A Game Theory Approach for the Measurement of Transport Network Vulnerability from the System Perspective

Wenxin Qiao\textsuperscript{a,*}, Yang Lu\textsuperscript{b}, Chenfeng Xiong\textsuperscript{c} and Ali Haghani\textsuperscript{d}

\textsuperscript{a} MOE Key Laboratory for Urban Transportation Complex Systems Theory and Technology, School of Traffic and Transportation, Beijing Jiaotong University, Beijing, China
\textsuperscript{b} Singapore-MIT Alliance for Research and Technology (SMART), Singapore
\textsuperscript{c} Department of Civil and Environmental Engineering, University of Maryland, College Park, U.S.A.

ABSTRACT

Measuring the transport network vulnerability has become an important research issue recently. With the increase on the road user’s value of time, users are now not only concerned about taking the shortest route to save travel times, but also decrease the variances by choosing a route that is more reliable to arrive at the destination within acceptable time frame. Ensuring a reliable network and providing alternative options under network breakdowns are very important to reduce the network vulnerability. This paper proposed a computationally efficient approach to measure system-level network vulnerability through a game theory approach. The most vulnerable link is indicated by link failure probabilities and the overall vulnerability measure of the network is represented by the expected total travel time. The performances are compared and discussed through the numerical results from several reliability improvement strategies.

Key words: game theory, vulnerability, network, system perspective

Introduction

Network reliability refers to the ability of the network to maintain an acceptable level of performance when network failure occurs. Improving the transport network reliability has been an extensively studied research problem. Great efforts had been involved to identify and measure the performance reliability of the transport network in the purpose of construct and maintain a robust, reliable network for the benefits of road users. With the rapid economic growth, the value of time of the trip makers has raised significantly. Road users are not only concerned about taking the shortest route to save the travel times, but also choosing a route that is more reliable to arrive at the destination within acceptable time frame. Ensuring a reliable network and providing alternative options under network breakdowns and disruptions are very important issues now.

As road users are trying to save travel time and decrease the variability at the same time, the sources of the variances need to be identified first. Variances or uncertainties in the network may come from both demand and supply sides (Lam et al. 2008). The variances in supply side may come from various network disturbances such as accident, road work or adverse weather that result in capacity reduction. For the demand side, the variances may come from the variations in day-to-day travel demand or special events.

Many networks are designed to offer alternative routes considering the risk of single or several components failures. Methodologies to identify the most vulnerable links, whose failure would cause the most damage to the network performance, would be very useful. The

*Corresponding Author. Email: wxqiao@bjtu.edu.cn
network is robust if the links with a large potential impact on the network have low probability of failure.

Game theory was introduced to provide mathematical background for the analysis of interactive processes for decision making (Neumann and Morgenstern, 1944). Applications of game theory to transportation systems have addressed a variety of problems including: network design, pricing and reliability evaluation, competition between transport modes, dynamic traffic assignment on urban networks and so on. Two main applications are: application to the traffic user equilibrium problems and application to reliability problems.

The user equilibrium problem can be defined as determining the traffic flow on every link of network. Wardrop (1952) was the first person to provide a theoretical framework for formulating this problem. Later on, research indicated that his principles resembled a Nash Equilibrium and the Game Theory gave transportation researchers a new way of looking at the traffic user equilibrium problem (Boyce et al. 2005).

This research will focus on a two-player non-cooperative zero sum game between the network user seeking a path to minimize the expected trip cost and a demon choosing link performance scenarios to maximize the expected trip cost. A minmax optimization model is proposed to evaluate the network vulnerability through game theory approach. Numerical example is provided for discussions on possible approaches to reduce the network vulnerability.

**Literature Review**

The network reliability problems have been studied over the decades and the research work can be summarized in two folds (Bell, 2000): the network connectivity and performance reliability. Earlier work on reliability problems had focused on the connectivity issues when network becomes disconnected from link failure that one cannot reach his destination (Iida and Wakabayashi, 1989; Du and Nicholson, 1997). On the other hand, a connected network may not always provide sufficient road capacity or service level to ensure the users to arrive their destination on time, which leads to the discussion of the network performance reliability. One approach to study network performance reliability is to first gather the link performance statistical distributions; then study the impact of link performance variation on network performance (Bell et al., 1999). However, there are limitations in insufficient data and the stability issues for this approach.

Other than connectivity and capacity measures, as in Bell’s paper (Bell, 2003), an alternative method is proposed that seeks to identify the links whose failure would impair the network performance the most, which is to measure the vulnerability of networks. Also, Berdica (2002) discussed various other definition of network vulnerability. More recently, Igor et al. (2010) measured the vulnerability of complex networks with different topologies through game theoretic approach and indicated the vulnerability heavily depends on topology. Chen et al. (2012) discussed a network vulnerability index called “impact area” vulnerability which is obtained by evaluating the consequence of each link closure on the overall network performance within a reasonable “sub network” defined as impact area. Szeto and Sumalee (2009) used a game theoretical model to identify routing and scheduling decisions for multiple hazmat carriers through a zero sum game. While the majority of traditional definitions of network vulnerability were based on topology, connectivity, or capacity, this paper defined vulnerability alternatively as the system-level total travel cost at the optimum
state, following Bell’s measurement of vulnerability (Bell 2003). Compared to other measures, this measure can be more conveniently calculated. When the model is potentially applied to any network models, the implementation of the proposed approach is of less computational burden. It is worth noting that the link failure probabilities are used to indicate the most critical links for the network performance in order for the decision-makers to determine strategies accordingly and achieve more reliable system-level outcome.

The network reliability is a research topic drawing increasing concern from transportation communities. The definition of network reliability or network vulnerability also varies among different studies. Broadly speaking, network reliability definitions from previous studies can be grouped into the following three categories:

(1) Network connectivity reliability. The connectivity reliability defines the reliability of a transportation network to be the probability of connectivity between different O-D pairs to remain intact given particular links is disrupted (Wakabayashi and Iida, 1992). The main problem with connectivity definition is that the method does not consider the capacity and travel time of different links.

(2) Capacity reliability. The capacity reliability takes into the account of link capacities within the network and defines the network reliability as the probability of the transportation network accommodates a certain level of demand with acceptable level of service quality. Relevant works include Chen et al., 2002.

(3) Travel time reliability. Under the travel time reliability concept, the network reliability is measured by the expected travel time between O-D pair considering the possibility of link capacity drop. Also the concept of travel time can be further generalized into travel cost which considers the monetary cost of the transportation. Therefore this group of study can be also named as travel cost reliability. Since travel time or travel cost is the most popular measurement of network service quality, the travel cost reliability received high degree of interests among researchers and practitioners.

Based on how the disturbance probability of each link is computed, travel time reliability studies can be further categorized into two branches. The first group intends to investigate the adverse impact of rare incidents on the network performance. Rare incidents include traffic accidents, traffic flow breakdown, harsh weather, etc. These incidents happen at low probability but can potentially cast huge negative impact to the network. For example, Dalziell and Nicholson (2001) developed link failure duration probability distributions for hazards using Monte Carlo simulation method. Regarding this group of models, link failure probabilities are required inputs which are difficult to obtain unless there is a comprehensive historical incident database.

The second branch along this direction is the game theory approach. Different from other approaches, game theoretical formulation of network reliability, which is first introduced by Bell (2000), is based on concept of depicting the expected network condition as the outcome of a game between two players: network users and hypothetical demon (or network tester). The hypothetical demon, which is also called network tester, seeks to maximize the total network travel cost by adjusting the disturbance probability of each link; on the other hand, users makes their own route choice usually in a non-cooperative way to minimize their respective travel time. Bell (2000) first formulated the problem considering one driver and one demon. In his study, the travel time of the disrupted link becomes ten times longer
compared with its usual travel time. Following the same path, Bell and Cassir (2002) enhance the model to include multiple drivers and demons. Since the demon is allowed to degrade any link, the game theory model provides “pessimistic” estimation of network travel cost. Therefore the outcome of the model describes the vulnerability of transportation network. Bell (2003, 2006, 2008) presented a series of research revolving this topic and named the model as “attacker-defender” model. Relevant studies along this direction also include Szeto et al. (2006, 2007), Szeto and Sumalee (2009) and Szeto (2011, 2013). The game between the network tester and drivers in this type of model is often transformed into a bi-level optimization problem in which the upper level is controlled by the hypothetical demon who attempts to maximize the expected total network travel cost while the lower level is controlled by the network users who want to minimize their own travel costs. And based on the definition of players, the game theory formulation may vary between different studies. For interested readers, there are also more comprehensive introduction of game theory method, for example Cassir and Bell (2001). Hollander and Prashker (2006) conducted an extensive literature review on the applicability of non-cooperative game theory in transport analysis.

Due to the complex nature of bi-level optimization formulation, effective solution algorithms need to be developed. A solution method which iterates between upper and lower level problem was proposed by Yang (1995) in order to solve the bi-level O-D flow estimation problem considering user equilibrium assignment. Bell and Cassir (2002) proposed a risk averse equilibrium assignment algorithm based on MSA (Method of Successive Average). Also similar approach was also adopted in Bell (2003) and Bell and Kanturska (2008). Also based on game theoretical modelling approach, several studies were reported on optimal design of the transportation network from reliability point of view, such as Chen et al (2007) and Bianco et al. (2009).

In this study, we developed a new game theoretical formulation for network vulnerability from a system perspective, thus in order to minimize the adverse impact from the demon, a network dispatcher is assumed to adjust the link flows according to the strategy of the hypothetical network disrupter. A zero sum game between these two entities is formulated in this study. Compared with previous studies, drivers no longer make their route choice only considering their own utility but rather controlled by the network dispatcher. Such kind of system optimal assignment is adopted to counter the link disturbances from the network tester. Then the system vulnerability is estimated by computing the expected total travel time of network users. Also in this study, the travel time of each link is modelled as non-linear function of link flow (BPR function) to better measure the impact of traffic volume on the vulnerability of the network. The sensitivity of link capacity and traffic volume is investigated using the proposed game theory formulation. A heuristic solution algorithm is also proposed based on MSA principle. Finally the application of the proposed model is presented and discussed using numerical examples.

**Problem Statement and Solution Methodology**

In this paper, a game theoretical model is used to estimate the network vulnerability. The game theoretical model is formulated as a minmax problem following the original “attacker-defender” model proposed by Bell (2000, 2002, 2003, 2006 and 2008). The network vulnerability is considered as an equilibrium outcome of a two player non cooperative zero sum game: the first player is a network coordinator who tries to minimize the total cost of the
network by controlling the flow assignment on each link subject to OD flow constraints; the other player is a hypothetical demon who attempts to maximize the total network cost by disrupting a particular link of the network. In the remaining part of this paper, these two players are referred as network coordinator and network tester respectively. In this study, we emphasize on predicting the network vulnerability using the equilibrium outcome of above two-player zero sum game considering the non-linear relationship between demand flow volume and travel time. In this study, the correlation between link flow \( x \) and link travel time \( t \) is modeled by the following BPR function form,

\[
t(x) = t_f \left(1 + \alpha \left(\frac{x}{c}\right)^\beta\right)
\]

\( t_f \) and \( c \) are respectively free flow travel time and link capacity; \( \alpha \) and \( \beta \) are shape parameters of the function.

Consider a general transport network represented by a directed graph \( <M, N> \) where \( M \) and \( N \) are node and link set, the notations used in this paper are given as follows: 

- \( x_i \) the traffic flow on link \( i \);
- \( y_j \) probability of link \( j \) to be disturbed by the network tester;
- \( X \) is the link flow volume vector determined by the network dispatcher;
- \( Y \) is the link disturbance probability vector determined by the demon or network tester;
- \( t_{ij}(x_i) \): the travel time of link \( i \) under the scenario when link \( j \) is disrupted. \( t_{ij} \) is a function of both link flow \( x_i \) and disturbance strategy of the demon. Since a link is either disturbed or not disturbed, therefore \( t_{ij} \) takes the following form:

\[
t_{ij}(x_i) = f_{ij} \left(1 + \alpha \left(\frac{x_i}{c_{ij}}\right)^\beta\right)
\]

where \( f_{ij} \) is the free flow travel time of link \( i \) in scenario \( j \), \( c_{ij} \) is the capacity of link \( i \) in scenario \( j \) and \( \alpha \) and \( \beta \) are parameters;

- \( d_m \): the demand generation or absorption of node \( m \);
- \( \delta_{im} \): Node-link incidence matrix defined by the following expression,

\[
\delta_{im} = \begin{cases} 
1 & \text{if link } i \text{ is the incoming link of node } m \\
-1 & \text{if link } i \text{ is the outgoing link of node } m \\
0 & \text{if link } i \text{ is not connected with node } m
\end{cases}
\]

In this study, the status of each link is either disturbed or not disturbed. When the link is not disturbed, it remains its original capacity \( c_i \); otherwise when the link is disrupted, its capacity will be reduced to a significantly lower level \( \gamma c_i \) where \( \gamma \) is a fraction between zero and one. Therefore when a particular link is disturbed, the travel time of all paths using the link will increase depending on the volume passing the link. Therefore the two player zero sum game is formulated as a minmax problem presented in P1, the network coordinator tries to minimize the total network flow cost by adjusting \( x_i, i = 1, 2, ..., N \); on the other hand, the network tester aims at maximizing the total network flow cost by changing \( y_j, j = 1, 2, ..., N \); Note that we assume only one link is degraded by the demon under one scenario. Due to the property of zero-sum game, the payoff of the network coordinator and the demon sums up to zero, namely the game is a zero sum game.

\[
p_c = \sum_i \sum_j x_i t_{ij}(x_i)y_j
\]
Where \( p_c \) and \( p_d \) are the expected payoff of network coordinator and tester respectively. Given above notations, this two-player zero sum game can be formulated into the following minmax problem (P1).

\[
\begin{align*}
\text{P1:} & \quad \min_{x_i,y_j} \max_{x_i,y_j} \sum_{i=1}^{N} \sum_{j=1}^{N} x_i t_{ij} (x_i) y_j \\
\text{s.t.} & \quad \sum_{j=1}^{N} y_j = 1 \\
& \quad \sum_{i=1}^{N} x_i \delta_{ik} + d_k = 0, k = 1,2,...,M \\
& \quad x_i \geq 0, y_j \geq 0
\end{align*}
\]

Above minmax problem can then be transformed into the following bi-level optimization problem (P2):

\[
\begin{align*}
\text{P2:} & \quad \max_{y_j} \sum_{i=1}^{N} \sum_{j=1}^{N} x_i t_{ij} (x_i) y_j \\
\text{s.t.} & \quad \sum_{j=1}^{N} y_j = 1, y_j \geq 0
\end{align*}
\]

Lower level:

\[
\begin{align*}
\min_{x_i} \sum_{i=1}^{N} \sum_{j=1}^{N} x_i t_{ij} (x_i) y_j \\
\text{s.t.} & \quad \sum_{i=1}^{N} x_i \delta_{ik} + d_k = 0, k = 1,2,...,M \\
& \quad x_i \geq 0
\end{align*}
\]

In the upper level of P2, given fixed link flows \( x_i \), the network tester attempts to maximize the expected total network travel time by adjusting link disturbance probabilities \( Y \); on the lower level, the network dispatcher performs a system optimal assignment given link disturbance probabilities given by the upper level problem. The existence of the solution of problem P2 is proved by Proposition 1. For each set of given link disturbance probabilities, the lower level optimization problem is proved to be a non-linear minimization problem with
convex objective function and convex constraints under certain assumption of the shape of link cost functions.

Proposition 1: If all link cost functions are continuous and differentiable functions that satisfy condition (15), then for each set of link disturbance probabilities \( y_j, j=1,2,\ldots, N \), the lower level optimization problem of P2 is a convex optimization problem with unique solution:

\[
\frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i^2 + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} > 0 \quad \forall i, j
\]  

(15)

**Proof**

The Hessian matrix of objective function of lower level is computed as follows,

\[
\frac{\partial}{\partial x_m} \sum_{i=1}^{N} \sum_{j=1}^{N} x_i t_{ij}(x_i) y_j = \left\{ \sum_{j=1}^{N} \left[ \frac{\partial t_{mj}(x_m)}{\partial x_m^2} x_m + 2 \frac{\partial t_{mj}(x_m)}{\partial x_m} \right] y_j, \text{if } m = r \right. \\
\left. 0 \quad \text{o. w.} \right\}
\]

(16)

\[
\begin{bmatrix}
\sum_{j=1}^{N} \frac{\partial t_{1j}(x_1)}{\partial x_1^2} x_1 & 2 \frac{\partial t_{1j}(x_1)}{\partial x_1} y_j & \cdots & 0 \\
& \ddots & \ddots & \ddots \\
& & \ddots & \ddots & \ddots \\
0 & \cdots & \sum_{j=1}^{N} \frac{\partial t_{nj}(x_n)}{\partial x_n^2} x_n & 2 \frac{\partial t_{nj}(x_n)}{\partial x_n} y_j & \cdots \\
\end{bmatrix}
\]

(17)

Hence the determinant of Hessian matrix is given by Eq. (18)

\[
\text{Det}(\nabla^2) = \prod_{i=1}^{N} \prod_{j=1}^{N} \left[ \frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} \right] y_j
\]

(18)

We will show that if the link cost function takes the form of BPR function, then the above determinant is strictly larger than zero. Since

\[
\frac{\partial t_{ij}(x_i)}{\partial x_i} = \frac{\alpha \beta}{c_{ij}} \left( \frac{x_i}{c_{ij}} \right)^{\beta-1}, \quad \frac{\partial^2 t_{ij}(x_i)}{\partial x_i^2} = \frac{\alpha \beta (\beta - 1)}{c_{ij}^2} \left( \frac{x_i}{c_{ij}} \right)^{\beta-2}
\]

(19)

Then

\[
\frac{\partial^2 t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial^2 t_{ij}(x_i)}{\partial x_i} = \frac{\alpha \beta (\beta - 1)}{c_{ij}^2} \left( \frac{x_i}{c_{ij}} \right)^{\beta-1} x_i + 2 \frac{\alpha \beta}{c_{ij}} \left( \frac{x_i}{c_{ij}} \right)^{\beta-1}
\]

(20)
Because $\alpha, \beta$ and $c_{ij} > 0$, the value of $\frac{\alpha \beta (\beta + 1)}{c_{kl}} \left( \frac{x_k}{c_k} \right)^{\beta - 1}$ is strictly larger than zero for any link $i$. Therefore,

$$\sum_{j=1}^{N} \left[ \frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} \right] y_j > 0, i = 1, 2, ..., N \to \prod_{i=1}^{N} \sum_{j=1}^{N} \left[ \frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} \right] y_j \quad (21)$$

$$> 0$$

More generally,

$$\frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} > 0 \text{ for all } i \text{ and } j \to \prod_{i=1}^{N} \sum_{j=1}^{N} \left[ \frac{\partial t_{ij}(x_i)}{\partial x_i^2} x_i + 2 \frac{\partial t_{ij}(x_i)}{\partial x_i} \right] y_j \quad (22)$$

$$> 0$$

Therefore, if the link cost functions of the network satisfies condition (15), then the lower optimization problem of P2 is a minimization problem with convex objective function and convex constraints. A unique global solution exists. Essentially, the lower level of P2 is a system optimal traffic assignment given modified link capacities given by link disturbance probabilities from the network tester. Therefore there exists a single set of optimal link flows which minimize the total network travel time. Such property of the model allows us to construct a heuristic algorithm which is discussed in the next section.

Solution Algorithm

The solution method developed in this section resembles to the iterative solution method proposed by Yang (1995). The basic idea is to iterate between upper and lower level problem until the stopping criteria is met. Let $X^{(k)}$ and $Y^{(k)}, k = 1, 2, ..., K$ be the estimated link flow and disturbance probability vector after $k$th iteration. And $\tilde{X}^{(k)}$ and $\tilde{Y}^{(k)}$ are the auxiliary link flows and disturbance probability vector at iteration $k$. The solution procedure is summarized here.

1) Step 1, initialization: Let $y_1^{(0)} = y_2^{(0)} = ... = y_N^{(0)} = \frac{1}{N}$, then solve $X^{(0)}$ using system optimal assignment method given $Y^{(0)}$.

2) Step 2, determine the auxiliary link disturbance probability $\tilde{Y}^{(k)}$: based on link volumes from previous iteration, $X^{(k-1)}$, determine the optimal disturbing strategy of the network tester by finding the scenario with highest marginal increase of expected network travel time. Thus, find $j$ which maximize the following expression,

$$\max_j \sum_{i=1}^{N} x_i t_{ij}(x_i)$$

And auxiliary link disturbance probability vector $\tilde{Y}^{(k)}$ is a vector whose $j$th element is one while all remaining elements are zero.

3) Step 3, update $Y^{(k)}$ using moving successive average (MSA) method,

$$Y^{(k)} = Y^{(k-1)} + \frac{1}{k} [\tilde{Y}^{(k)} - Y^{(k-1)}]$$

4) Step 4, update link flows. Given $Y^{(k)}$, the network dispatcher solve for a set of new auxiliary link flows $\tilde{X}^{(k)}$ using system optimal assignment principle. Then update network link flows using MSA.
\[ X^{(k)} = X^{(k-1)} + \frac{1}{k} [\bar{X}^{(k)} - X^{(k-1)}] \]

5) check stop criteria: if \( |Y^{(k)} - Y^{(k-1)}| \leq \varepsilon \) and \( |X^{(k)} - X^{(k-1)}| \leq \varepsilon \) then stop computation, return to step 2 otherwise. Here \( \varepsilon \) is the pre-defined tolerance.

**Numerical Example**

In the process of transport network design, it is an important practical problem to establish the performance reliability of a transport network. There are various approaches to enhance the network reliability such as enhancing the link component strength, performing preventive maintenance work, improving network structure, and having alternative route choices for the users. In the network design problems, Braess presented an example demonstrating where adding a new route can increase travel time for all, called the Braess Paradox. Similarly, there is phenomenal that increasing capacity to an existing link in a congested network may not necessarily improve the overall network performance which is referred as the “Pigou-Knight-Downs paradox” by Arnott and Small (1994) and may actually increase the travel time (Yang, 1997). Yang and Bell (1998) introduced the capacity paradox and demonstrated that creating a new link in a network may actually reduce the potential capacity of the network and proposed the concept of network reserve capacity to avoid this capacity paradox.

In this paper, some possible approaches to improve the road network vulnerability are discussed through several numerical examples and the performance test results under different improvement strategies are analyzed.

**Network Setup**

The network structures of the numerical examples are designed to test the impact of various planning and policy strategies on the system-level vulnerability performance measures. Two types of networks are specified in this section, as illustrated in Figures 1(a) and 1(b). The two networks are used in Scenario A and Scenario B, respectively. On Scenario A network, a number of incremental link capacity levels are defined and tested. For Scenario B, the addition of a new roadway segment is defined based on the network for Scenario A. Both networks consider a 4-node system with single origin-destination (OD) pair (origin: Node 1, destination: Node 4). The demands are set to be external and constant in the numerical example for illustrative purposes.
The above two networks have similar link setups. Links 1 to 7 are identical in Figures 1(a) and 1(b). The Scenario network in Figure 1(a) has only one “express” link connecting Node 1 and 4 directly, while in Figure 1(b), Link 8 is added as the new expressway to the Scenario A network. And the impacts of its capacity variations on the performance of network reliability are examined in Scenario B and C. This example seeks answer to the empirical question that through which way one can more efficiently enhance the system reliability, capacity expansion (i.e. increase the capacity of existing links) or infrastructure expansion (i.e. add more links on the system). The BPR volume-delay function is used to compute travel time for simplicity. For each case, it is assumed that the capacity of one link is decreased to 10% if the demon selects that specific link to disrupt. Detailed link properties are provided in Table 1 below.

Table 1. Link setup of the numerical example

<table>
<thead>
<tr>
<th>Link</th>
<th>Free-flow time (minutes)</th>
<th>Capacity (vph)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scenario A</td>
<td>Scenario B</td>
</tr>
<tr>
<td>1</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>7</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>8</td>
<td>n/a</td>
<td>30</td>
</tr>
</tbody>
</table>

The capacity variables tested by the three scenario setups are denoted by V. Link 1 capacity in Scenario A is set always equal to the total capacity of Link 1 and 8 in Scenario B in order to make the expressways in these two cases comparable (Link 1 in Scenario A v.s. Link 1 and 8 in Scenario B). Scenario C assumes that the total capacity of link 1 and 8 remains the same and seeks the optimal capacity design.
In Scenario A, the analysis of a series of capacity decreases is conducted. First, the “do-nothing” scenario is studied and the most vulnerable link is identified, based on which we designed various capacity scenarios. The solution results are provided in the Figure 2. The two numbers shown in bracket on each link indicate the percentage of the optimal volume and the disturbance probability, respectively.

Based on the result, Link 1 is identified as the most vulnerable link since it attracts the highest traffic volume and has the highest failure probability. This result is as expected since link 1 is set to be a relatively faster (with capacity: 2500 vph) freeway connecting the origin and the destination directly. In this case, one key operations and planning question regarding reliability is, what if the capacity of this vulnerable link drops significantly due to an unexpected event such as a severe incident. In Scenario A, capacity decrease scenarios of the link 1 are specified, varying the capacity for 0 to 50% decrease (capacity varies from 2500 vph to 1250 vph) in a uniform step size.

In Scenario B we try to explain the impact of link addition on an existing Scenario A network and compare this policy strategy with Scenario A. For comparison purposes, the total capacity and the capacity decrease between the origin and destination are kept the same in the two scenario setups. For instance, if link 1 capacity is set to drop by 250 vph (10% decrease, from 2500 vph to 2250 vph) in Scenario A, the corresponding Scenario B case is to set link 8 capacity to drop from its original 1250 vph down to 1000 vph while link 1 capacity (1250 vph) remains unchanged. When the capacity decrease is set to 1250 vph, the two scenarios are identical. The solutions are presented in Figure 3. By comparing these two scenarios, we can gain some insights in the vulnerability of the two network designs when the capacity drops to a certain level. In Scenario C, we try to obtain the optimal capacity given that the sum of Link 1 and Link 8 capacity is set at a certain level. This scenario helps answer network design questions, such as: (1) how many links should it build to meet the predetermined travel demand; (2) What is the optimal capacity for each of the links.

**Results**

To solve this network problem, the authors employed the proposed bi-level optimization and iterative solution algorithm. An interesting question that arises naturally is how the proposed algorithm performs compared to other algorithms. To demonstrate the contribution in terms
of computational efficiency, the proposed method is compared with the MultiStart Algorithm (Ugray, et al., 2007). This heuristic endeavors to find the global optima by seeking a series of local solutions from a subset of \( n \) starting points. The search from multiple starting points which are defined on the feasible region improves the heuristic’s efficiency in finding the best local optimum. And this algorithm can run in parallel, distributing start points to multiple processors for local solution. This method is still an approximation to the global optimum. Both algorithms are employed to solve the problem raised in Scenario B. Comparing the two algorithms, it is clear that Bi-level optimization and iterative solution algorithm performs as good as the Multi-Start Algorithm. The average computational time for the proposed algorithm is 118.7 seconds compared to 547.3 seconds for the Multi-Start Algorithm (both experiments conducted on a computer with Intel Core-i7 CPU 2.90 GHz and 4G RAM). The results are compared in Appendix. More rigorous discussion on algorithms to solve this proposed system optimization model can be a direction for future studies.

The results of these scenarios are presented in Figure 3(a), 3(b), 3(c), and 3(d). The X axis of Figures 3(a), 3(b), and 3(c) represents the amount of capacity decrease. The Y axis of Figure 3(a) represents the system-level reliability measure (i.e. the expected total travel time, in minutes). We consider the network more robust with lower value of the reliability measure. Figure 3(a) indicates that capacity expansion of an existing roadway (Scenario A) is not always a desirable network development option. In some cases, infrastructure expansion (Scenario B) can be more efficient in reducing system vulnerability. Figure 3(b) illustrates different performance measures of Scenario A and B. We employ the difference of the system expected total travel times of Scenario A and Scenario B as the measure of travel time savings from infrastructure expansion when compared with capacity expansion. When there is no capacity drop at point 0, the vulnerability measure of the infrastructure expansion case (Scenario B) is 32.5% lower than that of Scenario A. The percentage of travel time savings gradually decreases when the capacity drops in Scenario A and B. However, in terms of absolute travel time saving, it is observed that when Link 8 capacity decreases to 350, the infrastructure expansion achieves the highest total travel time savings when compared to Scenario A. Figure 3(c) illustrates the expressway volume. When the capacity drops, the number of vehicles served by expressways also decreases. Compared with the expressway link in Scenario A, the expressway links in Scenario B can serve more travel demand. Figure 3(d) illustrates the system-level vulnerability measures of Scenario C. It indicates that the optimal design whence the total capacity of expressway link 1 and 8 is set to 2500 vph is 1250 vph for each expressway link. And the optimal total expected travel time is about 30% lower than that of the do-nothing scenario (point zero in Scenario C).

![Graphs](chart.png)

- a. System-level vulnerability measure (Scenario A and B)
- b. Travel time saving from infrastructure expansion (Scenario A and B)
c. Expressway Traffic Volume  
(Scenario A and B)  

Figure 3. The comparison results from scenario A and B

In this numerical example, the results of capacity variation and adding infrastructure vary drastically with respect to the system-level reliability measures. Planning strategies should be carefully examined since it can be detrimental if the capacity expansion is intended to accommodate a future fast-growing demand for travel. The implication of this comparison is that the network travel time reliability should be considered in the decision making process in network infrastructure design. Compared to Scenario A, evidently, the addition of link 8 results in a significant improvement of the network reliability. Scenario C further demonstrates that an optimal design of the network can be derived through this analysis. Overall, these three scenarios are designed for illustration purposes, demonstrating the capability of the model in supporting decision-making processes. More general conclusions should be carefully drawn based on a complete scenario analysis with the specifications of various supply- and demand-side uncertainties.

Conclusion and Direction for Future Research

This paper proposed a more computationally efficient approach to measure system-level network vulnerability. The first contribution of the paper was the originality of the model. It formulated a game theoretical model to solve the network vulnerability problem and the reliability performances are compared and discussed through the results from several reliability improvement strategies. Also, link-level BPR functions were built in the model formulation to reflect network traffic details.

The paper also contributed to the state-of-the-practice in how to solve this type of minmax problems. Solving the problem in its original form can be computationally extensive. The paper transformed the problem into a bi-level optimization model. Then a heuristic algorithm that iteratively solves the bi-level optimization model is also discussed and compared with multi-start algorithm in the numerical example.

The model has its practical value in various decision-support applications, including identifying the most vulnerable network link(s), achieving a more reliable system through network design strategies, among others. As demonstrated by the numerical example, the model is capable in analyzing system-level reliability measures under various planning and policy scenarios. Using a simple network example, this paper illustrated that the expansion to the capacity of existing road may actually reduce the network reliability at certain service level. This situation could be detrimental if the network improvement plan such as expanding
one lane for existing freeway corridor is designated to accommodate future potential high travel demands.

The second scenario further indicates that the addition of a new “express” road almost always improves the network reliability, as the users of the most vulnerable link (link 1) are provided with an alternative route (link 8). It is worth noting that the expansion to the existing network may or may not be a wise choice because of the possible existence of the capacity paradox (Yang and Bell, 1998) and the stochastic Braess’ paradox (Szeto, 2011).

For future research, first, more rigorous discussion on algorithms to solve this proposed system optimization model can be future studied. Second, the network reliability measure can be extended to be time-dependent. Finally, the potential integration of this model with other network and/or demand models may be studied to provide a more insightful suggestion to this research issue.

REFERENCES


Berdica, K., (2002) An introduction to road vulnerability: what has been done, is done and should be done. Transport Policy, 9, pp. 117-127.


Appendix

Table A1: Experimental Results Using the Bi-level Optimization and Iterative Solution Algorithm

<table>
<thead>
<tr>
<th>Scenario B Obj. Function Value</th>
<th>Computational Time</th>
<th>Scenario B Obj. Function Value</th>
<th>Computational Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bi-Level Multi-Start</td>
<td>Bi-Level Multi-Start</td>
<td>Bi-Level Multi-Start</td>
<td>Bi-Level Multi-Start</td>
</tr>
<tr>
<td>1</td>
<td>1.3445</td>
<td>1.3440</td>
<td>123.2</td>
</tr>
<tr>
<td>2</td>
<td>1.3778</td>
<td>1.3775</td>
<td>119.2</td>
</tr>
<tr>
<td>3</td>
<td>1.4126</td>
<td>1.4124</td>
<td>122.0</td>
</tr>
<tr>
<td>4</td>
<td>1.4486</td>
<td>1.4482</td>
<td>112.9</td>
</tr>
<tr>
<td>5</td>
<td>1.4855</td>
<td>1.4855</td>
<td>118.8</td>
</tr>
<tr>
<td>6</td>
<td>1.5237</td>
<td>1.5235</td>
<td>113.7</td>
</tr>
<tr>
<td>7</td>
<td>1.5628</td>
<td>1.5628</td>
<td>115.7</td>
</tr>
<tr>
<td>8</td>
<td>1.6039</td>
<td>1.6035</td>
<td>117.1</td>
</tr>
<tr>
<td>9</td>
<td>1.6459</td>
<td>1.6459</td>
<td>116.2</td>
</tr>
<tr>
<td>10</td>
<td>1.6896</td>
<td>1.6892</td>
<td>121.2</td>
</tr>
<tr>
<td>11</td>
<td>1.7366</td>
<td>1.7364</td>
<td>113.3</td>
</tr>
<tr>
<td>12</td>
<td>1.7821</td>
<td>1.7815</td>
<td>114.6</td>
</tr>
<tr>
<td>13</td>
<td>1.8299</td>
<td>1.8293</td>
<td>113.0</td>
</tr>
<tr>
<td>14</td>
<td>1.8798</td>
<td>1.8795</td>
<td>113.3</td>
</tr>
<tr>
<td>15</td>
<td>1.9323</td>
<td>1.9320</td>
<td>123.5</td>
</tr>
<tr>
<td>16</td>
<td>1.9848</td>
<td>1.9846</td>
<td>126.8</td>
</tr>
<tr>
<td>17</td>
<td>2.0411</td>
<td>2.0406</td>
<td>128.5</td>
</tr>
<tr>
<td>18</td>
<td>2.0965</td>
<td>2.0964</td>
<td>114.0</td>
</tr>
<tr>
<td>19</td>
<td>2.1581</td>
<td>2.1578</td>
<td>112.0</td>
</tr>
<tr>
<td>20</td>
<td>2.2200</td>
<td>2.2196</td>
<td>112.4</td>
</tr>
<tr>
<td>21</td>
<td>2.2838</td>
<td>2.2838</td>
<td>110.5</td>
</tr>
<tr>
<td>22</td>
<td>2.3504</td>
<td>2.3504</td>
<td>109.7</td>
</tr>
<tr>
<td>23</td>
<td>2.4194</td>
<td>2.4194</td>
<td>119.7</td>
</tr>
<tr>
<td>24</td>
<td>2.4911</td>
<td>2.4911</td>
<td>110.6</td>
</tr>
<tr>
<td>25</td>
<td>2.5651</td>
<td>2.5651</td>
<td>112.2</td>
</tr>
</tbody>
</table>