compositing the origin-destination matrix. Let $q_m$ denote the flow on the link m and $t_m$ denote the travel time on the link m. For the assumption of congestion, $t_m = t(q_m)$, indicating that the travel time of the link m is related to the
flow on it. Let $\psi_{ir}^{rs}$ be the flow on route $i$. We can get the relationship that

$$x_m = \sum_r \sum_s \psi_{ir}^{rs} \delta_m^{rs}, \forall m$$

meaning that flow on each link is summed by flow of all the routes through the link. Here, $\delta_m^{rs} = 1$ if route $i$ goes through the link $m$ and $\delta_m^{rs} = 0$ if not. Table 3.1 gives the summarization.

<table>
<thead>
<tr>
<th>Table 3.1 Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbol</td>
</tr>
<tr>
<td>Θ</td>
</tr>
<tr>
<td>Λ</td>
</tr>
<tr>
<td>$q_m$</td>
</tr>
<tr>
<td>$t_m$</td>
</tr>
<tr>
<td>$\psi_{ir}^{rs}$</td>
</tr>
<tr>
<td>$\delta_m^{rs}$</td>
</tr>
</tbody>
</table>
3.2 UE Model

To obtain the link-flow pattern, UE model can be constructed as a program with a nonlinear objective function and some linear constraints. Beckmann et al. [1] gave the formulation.

$$\min z(\tilde{q}) = \sum_m \int_0^{\tilde{z}_m} t_m(\tau) d\tau$$

subject to

$$\sum_i \psi_i^{rs} = x_{rs} \quad \forall r,s$$

$$\psi_i^{rs} \geq 0 \quad \forall i,r,s$$

$$q_m = \sum_r \sum_s \sum_i \psi_i^{rs} \delta_{mjs} \quad \forall m$$

In this formulation, the objective function doesn’t have a practical interpretation. It is just a mathematical construct that can guarantee equilibrium. Constraint [3.1b] represents that the flow on all routes from the origin to destination is equal to the O-D travel rate. Constraint [3.1c] is the non-negativity constraint. Equation [3.1d], defining the flow on link m, is to collect all the flow of routes that go through the link m.

Beckmann et al. [1] also proved the equivalence of formulation [3.1] and UE assumption, as well as the uniqueness of the solution. For a detailed proof, the reader can refer to their 1956 paper.
3.3 Convex Combination Algorithm

To solve the UE model, the convex combination method transforms the original nonlinear objective function to a linear approximation one. With subsequent iterations, the optimum of the linear program gets closer and closer to the optimum of the original program. Once it satisfies the convergence condition, the optimal solution for the UE model is obtained from the transforming program.

In detail, in the n-th iteration, the direction that minimizes $z(q^r)$ is $p - q^r$. The slope of $z(q^r)$ in this direction is

$$
-\nabla z(q^r) \cdot \frac{(p - q^r)^T}{\|p - q^r\|} \quad [3.2]
$$

Here $\tilde{y}$ is an auxiliary feasible direction in the entire feasible region. For a certain $\tilde{y}$, the objective function can be changed to a linear approximation.

$$
z^n(p) = z(q^n) - \left[ -\nabla z(q^n) \cdot \frac{(p - q^n)^T}{\|p - q^n\|} \right] \|p - q^n\| = z(q^n) + \nabla z(q^n) \cdot (p - q^n) \quad [3.3]
$$

Therefore, in the n-th iteration, the approximation linear program is presented as,

$$
\min z^n(p) = z(q^n) + \nabla z(q^n) \cdot (p - q^n) \quad [3.4]
$$

subject to

$$
\sum_{i} y_i^{rs} = x_{rs} \quad \forall r, s \quad [3.5]
$$

$$
y_i^{rs} \geq 0 \quad \forall i, r, s \quad [3.6]
$$
After the direction $\overline{p} - \overline{q}^n$ is known, the flow assignment for the next iteration is easy to get.

$$\overline{q}^{n+1} = \overline{q}^n + \alpha(\overline{p} - \overline{q}^n)$$ \[3.7\]

$\alpha$ is the step size, which can be calculated from the following formula.

$$\frac{\partial}{\partial \alpha} z \left[ \overline{q}^n + \alpha(\overline{p} - \overline{q}^n) \right] = 0$$ \[3.8\]

To conclude, the Convex Combination Algorithm can be stated as follows:

Step 0: Initialization. Load flow $\overline{q}^1$ to the empty network according to $t_m^1 = t(0), \forall m$. Set $n = 1$.

Step 1: Direction searching. Load flow $\overline{p}$ to the empty network according to $t_m^n = t(\overline{q}^n), \forall m$.

Step 2: $\alpha$ calculation. Find $\alpha_n$ by solving equation below.

$$\frac{\partial}{\partial \alpha} z \left[ \overline{q}^n + \alpha(\overline{p} - \overline{q}^n) \right] = 0$$

Step 3: Move. Move flow to $\overline{q}^{n+1} = \overline{q}^n + \alpha(\overline{p} - \overline{q}^n)$

Step 4: Convergence. If the stopping criteria is satisfied (using flow tolerances for example), output $\overline{q}^{n+1}$; otherwise, set $n \leftarrow n + 1$ and go to step 1.
Chapter 4
Algorithm Description

4.1 Attack-to-Protect (ATP) Method

In order to improve the road network against congestion and attacks, our task consists of two critical problems to be solved. The first problem is to determine UE flows. The second problem is to protect the network via an attack-to-protect method (ATP method) by defining the links transporting the largest vehicle flow as the most vulnerable and critical links, and protecting them from being compromised indefinitely.

The ATP method and convex combination method are nested for use: the convex combination algorithm optimizes the traffic flow; ATP method interdicts the unprotected links with maximum flows by deleting them from the original network; after a “vulnerable” links are identified in continuously updated networks, we restore these deleted links back to the network and harden them against attacks.

The specific steps are listed below.

Step 0-1: Initialization. Set $j = 0$ and $\Omega = [ ]$. 
Step 0-2: Initialization. Set \( l = 0 \) and \( K = [ ] \).

Step 1: Attacks Scenario. Run Convex Combination method to assign UE flows. Select the arc(s) of maximum flow and remove from the network. If there is more than one such arc, select randomly. If it is an element in \( \Omega \), select the “next maximum” arc to attack. This selected arc is added into \( K \).

Step 2: Set \( l = l + 1 \) and go back to step 1, until \( l = a \). (\( a \) is a predetermined number of arcs to be added to set \( \Omega \) per time).

Step 3: Add \( K \) into \( \Omega \).

Step 4: Set \( j = j + 1 \) and return to step 0-2, until \( j = b \). (\( b \) is a set number of maximum iterations.)
Chapter 5

Illustrative Example

5.1 Data description

We apply our method to the Manhattan road network (shown in Figure 5.1a) which is a Cartesian grid network. We focus on with a subset of this network with 10 Avenues and 10 Streets around Times Square, as displayed in Figure 5.1b. We note every node in consecutive number in figure 5.1c. For simplification, we assume that all nodes are identically spaced at 0.1 mile. Link travel speed is assumed to be 20 mile/hour when no congestion exists. We assume that relationship between the travel time and flow is quadratic as the format of \( t = b + cx^2 \). When \( x=0 \), the travel time is the intercept which is 0.1 mile divided by 20 mile/hour, equal to 18 seconds per block. The coefficient of second-order is assumed to 0.05 and that of first-order is assumed to 0. So the congestion function is \( t_m = 18 + 0.05x_m^2 \). A future point of research can be to test actual BPR functions where the relationship between travel time and link flow is nonlinear as well but defined by two parameters alpha and beta, which are related to the capacity of the link and the speed limit on the link.
Since Times Square is the center of this network, we set a small square (5X5) matrix as the center area. We consider the combination of an origin and a destination as an O-D pair. An existing O-D pair means that a driver travels from this origin to this destination. As O-D pairs consist of traffic flow, the traffic flow in this paper is referring to the number of O-D pairs in the traffic. For example, 100 traffic flows here indicate there are 100 O-D pairs in the traffic. This will make the density of the traffic easily measured.

Another assumption is that all the streets are one-direction.

Figure 5.1a Overview of Manhattan

Figure 5.1b Study Area

Figure 5.1c Simplified Network Model
5.2 Measurement

This new approach is expected to protect some important streets so as to reduce the impact of attacks. Based on this goal, performance of this method can be measured as the improvement proportion of system cost comparing to the system cost of the unprotected network.

\[
\text{improvement} = - \frac{(c_2 - c_0) - (c_1 - c_0)}{c_1 - c_0} \tag{5.1}
\]

Here, \( c_0 \) is the system cost of the original network without attacks. \( c_1 \) is the system cost of the original network encountering random attacks. \( c_2 \) is the system cost of network in which important streets have been protected from attacks encountering random attacks.

5.3 Result

MATLAB 2012b was used to run experiments. With input data being network links information and O-D pairs. Network is programmed by a matrix consisted of value 0 and value 1. Value 1 means the link from node of row index to node of column index is connected; value 0 means disconnection. O-D pairs are stored in an n×2 matrix whose first column lists origins and second column destinations. The experiment is implemented on an Intel Xeon 3.06 GHz processor.
There are total 162 streets in this network. Based on reality, we cannot protect too many streets from attacks. Hence, we set 4 iterations for our method and in every iteration, four links with maximum flow are interdicted sequentially so that we determine 16 streets as the important streets, around 10% of the network. Computation time on the LionXC system was roughly 10 hours. The resulting list of critical links is provided in Table 5.1.

**Table 5.1 Critical Links**

<table>
<thead>
<tr>
<th>Link number</th>
<th>Link (node, node)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(34,35)</td>
</tr>
<tr>
<td>2</td>
<td>(54,55)</td>
</tr>
<tr>
<td>3</td>
<td>(14,15)</td>
</tr>
<tr>
<td>4</td>
<td>(56,66)</td>
</tr>
<tr>
<td>5</td>
<td>(56,57)</td>
</tr>
<tr>
<td>6</td>
<td>(36,37)</td>
</tr>
<tr>
<td>7</td>
<td>(16,17)</td>
</tr>
<tr>
<td>8</td>
<td>(68,78)</td>
</tr>
<tr>
<td>9</td>
<td>(45,46)</td>
</tr>
<tr>
<td>10</td>
<td>(35,45)</td>
</tr>
<tr>
<td>11</td>
<td>(65,66)</td>
</tr>
<tr>
<td>12</td>
<td>(26,36)</td>
</tr>
<tr>
<td>13</td>
<td>(45,55)</td>
</tr>
<tr>
<td>14</td>
<td>(43,53)</td>
</tr>
<tr>
<td>15</td>
<td>(47,57)</td>
</tr>
<tr>
<td>16</td>
<td>(41,51)</td>
</tr>
</tbody>
</table>

With random selection of links under attack, we run 100 replications and get the average improvement to be 13.0855%. This indicates that if we protect the critical links listed in the table 5.1, we can get a 13% improvement in system performance compared to the unprotected network.
Chapter 6

Numeral Experiment

The effectiveness of our approach is influenced by external factors and internal factors. External factors relate to the road network and include the size of the network, the vehicle flow (the number of O-D pairs), the number of activity centers, and directional flow characteristics of streets. Internal factors involve robustness of hardening. The following two sections will illustrate the two aspects in detail.

6.1 External Factors

By changing these four factors, network performance may differ under protection. In order to figure out what factors affect protection performance significantly, we design a $2^{4.1}$ fractional factorial experiment and studied a set of 8 urban traffic models which are based on the example in Chapter 5. Every node except the boundary node is linked with other four nodes in the same distance.

The input data of the four factors are controlled to two levels that are listed below.
Table 6.1 Experimental Design Factors

<table>
<thead>
<tr>
<th>Codes</th>
<th>Factor</th>
<th>Level</th>
<th>Data</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Size</td>
<td>1</td>
<td>10*10 nodes</td>
<td>Small township</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>20*20 nodes</td>
<td>Manhattan Core</td>
</tr>
<tr>
<td>B</td>
<td>Flow</td>
<td>1</td>
<td>100</td>
<td>Non-peak hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>200</td>
<td>Peak hour</td>
</tr>
<tr>
<td>C</td>
<td>Center</td>
<td>1</td>
<td>1</td>
<td>Single activity center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td>Multiple activity centers</td>
</tr>
<tr>
<td>D</td>
<td>Direction</td>
<td>1</td>
<td>1-direction</td>
<td>One-direction street</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>2-direction</td>
<td>Two-direction street</td>
</tr>
</tbody>
</table>

For convenience, level 2 data are coded as +, and level 1 data are coded as -. In this way, the construction of two-level fractional factorial design is shown in the following Table 6.2. This experiment would provide sufficient data to explain the main effects and two-factor interactions between the four factors.

Table 6.2 Experiment Design

<table>
<thead>
<tr>
<th>run</th>
<th>Size</th>
<th>Flow</th>
<th>Center</th>
<th>Direction</th>
<th>Response(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>13.0855</td>
</tr>
<tr>
<td>2</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>2.2755</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>22.3205</td>
</tr>
<tr>
<td>4</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>6.8237</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>11.7621</td>
</tr>
<tr>
<td>6</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>4.3218</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>22.8796</td>
</tr>
<tr>
<td>8</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>4.6801</td>
</tr>
</tbody>
</table>
Table 6.3 summarizes the analysis of variance for this experiment. Among these four factors, network size is a significant factor that influences network performance with our algorithm since the p-value is less than 5% (confidence level). The p-value of “activity center” and “direction of streets” are much larger than 5%, which means that these factors we investigate don’t affect network performance with our algorithm significantly. For the factor of “traffic flow”, its p-value is near 0.05, which means that this factor is near-significant.

Table 6.3 Analysis of Variance for response(%)  

<table>
<thead>
<tr>
<th>Source</th>
<th>DF</th>
<th>Seq SS</th>
<th>MS</th>
<th>F</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Effects</td>
<td>4</td>
<td>430.666</td>
<td>107.666</td>
<td>12.12</td>
<td>0.034</td>
</tr>
<tr>
<td>Size</td>
<td>1</td>
<td>350.418</td>
<td>350.418</td>
<td>39.45</td>
<td><strong>0.008</strong></td>
</tr>
<tr>
<td>Traffic Flow</td>
<td>1</td>
<td>73.562</td>
<td>73.562</td>
<td>8.28</td>
<td>0.064</td>
</tr>
<tr>
<td>Activity Center</td>
<td>1</td>
<td>0.433</td>
<td>0.433</td>
<td>0.05</td>
<td>0.839</td>
</tr>
<tr>
<td>Direction of streets</td>
<td>1</td>
<td>6.252</td>
<td>6.252</td>
<td>0.70</td>
<td>0.463</td>
</tr>
<tr>
<td>Residual Error</td>
<td>3</td>
<td>26.647</td>
<td>8.882</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>457.313</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.2 Internal Factor

For the algorithm itself, the effort to protecting network is the internal factor that impacts its performance. It is obvious that the larger the number of streets to be protected, the higher the cost for government. Therefore, it is a trade-off between budget and security.
We randomly pick the third network designed in Section 6.1 as our study scenario. We incrementally increase the protected link count, and observe the effectiveness of the ATP method as listed in Table 6.4.

<table>
<thead>
<tr>
<th>Number of lines protected</th>
<th>Proportion of protected lines</th>
<th>Effectiveness (%)</th>
<th>Response/proportion of protected lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4.94</td>
<td>12.74</td>
<td>2.57985</td>
</tr>
<tr>
<td>16</td>
<td>9.88</td>
<td>22.32</td>
<td>2.2599</td>
</tr>
<tr>
<td>24</td>
<td>14.81</td>
<td>34.07</td>
<td>2.299725</td>
</tr>
<tr>
<td>32</td>
<td>19.75</td>
<td>45.7</td>
<td>2.3135625</td>
</tr>
<tr>
<td>40</td>
<td>24.69</td>
<td>56.39</td>
<td>2.283795</td>
</tr>
</tbody>
</table>

*Proportion of protected links is calculated as the number of links divided by the total links (162) in the network

Table 6.5 presents the results of the simple regression analysis which assumes a linear relationship between performance and degree of protection. The scatterplot in the Figure 6.1 gives us an apparent impression of their relationship.

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Coefficient</th>
<th>SE Coef</th>
<th>T</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>1.0334</td>
<td>0.6967</td>
<td>1.48</td>
<td>0.235</td>
</tr>
<tr>
<td>Protection effort (%)</td>
<td>2.24184</td>
<td>0.04254</td>
<td>52.70</td>
<td>0.000</td>
</tr>
</tbody>
</table>

The regression equation is \( \text{effectiveness} (%) = 1.03 + 2.24 \times \text{protection effort} (%) \)

\( S=0.664147 \quad \text{R-Sq}=99.9\% \quad \text{R-Sq(adj)}=99.9\% \)
Figure 6.1 Scatterplot of effectiveness(%) vs effort(%)

With the linear relationship, the government has to decide their acceptable risk and available budget, and then derive the optimal decisions for this multiple criteria decision problem.
Chapter 7

Conclusions

This thesis addresses congestion and interdiction together in a non-trivial network, and demonstrates a practical application of an algorithm to evaluate network performance.

We develop a simple network travel time performance measure using an ATP approach that nests the method of convex combinations with link hardening.

To analyze the influencing factors of the approach, we design a $2^{4-1}$ fractional factorial experiment involving two-level definitions of network size, traffic flow, activity centers and street directional constraints. Our finding is that network size is significantly associated with network performance, while traffic flow effects are near-significant. We then evaluate the sensitivity of network performance to the degree of network protection by incrementally increasing the number of protected links. We find that the network performance effectiveness and the number of protected links are potentially linearly related. From a policy standpoint, this implies that trade-offs between protection cost and performance vulnerability of the transportation network can be considered in a simplified manner through the identification of critical links alone. The potential for our ATP
approach lies in the increased efficiency. Not accounting for fixed costs of protection, the network performance levels improve by up to 100% based on our analysis.

Further research may consider the congestion and interdiction in a dynamic way. For example, after the government responds to the attack, how could it regulate traffic flow on the network by using demand-responsive traffic signals or police to reduce the total loss. Capacity and traffic flow effects are also factors which have been assumed to be ignorable in our analysis. Further, the analysis of demand variation under attack is an issue for consideration.
References:


equilibria.


