1-1-2021

APPROACHES TO VULNERABILITY ANALYSIS FOR DISCOVERING THE CRITICAL ROUTES IN ROADWAY NETWORKS

Hana Takhtfiroozeh

APPROACHES TO VULNERABILITY ANALYSIS FOR DISCOVERING THE CRITICAL ROUTES IN ROADWAY NETWORKS

By

Hana Takhtfiroozeh

A Dissertation

Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Civil Engineering

The University of Memphis

December 2021

Submitted to the Graduate Faculty as partial fulfillment of the
requirements for the Doctor of Philosophy Degree in Civil Engineering

Committee Members:

Dr. Mihalis M. Golias, Committee Chair

Dr. Charles Camp, Committee Member

Dr. Dincer Konur, Committee Member

Dr. Sabyasachee Mishra, Committee Member

Dr. Maryam Salehi, Committee Member

To my family for all their unconditional love and support

&

to the people in less-developed regions around the world who deserve a peaceful and better life

ACKNOWLEDGMENTS

I would like to sincerely thank my advisor, Dr. Mihalis Golias, for his trust and for presenting me with the great opportunity to work with him. I would personally and sincerely thank him for offering me his continuous support and guidance throughout this long journey. My gratitude is also extended to the members of my defense committee, Dr. Sabyasachee Mishra, Dr. Charles Camp, Dr. Maryam Salehi, and Dr. Dincer Konur.

I would like to thank my dad for all his love and support, and my mom for all her kindness and compassion throughout my whole life. I also want to thank my amazing friends, who were always there for me on my bad and my good days.

ABSTRACT

All modes of transportation are vulnerable to disruptions caused by natural disasters and/or man-made events (e.g., accidents), which may have temporary or permanent consequences. Identifying crucial links where failure could have significant effects is an important component of transportation network vulnerability assessments, and the risk of such occurrences cannot be underestimated. The ability to recognize critical segments in a transportation network is essential for designing resilient networks and improving traffic conditions in scenarios like link failures, which can result in partial or full capacity reductions in the system. This study proposes two approaches for identifying critical links for both single and multiple link disruptions. New hybrid link ranking measures are proposed, and their accuracy is compared with the existing traffic-based measures. These new ranking measures integrate aspects of traffic equilibrium and network topology. The numerical study revealed that three of the proposed measures generate valid findings while consuming much less computational power and time than full-scan analysis measures. To cover various disruption possibilities other than single link failure, an optimization model based on a game theory framework and a heuristic algorithm to solve the mathematical formulation is described in the second part of this research. The proposed methodology is able to identify critical sets of links under different disruption scenarios including major and minor interruptions, non-intelligent and intelligent attackers, and the effect of presenting defender. Results were evaluated with both full scan analysis techniques and hybrid ranking measures, and the comparison demonstrated that the proposed model and algorithm are reliable at identifying critical sets of links for random and specially targeted attacks based on the adversary's link selection in both partial and complete link closure scenarios, while significantly reducing computational complexity. The findings indicate that identifying critical sets of links is highly

dependent on the adversary's inelegancy, the presence of defenders, and the disruption scenario. Furthermore, this research indicates that in disruptions of multiple links, there is a complex correlation between critical links and simply combining the most critical single links significantly underestimates the network's vulnerability.

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER 1 : INTRODUCTION

Background

Every society is highly reliant on a variety of critical infrastructures, such as electricity, communication networks, water distribution systems, and transportation networks, which are the foundations of any country's economic and sustainable development. As these infrastructure systems became more complicated and interdependent, their vulnerability has increased as a result of technological advancements and improvements in their efficiency (1). By providing the means for travel, production logistics, and service delivery in everyday life, a functional and efficient transportation infrastructure significantly contributes to economic growth and prosperity. Also, a resilient transportation network is critical for rescue and evacuation during natural disasters like earthquakes and floods (2). Transportation systems, particularly roadway infrastructure, must be functional and resilient to disruptions and disasters in order to provide service to people on a daily basis. Additionally, to design infrastructures which can withstand such disasters while remaining economically feasible, it is crucial to configure the network in a way that sufficient accessibility is maintained when portions of the infrastructure fail.

Transportation network vulnerability has been extensively studied in recent years and has gained even more attention as the number of threats (e.g., climate change, man-made attacks, natural disasters, etc.) are increasing. Depending on the type of infrastructure and its functionality, vulnerability can be defined differently. In general, vulnerability is defined by two components; first is the susceptibility to disruptions, or in other words and according to the OXFORD dictionary, “Likely or liable to be influenced or harmed by a certain object,” which is a direct feature of the risk. The second component of the vulnerability definition is the degree of

performance reduction of the network. The strength and duration of the disruption, as well as the readiness of the system to cope with the disruption are the factors that can directly affect the performance reduction of the system.

There are different terminologies close to the vulnerability and identifying them and illustrating the relationships and distinctions between them can be extremely beneficial in comprehending the concept of vulnerability. The following is a very brief description of these concepts, and Figure 1-1 illustrates the boundaries and interactions between these terminologies.

- Risk is the probability of occurrence of a disruption multiplied by the failure probability of the network
- Reliability is the probability that a network can deliver the standard performance
- Robustness is the ability of the network for maintaining its originally standard function during the disruption
- Flexibility is the ability to adapt to possible planning changes in the aftermath of disruptions.
- Resilience is the closest concept to vulnerability, and it will be defined as the capability of the network for resisting and recovering from the disruption.

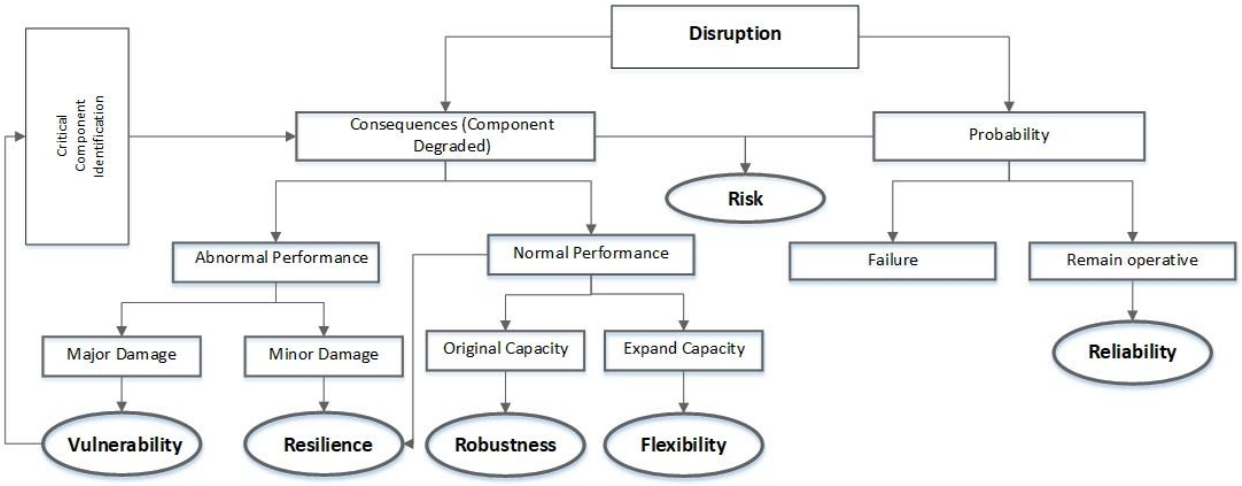


Figure 1-1 A schematic of the interactions of vulnerability terminologies.

Problem Statement

The goal of vulnerability and resilience analysis is to evaluate and predict the impact of disruptions and identify the important segments in the system. Numerous studies examine various techniques to addressing the system's vulnerability and evaluate its components. A vulnerability measure value is used to quantify the impact of network disruptions and to assess the system's performance. Due to network topological features, the intensity of link usage, or the existence of significant destinations, a certain segment of the network may be more important than others. In other words, some links are more critical than the others and any damage or in the worst-case scenario failure of these links or a group of them may have more severe damage to the system and can result, resulting in a significant increase in travel costs. Therefore, identifying and ranking the links that have the most significant effects on the overall performance of the network disruptions is an important consideration for operators and planners. A single factor cannot solely determine the criticality of a link; several factors with various weights determine the criticality of a link in different contexts. As a result, given the varying criticality of various links and budgetary constraints, strengthening and maintaining transportation network links needs to be considered based on a prioritization methodology that incorporates multiple factors (3).

Research Objective

The primary goal of this research is to present different frameworks for identifying critical single links and groups of critical links to assist decision-makers in developing an optimal investment strategy that maximizes network resilience to different disruptions. The contribution of this research is two folds. First, proposing new link criticality measures and evaluate their

accuracy. These measures balance accuracy and computational complexity by combining traffic equilibrium and network structure parameters. Second, presenting a methodology based on the game theory framework for identifying the most critical set of links in a roadway network under minor and major disruptions and evaluate the results. Both presented methodologies are capable of being applied to large-scale networks with minimal computational overhead.

Significance

Assessing the vulnerability of large-scale roadway networks while taking user behavior into account is a computationally intensive process. To propose vulnerability measures, the majority of studies either focus exclusively on the topological aspects of the network, which is inaccurate for transportation networks, or consider travelers' behavior in all possible scenarios of link failure, which requires significant computational power and time which is not always applicable to real-world networks. First part of this research proposes a method for considering network structure and traffic attributes concurrently without imposing a computational burden on planners and decision makers, which can be used as valid ranking measures for rating links in a large-scale road network.

Due to the intricacy and time-consuming nature of the investigation, most current studies on roadway vulnerability focus exclusively on single link failure, which does not reveal much about the big-picture network vulnerability. In real-world road network circumstances, disruptions affect many links. Additionally, the majority of studies have examined only complete disruption of the links, which results in an incorrect representation of regular small incidents and everyday accidents, such as the closure of many lanes along a path due to car accidents or severe weather. The second section of this research proposes an optimization framework that is capable of

identifying a crucial set of links in a large roadway network that is subjected to minor and major disruptions. Additionally, the presented methodology is capable of evaluating the various decision-making budget restrictions involved in improving the network's resilience.

Dissertation Organization

The remaining chapters of this dissertation are comprised of two papers. This Introduction is the first chapter of the dissertation and discusses the dissertation's primary problem and purpose. The remainder of the dissertation is organized as follows.

Chapter 2: *Topological-Based Measures with Flow Attributes to Identify Critical Links in a Transportation Network*

This chapter presents new link criticality measures for ranking individual links in roadway networks. The presented measures were applied to various case study networks, and the results were compared to three previously published vulnerability measures. This chapter includes the current literature regarding the various types of ranking measures in vulnerability roadway analysis.

Chapter 3: *Identifying Critical Sets of Links in a Roadway Network under Different Disruption Scenarios Using the Game Theory Framework*

This chapter introduces an optimization model based on the game theory framework for identifying the most critical combination of critical links in a roadway network under various disruption scenarios. This was accomplished by defining various attack scenarios and evaluating the resulting outcomes using both full scan analysis techniques and hybrid ranking measures on the case study network. This chapter also summarizes the literature of the various approaches in vulnerability roadway analysis.

Chapter 4 presents the result of implementing proposed methodologies in a real case study network to identify the most critical single and multiple critical links in Broward County, Florida.

Chapter 5 is the discussion chapter and summarizes the research approach, lists the main findings and conclusions, and provides recommendations for future research.

CHAPTER 2 : TOPOLOGICAL-BASED MEASURES WITH FLOW ATTRIBUTES TO IDENTIFY CRITICAL LINKS IN A TRANSPORTATION NETWORK

An important part of transportation network vulnerability analysis is identifying critical links where failure may lead to severe consequences, and the potential of such incidents cannot be considered negligible. Existing transportation network vulnerability assessment can be categorized as topological, or traffic based. Topological-based assessment identifies the most critical components in the network by considering network structure and connectivity. Traffic-based assessment identifies the most critical components in the network by full-scan analysis and takes into consideration effects of link failures to traffic flow assignment. The former approach does not consider traffic flow dynamics and fails to capture the non-linearity performance function of transport systems while the latter, even though accurate and robust, requires significant computational power and time and may not always be feasible for real life size networks. The primary objective of this research is to propose new link criticality measures and evaluate their accuracy for transportation network vulnerability assessment. These measures combine characteristics of traffic equilibrium and network topology to balance accuracy and computational complexity. Nine measures are proposed, and their accuracy are compared to three existing traffic-based measures using three case study transportation networks from the literature. Results indicate that three of the proposed measures show strong correlation to the three traffic-based measures while requiring significantly less computational power and time.

Abbreviations

BC	Betweenness Centrality
BC*	Flow Weighted Betweenness Centrality
CCL	Common Critical Links
CSN	Chicago Sketch Network
EMN	Eastern Massachusetts Network
FBC	Flow Betweenness Centrality
FFTT	Free Flow Travel Time
IS	Importance Measure
NRI	Network Robustness Index
NRI*	Network Robustness Index, Modified
SFN	Sioux Falls Network
$T_{FF}BC$	Free Flow Travel Time Betweenness Centrality
$T_{C}BC$	Congested Travel Time Betweenness Centrality
$T_{L}BC$	Travel Time Loss Betweenness Centrality
$T_{FF}BC^*$	Flow Weighted Free Flow Travel Time Betweenness Centrality
$T_{C}BC^*$	Flow Weighted Congested Travel Time Betweenness Centrality
$T_{L}BC^*$	Flow Weighted Travel Time Loss Betweenness Centrality
FBC*	Flow Weighted Flow Betweenness Centrality
UE	User Equilibrium

Introduction

Transportation networks form the backbone of economic and sustainable development in a society and need to be functional and efficient to provide appropriate services to people during their normal daily life (e.g., providing the means for travel, production logistics, and delivery of services). These networks should also be robust against disruptions and disasters (2) (e.g., a lifeline for emergency services and medical care). Disruptions could be due to a wide variety of threats which may originate from inside the road transport systems, such as daily traffic crashes or maintenance activities, or could be due to external strains imposed to the system, commonly caused by nature (e.g., adverse of weather, earthquake, etc.).

Transportation network vulnerability studies started after the Tasman Bridge disaster in 1975, where Lock and Gelling (4) studied the impact of failures or loss of critical components of transportation infrastructures. However, while this area was studied in academia for years, it took decades for transport modelers to pay attention to this phenomenon. When substantial infrastructures were destroyed after the Great Kobe earthquake in 1994, causing more than $150 billion economic losses, resilience and vulnerability of the transportation infrastructure were considered by governments and transportation agencies as interesting and important topics (5). Over the last decades, vulnerability emerged as a significant area in transportation planning research and received more attention from researchers and planners for two main reasons: first, interest in developing the theory behind network vulnerability, and second, applying the new methodologies and models to large-scale networks. In the area of transportation systems, vulnerability analysis focuses on identifying and ranking infrastructure elements that would have the highest effect in case of failure (6). Resilience, on the other hand, reflects the dynamic performance of the network after a disruption (7) and is another term with definition and

interpretation akin to the term of vulnerability. Resilience encompasses vulnerability and, focuses on decision making (operational, tactical, and planning levels for individuals and communities) to develop a transportation system that can withstand disruptions, continue to operate within an acceptable level of efficiency during and right after a disruption, and return to normal operating conditions within the shortest possible time.

As will be discussed in more detail in the next section of this research, two main types of measures (topological and traffic-based) have been developed and presented in the literature to evaluate the importance of a link in a transportation network. Topological-based measures do not consider traffic flow dynamics and fail to capture the non-linearity performance function on transport systems. On the other hand, full-scan analysis (traffic-based measures), where the network is evaluated for every possible scenario of link failure, is more accurate and robust, but requires significant computational power and time and may not always be applicable to real life networks. This research suggests an approach where network structure and traffic attributes are jointly considered without the need of a full-scan analysis. The methodology proposed in this research extends the use of topological-based measures by incorporating flow characteristics to enhance their accuracy and reliability in large scale networks where traffic-based measures are expensive to use.

The remainder of the chapter is as follows: The next section provides a summary of the related literature, followed by a section presenting the proposed new measures. The fourth section presents and discusses results from a set of numerical experiments using three case study networks commonly found in the literature. The last section concludes the chapter, discusses the limitations of the proposed measures and future research directions.

Literature Review

An important part of transportation network vulnerability analysis and resilience is the identification of critical links where failure may lead to severe consequences for the whole network, and where the potential of such incidents cannot be considered negligible (3). According to Mattsson et al. (8) vulnerability analysis could be divided into two main groups: 1) topological-based analysis, and 2) traffic-based analysis, which based on these approaches, numerous measures for identifying critical components in the network have been proposed. However, some studies incorporate traffic characteristics into existing topological measures and develop hybrid measures for identifying the critical links in transportation network (9). A brief discussion of each is provided here in.

Topological-Based Analysis

Topological-based analysis considers the network structure and connectivity. It represents the transport network in the form of a graph with a set of nodes (vertices) and a set of links (edges). It mainly considers two main aspects of the network structure: network efficiency and node centrality. This analysis can provide a good understanding of the network structure and its connections but fails to account for the behavior of the user. There are several studies that evaluate network vulnerability using topological-related factors; however, only a few numbers have been published in transportation-focused journals. For example, an accessibility index based on distance-only and distance-traffic volume criteria is defined by Sohn (10). Demsar et al. (11) studied the urban street network of the Helsinki Metropolitan Area in Finland defining links with the high value of betweenness and cut links as more critical ones. By taking into account the alternative links, a topological indicator is presented by Knoop et al. (12). In another study, degree and betweenness centrality indicators for six real city road networks with simulating

attacks with remaining nodes was calculated (13). Table 2-1 summarized the topological based measures presented by researchers for assessing the roadway network.

Table 2-1 Topological-based Vulnerability Measures

Ref.	No. of degraded components	Approach	Indicator(s) to capture consequences	Method	Conclusions
(14)	Network	Distance	Network efficiency Global and Local efficiency	-Shortest path -Weighted and unweighted network	Global efficiency is a measure of the directness of the connections between all node pairs, however, local efficiency indicates the average directness of the connections between the neighbors of a node.
(10)	Single link	Distance & flow	Accessibility index	-Shortest path -Distance-traffic volume indicated a link with heavy traffic (efficiency-oriented)	These two criteria give accessibility loss to completely different links
(15)	Nodes	Distance	-Degree distribution -Degree correlations -Clustering coefficient	-A dual graph is presented -A comparison between primal and dual graph	A complex network approach to the urban street networks has advantages with compare to syntax formalism
(16)	Single link	generalized cost	Accessibility measure	Analyzing the network vulnerability in terms of topological configuration and socio-economic impacts	more efficient algorithm for applying on large network is needed and calculating sets of critical links is needed.
(11)	Single link	Shorter Distance	-Cut vertices measure, -Betweenness measure, clustering coefficient measure	-Combining dual graph modeling with connectivity analysis and betweenness and clustering coefficient -Undirected and unweighted network	Links with the high value of betweenness and cut links are more critical ones. locations have one or more of the following three properties: • Cut links • High betweenness • Low clustering coefficient
(13)	Nodes	Shorter Distance	-Betweenness centrality -Degree of Distribution	-undirected graph -choose three types of road granularities, -four successive attack strategies applied	Topological structure such as betweenness centrality distribution is more essential to the robustness of a network that geographical features of the network. the robustness pattern was quite similar for different cities
(17)	Nodes	Shorter Distance	Betweenness centrality	Developed an algorithm for computation of BC for real-time	Prove the existing a significant correlation between global efficiency and BC. Ranking Nodes based on their metric

Traffic-Based Analysis

The main disadvantage of topological based analysis is that it ignores the dynamic features of a transportation network and analyze a congested as an uncongested network (i.e., they do not account for traffic rerouting due to link failure). Topological analysis might be sufficient for analyzing some types of networks (e.g., social networks) where a failure of a link may only result in a re-route between nodes. Modeling of roadway networks on the other hand, is more complex and estimating an equilibrium after a change in the network's topology is more challenging as all traffic equilibrium models try to emulate human behavior. Hence, it may not be realistic to only consider the topological aspects of a road network for assessing link criticality.

To address these issues, researchers suggested traffic-based analysis which models the network as an abstract network and applies demand and supply analysis. Full-scan analysis is the most common approach used in the literature, where links are removed one by one, and a performance measure (usually a function of travel time) is calculated for each link removal, and the links are ranked based on the changes in value of the selected measure. Such measures require a User Equilibrium (UE) to be identified every time a link is removed. The main network's performance measure in most of these studies is based on increases in travel time, flow, or a generalized cost function (18–24). These methods provide more accurate results but are not applicable to real life large-scale networks. High computational times required from estimating multiple UEs and dis-connectivity that might occur during removal of links are the biggest issues for applying these methods large-scale transportation network (6).

In addition, a group of researchers have tried to adopt traffic-based analysis with game-theory concepts to identify sets of critical links, instead of individual links. Under these methods,

networks are part of a game between three players; the designer, attacker, and the users (3,25–28). Such models suffer from the same drawbacks of high computational and time requirements (requiring multiple UE solutions for the users of the network) and have been very difficult to implement in real size networks. Table 2-4 summarized the traffic-based measures presented by researchers for assessing the roadway network.

Table 2-2 Traffic-based Transport Vulnerability Measures

Ref.	Single /Multiple links	Approach	Indicator(s) to capture consequences	Method
(20)	Single	Generalized Cost	Exposure index Importance index	weighted cost by travel demand-link importance using the shortest path The Importance of a link is a function of the increase in weighted travel time that occurs when that link is disrupted.
(23)	Single	Travel Time	Robustness Index	Optimization Based System-wide re-assignment of traffic when a specific link is removed examined the relationship between volume, capacity and link criticality.
(29)	Single	Generalized Cost	Accessibility Index	Four Accessibility Index by combining travel demand model • Network accessibility, • Zonal accessibility, • O–D accessibility • O–D accessibility by each mode
(30)	Single/Multi	Generalized Cost	Accessibility Index	Assess system-wide effects Based on benefits
(31)	Single	Flow	efficiency measure for elastic or fixed demands	Optimization Based for elastic (no users want to alter his travel decision) or fixed demands (cost equity)
(32)	Single	Travel Time	Robustness Index	Rank-ordering critical link based on capacity-reduction and connectivity
(33)	Single	Generalized Cost	Accessibility Index	Optimization based-ranking links Used Hansen integral index as accessibility index
(21)	Multiple	Travel Time	Vulnerability index	Optimization-Based Grid-base full closure for finding the Worst-case Scenario
(12)	Single	Travel Time	Robustness Index	Alternate route indicator
(34)	Single	Generalized Cost	Accessibility Index	Optimization-based (Fuzzy Method) Two vulnerability index: • based on physical characteristics • Operational characteristics
(6)	Single	Flow	Link Importance Index	Ranking links based on local and global importance
(18)	Single	Generalized Cost	Accessibility Index	Deprivation cost and logistics cost Optimization-based, Find the worst-case scenario

Hybrid Analysis

A few studies have been published trying to incorporate traffic assignment characteristics (e.g., flow, travel time, etc.) into existing topological measures (e.g., centrality measures, efficiency, etc.) and develop new criteria which could be called hybrid measures. These approaches try to reduce computational and time requirements while retaining accuracy in ranking the critical links in transportation networks.

A simulation-based criticality measure called Stress Test Criticality developed to capture the effect of day-to-day disruptions (i.e., reduced link capacity instead of removing the link from the network) was proposed by Gauthier et al. (35) and considered four different link criticality measures based on Betweenness-Centrality i.e., Unweighted BC, Travel-time weighted BC, unweighted BC on entry/exit nodes only (BC entries–exits), and Travel-time weighted BC from entry to exit nodes only. Results of their study suggested that the adequacy of the proposed measures is highly variable. Link Criticality Index proposed by Almotahari and Yazici (9) is based on the link marginal cost and utilizing the convex combination solution of the UE problem. They compared ranking links using their proposed measure, three existing traffic-based measure (20,23,31), and one hybrid measure (35) with UE link flow. While ranking links using their proposed index had a very low correlation with the UE link flows (correlation = 0.2), the other measures were outperformed better by showing correlations ranged from 0.31 (for the hybrid measure) to 0.9 (for the traffic-based measures). Li et al (36), proposed an approach which by considering traffic flow betweenness index is able to identify the critical links in large scale network. The traffic flow betweenness index is calculated based on traffic flow betweenness and rerouted travel demand. The proposed index performed better in identifying critical facilities (e.g., bridges) when compared to the Hansen accessibility index.

To improve computational efficiency, this research proposes nine new measures making the balance between the accuracy of the traffic-based measures and the applicability of the topological -based measures for large-scale networks. The proposed measures combine elements of topology and traffic characteristics of a roadway network and require significantly less computational power and time. To evaluate the accuracy of the results, the proposed measures, through a set of numerical experiments, are compared to three traffic-based measures that are commonly used as benchmarks in the related literature. Next, the traffic-based measures selected to evaluate the proposed measures, the proposed new hybrid measures, and the methods used to evaluate their accuracy are discussed.

Methodology

In this research, nine hybrid measures which are variants of the link Betweenness Centrality (BC) measure are proposed and evaluated. Applying of these measures only require the UE conditions for the base network (i.e., network condition when all links are operational). BC was first introduced by Freeman (37), and it is known as finer-grained measure between other centrality measures such as closeness and degree centrality (35), and has been applied to a wide range of graph theory problems. For a link, the value of BC expresses the frequency the link falls on the shortest paths connecting pairs of nodes (Equation 1). Links with high betweenness centrality values represent a bridge-like connector between different parts of a network, a failure of which will affect the communication between multiple pairs of nodes through the shortest path.

$$\boldsymbol{BC(a)} = \sum_{s,t} \frac{\sigma_{st}(a)}{\sigma_{st}} \quad \text{(Equation 1)}$$

where $\sigma_{st}(a)$ is the shortest path from node *s* to node *t* that traverses link *a*, and σ_{st} is the number of the shortest path from node *s* to *t*.

According to Equation 1, equal weights are assumed for every edge between every pairs of nodes in the network and routes are chosen based on hop counting in shortest path strategy. In order to no longer treat links as binary interactions when calculating the shortest paths in a network, links can be weighted. Weighting links adds another dimension of heterogeneity to the network beyond the topological effects. The weights proposed herein combine elements of network connectivity and demand/supply attributes to balance accuracy and computational time in identifying critical links in a roadway network. A brief description of all nine proposed hybrid measures, applied weights, nomenclature and formulas are provided in Table 2-3. Next, the weighted measure categories proposed in this research are presented and discussed.

Proposed Weighted BC Measures

An edge-weighted graph is a pair of *(G,w)*, where *G=(V,E)* is a graph with a set of Vertices *(V)* and a set of Edges *(E)*, and *w:E⟶R* is a weight function, often referred to as the "cost" of the edge. Dijkstra (38) proposed an algorithm for finding the path of least resistance in a weighted graph. According to this algorithm, weights of the links represent the cost of transmitting (e.g., travel time) the links, therefore, high values indicate the weak or costly links. In this research, to examine the impact of distinct traffic attributes on modifying the BC, as a measure that only considers the topological aspects of the network, different traffic characteristics were assigned as link's weight in BC calculation. Therefore, the proposed measures can rank the links by

considering two fundamental network factors in analyzing their criticality, I) centrality and II) traffic characteristics.

Uncongested Network Weight

The UE principle assumes that users will always choose the shortest path from their origin to their destinations, irrespective of the type of the link (e.g., highway, arterial, collector etc.). To capture the UE principle in an uncongested network, Free Flow Travel Time (FFTT) was considered in this research as an edge weight when computing the shortest path used in the calculations of BC. FFTT can be effective in identifying critical links in uncongested conditions.

Congested Network Weight

Congested travel times (which are a function of FFTT, link utilization i.e., volume to capacity ratios, and class e.g., collector, arterial, etc.) are better indicators of shortest paths under congested conditions. In this research, two weights were considered in the BC calculations to capture user behavior in congested networks. The first weight was the actual travel time (which will be referred to as congested travel time), calculated using the Bureau of Public Roads (BPR) function (39). The second weight was the difference of actual travel time and free flow travel time of a link can be referred as travel time loss of a link.

Medium Congested Network Weight

To capture the importance of a link under medium congestion conditions, and based on how Dijkstra algorithm (38) treats the edge's weights in the shortest path calculation, a flow-based decay function weight is proposed in Equation 2.

$$w_a = F_{max}(1 - r)^{F_a} \quad \text{(Equation 2)}$$

where F_{max} is the maximum flow over all the links in the network, r is the decay rate set equal to 0.01 through experimentation discussed in the next section, and F_a is the flow on link a.

Social Efficiency

Based on the social efficiency perspective, roads with more demand serve more people and thus generate higher social and economic benefits, hence, need to be considered more significant. To account for social efficiency, four additional measures were introduced. These measures are based on the product of the weighted BC (uncongested, congested demand, and social efficiency weights) and link's flow. In Table 2-3, these measures are marked with a star sign.

Table 2-3 Proposed Hybrid Measures

Hybrid Measure's Name and Abbreviation	**Link Weight for BC Estimation**	**Formulation**	**Description**
Free Flow Travel Time BC (***$T_{FF}BC$***)	Free Flow Travel Time (T_a^{FF})	$T_{FF}BC_a = w_a BC_a$ $w_a = T_a^{FF}$	BC_a=Betweenness Centrality of link a $T_a^{\mathrm{FF}}=\frac{L_a}{FFS_a}$ FFS_a=Free Flow Speed of link a L_a=Length of link a
Congested Travel Time BC (***$T_C BC$***)	Congested Travel Time (T_a^C)	$T_C BC_a = w_a BC_a$ $w_a = T_a^C$	$T_a^C = T_a^{FF}\left[1+\alpha(\frac{F_a}{C_a})^{\beta}\right]$ F_a=Flow of link a C_a=Capacity of link a α & β =Model parameters
Travel Time Loss BC (***$T_L BC$***)	Travel Time Loss (T_a^L)	$T_L BC_a = w_a BC_a$ $w_a = T_a^L$	T_a^L=$T_a^C - T_a^{\mathrm{FF}}$ T_a^C= Travel Time of link a T_a^{FF}=Free Flow Travel Time of link a
Flow BC (***FBC)***	Flow as a decay function	$FBC_a = w_a BC_a$ $w_a = F_{max}(1-0.01)^{F_a}$	F_{max} = Maximum flow value in the network
Flow Weighted BC ***(BC*)***	Flow (F_a)	$BC^*{}_a = F_a * BC_a$	BC_a = Betweenness Centrality of link a
Flow Weighted Free Flow Travel Time BC (***$T_{FF}BC$*)***	F_a and T_a^{FF}	$T_{FF}BC^*{}_a = F_a * T_{FF}BC_a$	$T_{FF}BC_a$ = Free Flow Travel Time BC of link a
Flow Weighted Congested Travel Time BC (***$T_C BC$**)	F_a and T_a^{C}	$T_C BC^*{}_a = F_a * T_C BC_a$	$T_C BC_a$ = Congested Travel time BC of link a
Flow weighted Travel Time Loss BC (***$T_L BC$**)	F_a and T_a^{L}	$T_L BC^*{}_a = F_a * T_L BC_a$	$T_C BC_a$ = Travel Time Loss BC of link a
Flow weighted Flow BC (***FBC*)***	F_a and $F_{max}(1-0.01)^{F_a}$	$FBC^*{}_a = F_a * FBC_a$	FBC_a = Flow BC of link a

Benchmark Measures

To evaluate the proposed measures, we compare their performance to three existing traffic-based link ranking measures: the Network Robustness Index (NRI) (23), the Importance Measure (IS) (20), and the Network Robustness Index Modified (NRI*) (24). All these three measures use the full scan analysis methodology for ranking links where links are removed one by one, and a performance measure (usually a function of travel time) is calculated in each step, and the links are ranked based on the changes in value of the selected measure. Most of the published research proposing new vulnerability measures have used at least one of these three measures as benchmarks (9,36,40) as they are extremely accurate, albeit time consuming and not applicable for full-scan analysis on large-scale networks. It is worth mentioning that if a link's removal results in a disconnected network, such a link is automatically categorized as highly critical (although in large-scale transportation networks removal of a single link is highly unlikely to lead to a disconnected network, since multiple paths exist between each origin-destination pair). A brief description of each traffic-based link ranking measure is presented next. The formulas and notations for each measure are also provided in Table 2-4.

Table 2-4 Traffic-Based Measures from The Literature

Measure	Reference	Formulation	Description
NRI	(23)	$NRI_a = C_a - C_0$	C_0: Network travel time when all links are present in the network C_a: Network travel time when link *a* is removed from network
IS	(20)	$Is_a = \frac{\sum_i \sum_{j \neq i} x_{ij} (C_{ij}^a - C_{ij}^0)}{\sum_i \sum_{j \neq i} x_{ij}}$	x_{ij}: Travel demand between origin *i* and destination *j* C_{ij}^0: Travel time from origin *i* to destination *j* when all links are present in the network C_{ij}^a: Travel time from origin *i* to destination *j* when link *a* is removed from network
*NRI**	(24)	$NRI_a{}^* = \sum t_i^a x_i^a - \sum t_i x_i$	x_i^a: Travel demand on link *i* when link *a* is removed and network is re-routed t_i^a : Travel time on link *i* when link *a* is removed from the network x_i: Travel demand on link *i* when all links are present in the network t_i: Travel time on link *i* when all links are present in the network

NRI: Network Robustness Index, IS: Link Importance, NRI*: Modified Network Robustness Index

Network Robustness Index (NRI) presented by Scott et al. (23) could be considered as the first traffic-link based measure for analyzing the criticality of the road network. NRI was initially presented as an alternative for link-based volume/capacity ratio which is a local measure for identifying critical links in the system. NRI for a link was defined as the difference in total travel of the network between the base case when all links are present in the network and in a case when a specific link is removed from the network.

The exposure-importance method was developed for identifying the link importance index as a measure for finding critical links by Jenelius et al. (20). The Berdica's definition of vulnerability was utilized based on loss of serviceability in the system in this method (41). Link importance and site exposure measures were derived based on the increase in the generalized cost of travel in degraded networks considering social efficiency by weighting the travel cost by travel demand.

As mentioned earlier, the NRI index is the change in total travel time resulting from re-assignment of traffic when a specific link is removed, hence, it is a scaled index and cannot be used to compare the networks. The Network Trip Robustness index was proposed in order to compare the networks (24). Network Trip Robustness index is calculated by dividing the summation of a modified NRI (NRI*) value across all individual links by the total trip demand. The Modified NRI is the difference between sum of the product of each link's travel time and the flow across it when that link is removed and the base case scenario.

Hybrid Measures Evaluation Metric

Spearman's Rank Correlation between the traffic-based and hybrid measures is used to evaluate the reliability and sensitivity of the proposed measures in identifying the critical links of a roadway network. Spearman's rank correlation coefficient (r_s) (42) is a statistical measure for assessing the strength of a monotonic relationship (linear or not) between the elements of two sets. Let *X* and *Y* be two sets of link rankings based on two different measures. Both sets have the same cardinality *n*. Let x_i and y_i be the rank of link *i*. The Spearman's rank correlation coefficient (r_s) between the two sets *X* and *Y* is calculated using Equation 3:

$$r_s = 1 - \frac{6\sum_i (x_i - y_i)^2}{n(n^2 - 1)} \qquad \text{(Equation 3)}$$

The value of r_s lies between -1 and +1, with -1 indicating a perfect negative and +1 indicating a perfect positive association of ranks. A positive correlation coefficient expresses a positive relationship between two elements of sets (as rank of one element in one set increase, rank of the corresponding element in the other set also increases) while a negative value of

r_s indicates a negative relationship between two sets (as rank of the element in one set increase, rank of the corresponding element in the other set decrease) and a zero value for r_s means there is no correlation between the two sets. The aim of the evaluation is to find the perfect match with the benchmarks, so as much as results illustrate the higher value of r_s between presented and benchmark criticality measures, they have more monotonic relationship together. Since the correlation between the two sets of data depends on the size of the data set, there is no absolute description for interpretation of r_s. To make it more clear for interpretation, the strength of the correlation could be categorized using the guidelines presented in Table 2-5 for the value of r_s.

Table 2-5 Interpretation of Spearman's Rank Correlation Coefficient (r_s)

Range of r_s	**Strength of the Correlation** (positive/negative)
$-0.5 \leq r_s \leq 0.5$	Weak
$0.5 < r_s \leq 0.7\ , -0.7 \leq r_s < -0.5$	Moderate/Strong
$0.7 < r_s \leq 1, -1 \leq r_s < -0.7$	Strong/Very strong

Numerical Experiments

In this section results from numerical experiments used to perform the analysis to evaluate the proposed hybrid measures for three case study networks are presented and discussed. Figure 2-1 shows a flowchart of the steps taken to perform the analysis.

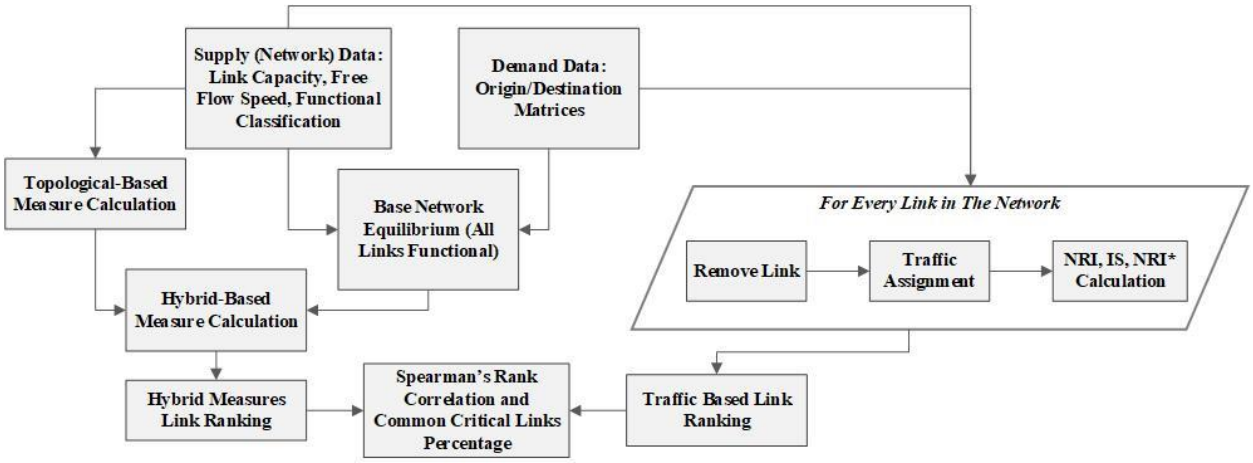


Figure 2-1 Numerical experiments steps

Case Study Networks

To evaluate the proposed hybrid measures, three case study networks commonly found in the literature were used (Sioux Falls-small size, Eastern Massachusetts-medium size, Chicago Sketch-large size). Table 2-6 provides the basic information of each network while Figure 2-2 provides schematics of the networks. Data for the networks was obtained from (43).

Table 2-6 Selected Networks for Evaluating the Hybrid Measures with Traffic-Base Measures

Network	No. of Nodes	No. of Links	No. of Zones	No. of UE Paths
Sioux Falls Network (SFN)	24	76	24	757
Eastern Massachusetts Network (EMN)	74	258	74	1196
Chicago Sketch Network (CSN)	933	2950	387	215,767

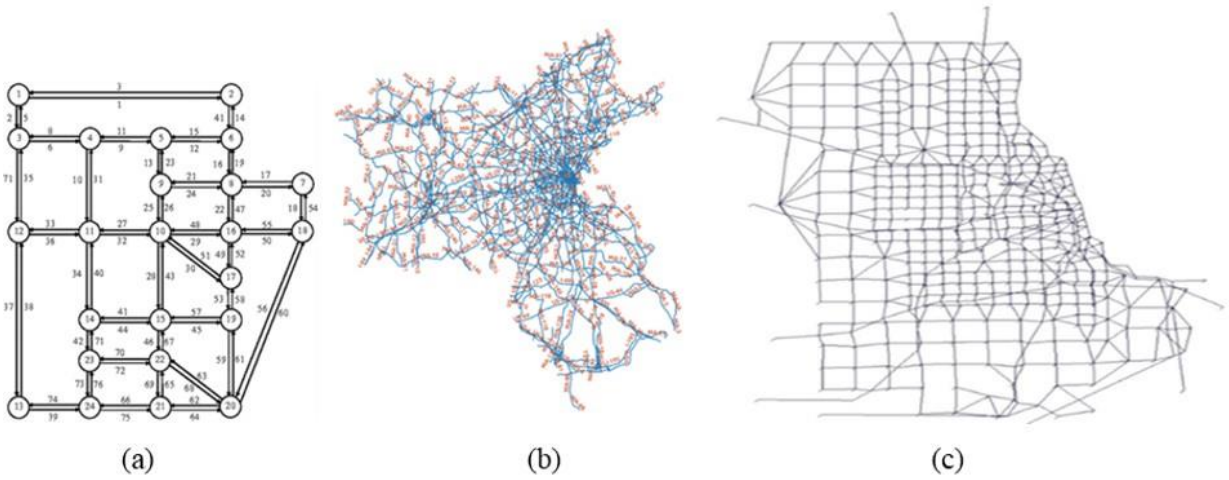


Figure 2-2 Case study networks: (a) Sioux Falls, (b) Eastern Massachusetts, and (c) Chicago Sketch

Spearman's Rank Correlation Results: Traffic-Based with Hybrid Measures

For each of the three-case study networks, the Spearman's rank correlation coefficient (r_s) values between the traffic-based and hybrid measures over all the links (excluding centroid connectors) were calculated. Results are reported in Table 2-7 and indicate that BC shows a weak correlation with all three traffic-based measures and degrades with network size, especially when compared to most of the proposed hybrid measures. For example, when the graph is weighted by the link's travel time (T_CBC), a much higher correlation is obtained with all traffic-based measures (r_s of about 0.70 for SFN). Results shown in Table 2-7 reveal that four of the hybrid measures (i.e., T_CBC, BC*, T_{FF}BC*, and T_CBC*) show promise and exhibit moderate to strong correlation (i.e., $r_s \in [(-1,-0.5) \cup (0.5,1)]$) with at least two out of the three traffic-based measures. Among these four measures, T_CBC does not perform well for the largest network (CSN) while the other three (BC*, T_{FF}BC*, T_CBC*), that consider social efficiency, exhibit strong correlations with the IS and NRI* as the network size increase.

Table 2-7 Spearman's Rank Correlation: Traffic-Based with Hybrid Measures

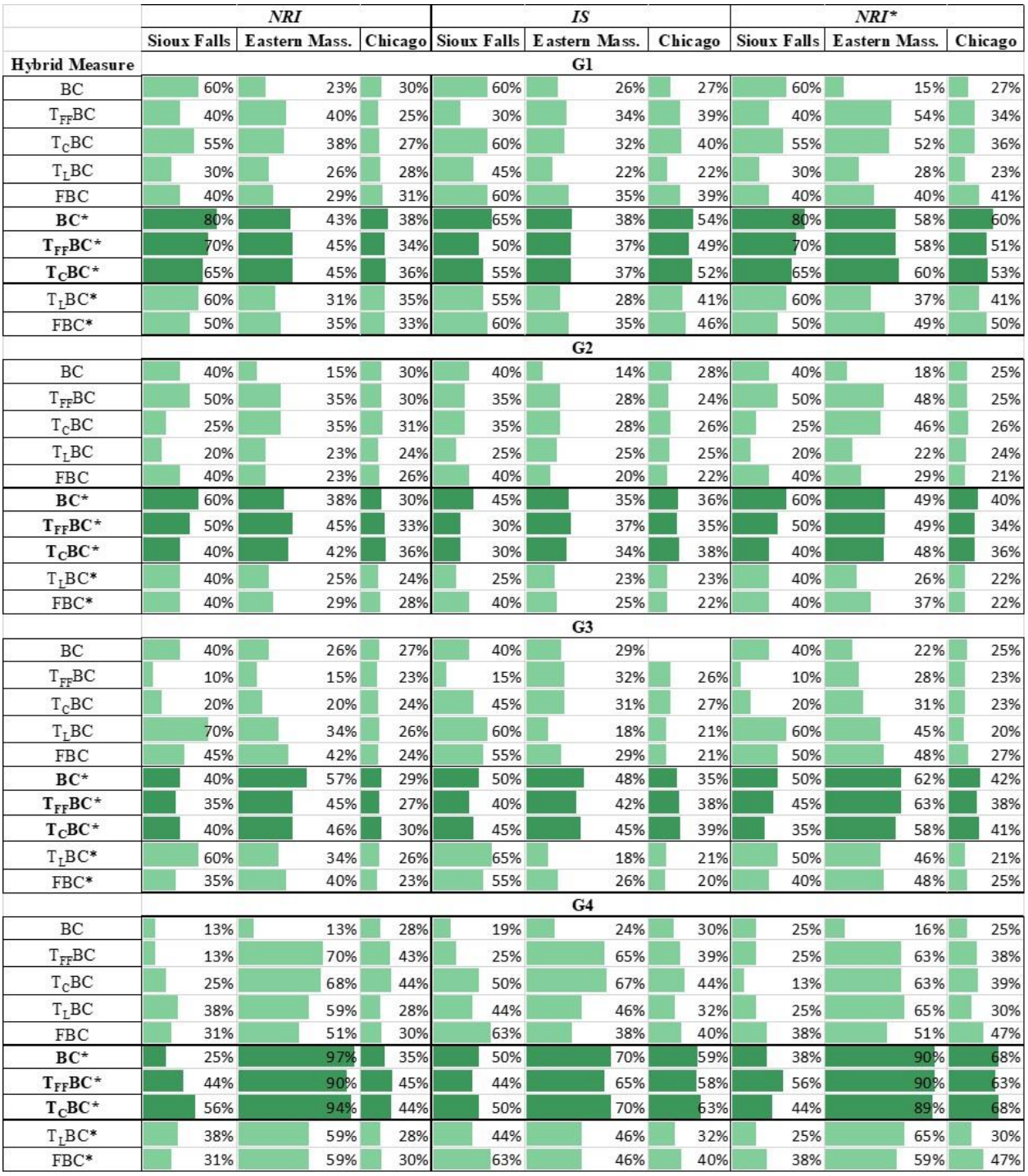
Hybrid Measures	Traffic-Based Measures								
	NRI			IS			NRI*		
	SFN	EMN	CSN	SFN	EMN	CSN	SFN	EMN	CSN
BC	0.29	-0.08	0.04	0.42	0.03	-0.01	0.33	-0.06	-0.01
T_{FF}BC	0.36	0.60	0.20	0.28	0.51	0.26	0.35	0.59	0.26
T_CBC	0.73	0.58	0.22	0.74	0.54	0.29	0.68	0.60	0.29
T_LBC	0.40	0.53	0.08	0.44	0.32	0.01	0.35	0.54	0.01
FBC	0.76	0.42	0.19	0.78	0.40	0.40	0.76	0.41	0.40
BC*	0.73	0.73	0.23	0.75	0.62	0.71	0.78	0.77	0.71
T_{FF}BC*	0.69	0.70	0.27	0.57	0.56	0.64	0.70	0.72	0.64
T_CBC*	0.87	0.70	0.28	0.82	0.58	0.69	0.84	0.75	0.69
T_LBC*	0.51	0.58	0.15	0.51	0.36	0.23	0.48	0.61	0.23
FBC*	0.81	0.53	0.21	0.79	0.45	0.48	0.81	0.54	0.48

Common Critical Links (CCL): Traffic-Based with Hybrid Measures

In addition to the Spearman's coefficient, further analysis was performed to estimate common critical links identified by both traffic-based and hybrid measures. For this analysis, links from each network were ranked based on the value of the traffic-based and hybrid measure and then were split into four sets (G1 through G4) with each set containing 25% of the links. For example, for the Sioux Fall network sets G1, G2, and G3 contained the first, second and third 20 most important links while subset G4 all the remaining links. Next, the percentage of CCL within each set between the traffic-based and hybrid measures were calculated, and results are reported in Figure 2-3. For example, for the SFN results in Figure 2-3 show that 60% of the first 20 critical links (i.e., set G1) as identified by BC are the same to the ones identified by NRI.

As part of the analysis, average percentages of CCL over all four sets were estimated for each of three case study networks. Average percentages were calculated by considering equal and unequal weights for the CCL in each set. For the unequal weight case percentages of CCL in

the first, second, and third subset were considered as four, three, and two times more important than the links in the last subset (G4), respectively (i.e., weights of 0.4, 0.3, 0.2 and 0.1 for subsets G1, G2, G3 and G4 were selected). Results are reported in Figure 2-4 where we observe that BC*, T_{FF}BC*, and T_{C}BC* provide the highest average percentage of CCL with the traffic-based measures across all three networks. These results are in line with the Spearman's coefficient analysis. In addition, it is noteworthy that unlike traffic-based measures, only one UE calculation is required to produce hybrid measures, while multiple UE are needed in the calculation of the traffic-based measures.



	NRI			*IS*			*NRI**		
	Sioux Falls	**Eastern Mass.**	**Chicago**	**Sioux Falls**	**Eastern Mass.**	**Chicago**	**Sioux Falls**	**Eastern Mass.**	**Chicago**
Hybrid Measure					**G1**				
BC	60%	23%	30%	60%	26%	27%	60%	15%	27%
T_{FF}BC	40%	40%	25%	30%	34%	39%	40%	54%	34%
T_CBC	55%	38%	27%	60%	32%	40%	55%	52%	36%
T_LBC	30%	26%	28%	45%	22%	22%	30%	28%	23%
FBC	40%	29%	31%	60%	35%	39%	40%	40%	41%
BC*	80%	43%	38%	65%	38%	54%	80%	58%	60%
T_{FF}BC*	70%	45%	34%	50%	37%	49%	70%	58%	51%
T_CBC*	65%	45%	36%	55%	37%	52%	65%	60%	53%
T_LBC*	60%	31%	35%	55%	28%	41%	60%	37%	41%
FBC*	50%	35%	33%	60%	35%	46%	50%	49%	50%
					G2				
BC	40%	15%	30%	40%	14%	28%	40%	18%	25%
T_{FF}BC	50%	35%	30%	35%	28%	24%	50%	48%	25%
T_CBC	25%	35%	31%	35%	28%	26%	25%	46%	26%
T_LBC	20%	23%	24%	25%	25%	25%	20%	22%	24%
FBC	40%	23%	26%	40%	20%	22%	40%	29%	21%
BC*	60%	38%	30%	45%	35%	36%	60%	49%	40%
T_{FF}BC*	50%	45%	33%	30%	37%	35%	50%	49%	34%
T_CBC*	40%	42%	36%	30%	34%	38%	40%	48%	36%
T_LBC*	40%	25%	24%	25%	23%	23%	40%	26%	22%
FBC*	40%	29%	28%	40%	25%	22%	40%	37%	22%
					G3				
BC	40%	26%	27%	40%	29%		40%	22%	25%
T_{FF}BC	10%	15%	23%	15%	32%	26%	10%	28%	23%
T_CBC	20%	20%	24%	45%	31%	27%	20%	31%	23%
T_LBC	70%	34%	26%	60%	18%	21%	60%	45%	20%
FBC	45%	42%	24%	55%	29%	21%	50%	48%	27%
BC*	40%	57%	29%	50%	48%	35%	50%	62%	42%
T_{FF}BC*	35%	45%	27%	40%	42%	38%	45%	63%	38%
T_CBC*	40%	46%	30%	45%	45%	39%	35%	58%	41%
T_LBC*	60%	34%	26%	65%	18%	21%	50%	46%	21%
FBC*	35%	40%	23%	55%	26%	20%	40%	48%	25%
					G4				
BC	13%	13%	28%	19%	24%	30%	25%	16%	25%
T_{FF}BC	13%	70%	43%	25%	65%	39%	25%	63%	38%
T_CBC	25%	68%	44%	50%	67%	44%	13%	63%	39%
T_LBC	38%	59%	28%	44%	46%	32%	25%	65%	30%
FBC	31%	51%	30%	63%	38%	40%	38%	51%	47%
BC*	25%	97%	35%	50%	70%	59%	38%	90%	68%
T_{FF}BC*	44%	90%	45%	44%	65%	58%	56%	90%	63%
T_CBC*	56%	94%	44%	50%	70%	63%	44%	89%	68%
T_LBC*	38%	59%	28%	44%	46%	32%	25%	65%	30%
FBC*	31%	59%	30%	63%	46%	40%	38%	59%	47%

Figure 2-3 Common critical links: traffic-based and hybrid measures

	NRI			*IS*			*NRI**		
	Sioux Falls	**Eastern Mass.**	**Chicago**	**Sioux Falls**	**Eastern Mass.**	**Chicago**	**Sioux Falls**	**Eastern Mass.**	**Chicago**
Hybrid Measure	**Average of Common Group Links Percentage (Equal Weights)**								
BC	38%	19%	29%	40%	23%	21%	41%	18%	26%
$T_{FF}BC$	28%	40%	30%	26%	40%	32%	31%	48%	30%
$T_{C}BC$	31%	40%	32%	48%	40%	34%	28%	48%	31%
$T_{L}BC$	40%	36%	27%	44%	28%	25%	34%	40%	24%
FBC	39%	36%	28%	55%	31%	31%	42%	42%	34%
BC*	51%	59%	33%	53%	48%	46%	57%	65%	53%
$\boldsymbol{T_{FF}BC^*}$	50%	56%	35%	41%	45%	45%	55%	65%	47%
$\boldsymbol{T_{C}BC^*}$	50%	57%	37%	45%	47%	48%	46%	64%	50%
$T_{L}BC^*$	50%	37%	28%	47%	29%	29%	44%	44%	29%
*FBC**	39%	41%	29%	55%	33%	32%	42%	48%	36%
	Weighted Average of Common Group Links Percentage (Decreasing Weights)								
BC	45%	20%	29%	46%	23%	22%	47%	17%	26%
$T_{FF}BC$	34%	37%	28%	28%	35%	32%	36%	48%	30%
$T_{C}BC$	36%	37%	29%	49%	34%	34%	35%	47%	31%
$T_{L}BC$	36%	30%	26%	42%	25%	24%	33%	33%	23%
FBC	40%	32%	28%	53%	30%	30%	42%	39%	33%
BC*	61%	50%	34%	55%	42%	45%	64%	59%	51%
$\boldsymbol{T_{FF}BC^*}$	54%	50%	33%	42%	41%	44%	58%	60%	45%
$\boldsymbol{T_{C}BC^*}$	52%	49%	36%	45%	41%	46%	49%	59%	47%
$T_{L}BC^*$	52%	33%	29%	47%	26%	31%	49%	38%	30%
*FBC**	42%	37%	29%	53%	31%	33%	44%	46%	36%

Figure 2-4 Common critical links Averages: traffic-based and hybrid measures

Spearman's Coefficient Evaluation

To evaluate the accuracy of the Spearman's coefficient, the average CCL percentages (reported in Figure 2-4) were regressed against the Spearman's coefficient values (shown in Table 2-7) and results are presented in Figure 2-5 (i.e., r_s against average CCL, linear fit, 95% prediction interval, and adjusted R^2 value). High adjusted R^2 values and low 95% intervals for the medium and large size case study networks (i.e., EMN and CSN) and low adjusted R^2 values and high 95% intervals for the SFN (i.e., small size network) can be observed, which was expected due to the small number of links that increases the weight of the outliers. These results showcase a strong correlation between CCL and the Spearman's Rank correlation coefficient (between traffic-based and hybrid measures), supporting the use of the latter, especially for medium to large networks where they are mostly needed.

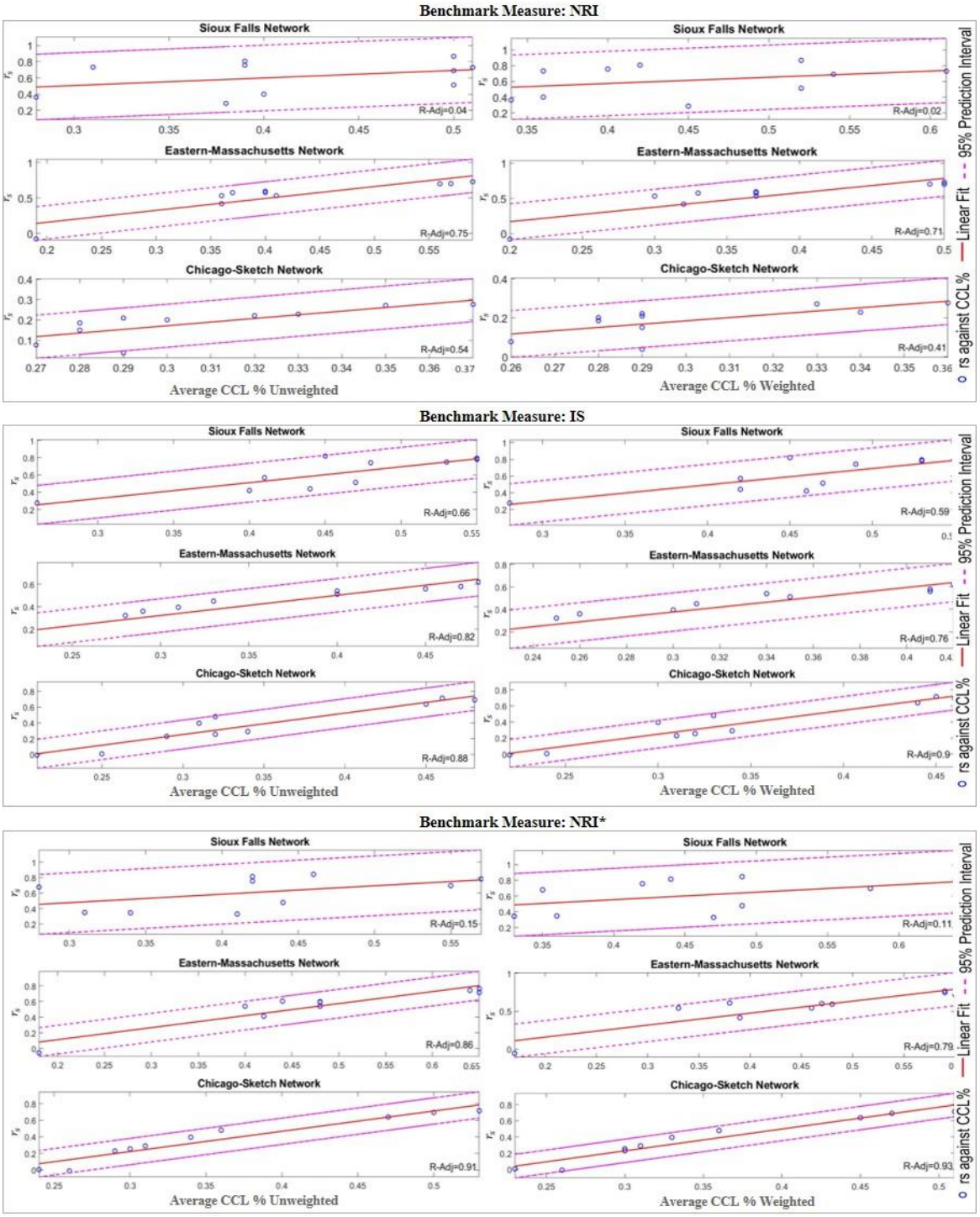


Figure 2-5 Linear fit of spearman's correlation against common critical link percentage with 95% prediction interval

Computational Time Differences: Hybrid vs. Traffic-Based

For the numerical experiments, MATLAB R2016a on a quad-core 3.5GHz CPU desktop computer with 16GB of memory was used. The traffic assignment algorithm used was the Slope-Based Path Shift Propensity Algorithm (SPSA) (44). The computational time for estimating the hybrid and traffic-based measures is shown in Table 2-8. Since each of the traffic-based measures considered all possible single link failures, their estimation requires multiple UE network estimations (as many as the number of network links plus one traffic assignment for the base case of the complete network). Hence, the computational time as compared to the hybrid measures (which only require the base network UE conditions) is significantly higher, especially for the large Chicago network.

Table 2-8 Computational Times

		Traffic-Based Measures		
Case Study Network	**Hybrid Measures**	**NRI**	**NRI***	**IS**
Sioux Falls	<1 minute	< 2 minutes		
Eastern-Massachusetts		<5 minutes		
Chicago-Sketch		~ 8 Hours		73 hours

Conclusions

In this chapter, new link criticality measures for transportation network vulnerability assessment were proposed and their accuracy was evaluated. These measures combine characteristics of traffic equilibrium and network topology to balance accuracy and computational complexity. These measures assign traffic-based weights to existing topological link criticality measures and require only running one traffic assignment in their calculation. Numerical experiments using three case study networks, commonly used in the literature as

benchmark networks, indicated that three of the proposed nine measures provide comparable results to a full-scan analysis. These three measures share the common factor of considering the direct effect of social efficiency, where if a link has more demand and is simultaneously more central, should be more critical to whole network. In addition to the social efficiency effect, the shortest path travel time (uncongested and congested situations) effect was also important and captured by the $T_{FF}BC^*$ and T_CBC^* measures. Based on $T_{FF}BC^*$ and T_CBC^*, links which are more central as compared to the others, and simultaneously has higher demand and more travel time require to commute on them (for both congested and non-congested situations), might be identified as the important links.

These three recommended measures showed promising results which can be utilized by planners and decision makers as reliable ranking measures for ranking links in large-scale road network, where due to computational burden applying the full-scan analysis is infeasible. Also, to support logistics planning analysis, they could be used to identify critical truck paths within a short space of time simply by replacing the passenger demand with freight demand (e.g., truck units or tonnage) in the estimation.

The proposed results are subjected to some limitations. The proposed method relied on a static user equilibrium which cannot capture the effects of link interaction and uncertainty of demand in the traffic assignment. Future research could focus on implementing dynamic traffic assignment and/or variable demand. Also, these proposed measures are not able to rank critical sets of links. Future research could focus on utilizing these measures in existing game theory-based models (i.e., hierarchical models) to reduce the computational efforts of user behavior modeling. Finally, research can focus on proposing new hybrid measures (by either modifying existing topological measures or combining the hybrid ones proposed in this research).

CHAPTER 3 : IDENTIFYING CRITICAL SETS OF LINKS IN A ROADWAY NETWORK UNDER DIFFERENT DISRUPTION SCENARIOS USING THE GAME THEORY FRAMEWORK

All modes of transportation are vulnerable to disruptions caused by natural disasters and/or man-made events (e.g., accidents), which may have temporary or permanent consequences. The ability to detect critical components in a transportation network is crucial for designing resilient networks and improving traffic conditions under partial or complete road disruptions. This research introduces an optimization model based on the game theory framework for identifying the most critical combination of critical links in a roadway network by considering both day-to-day and major disruptions. In this regard, various attack scenarios were defined, and the achieved outcomes were evaluated with both full scan analysis techniques and hybrid ranking measure on the Chicago-sketch network as the case study network. The findings indicate that identifying critical sets of links is highly dependent on the adversary's inelegancy, the presence of defenders, the attack's selection of links, and the disruption scenario. Additionally, this research indicates that in disruptions of multiple links, simply combining the most critical single links significantly underestimates the network's vulnerability and there is a complex correlation between critical links. The results demonstrate that the proposed model and algorithm is extremely reliable at identifying critical sets of links for random and specially targeted attacks based on the adversary's link selection in both partial and complete link closure scenarios, while significantly reducing computational complexity.

Introduction

Transportation networks serve as vital conduits for commodities and personal travel and are integral part of any society's complex freight and urban systems. Trucks are critical in inter- and intra-country freight transportation, particularly between neighboring countries. Trucks transported more than 62.9 percent of all transporter freight worth $772 billion in 2019 (45). Roads, which accounted for 87 and 91 percent of daily and work trips, respectively, are considered as the primary mode of personal travel in the United States in 2017 (46). As a result, robust transportation networks, particularly roadway systems, have been regarded as a requirement for economic growth and a high standard of living (47). Along with improvements in the transportation network's efficiency and design to operate at its near-maximum capacity over the last few decades, the vulnerability and sensitivity of this infrastructure system to various types of disruption has increased.

The fundamental objective of vulnerability analysis can be subdivided into numerous sub-objectives. One critical component of this analysis is identifying critical components of the network where certain incidents may have severe consequences (5). When it comes to road management, decision makers frequently employ quantitative methods to assess this infrastructure. Vulnerability analysis and identifying critical components of the road network may assist road authorities and agencies in identifying vulnerable segments of the road network prior to disruption. This knowledge is beneficial at both planning and operating stages, as it assists to focus on efforts to improve and maintain these critical connections.

The remainder of the chapter is as follows: The next section summarizes the relevant literature, followed by a section explaining the proposed methodology. The fourth section presents and discusses the results of a series of numerical experiments using a well-known case

study network. The final section of the chapter summarizes the findings and discusses the limitations of the proposed methodology as well as future research directions.

Literature Review

The general research methodology used by vulnerability researchers consists primarily of three key stages including mode of transport, definition of a disruption scenario, and analysis method. These stages are briefly explained here:

Mode of Transport

Each mode of transportation has a distinct research methodology and vulnerability characteristics. For instance, an approach developed and designed for a road network cannot be applied directly to a subway system, which is a capacity-constrained and frequency-based system with more significant interrelationships of tracks and stations than a road network (48).

Definition of a Disruption Scenario

A disruption is defined by a number of parameters, including the degree of degradation (full or partial closure), the number of components degraded (single or multiple segments), and the source of the disruption (internal or external threats). Internal threats include incidents caused by users or maintenance services, while external threats include natural disasters such as earthquakes, floods, adverse weather, and hurricanes. A disruption scenario is defined as simulating a disruption with these specific parameters on a particular link (Burgholzer et al. 2013).

Analysis Method

There are two broad categories of vulnerability analysis methods: I) vulnerability measures and II) optimization models.

I) Vulnerability Measures

Measuring the vulnerability of a network is highly dependent on the type of performance function defined for the transport system (49). Smooth traffic mobility, travel expenses (such as travel time, or a combination of different costs) are essential performance measures for roadway networks. Numerous research has established a variety of measures for assessing the vulnerability of systems and evaluating the network's components (6,20,23,30,35). The value of the vulnerability measure will be utilized to quantifying the impact of the disruption on the network and evaluating the system performance. Mattsson and Jenelius (8) classified vulnerability measures into two distinct categories; topological-based and traffic-based.

In topological-based analysis, the graph’s topological characteristics such as the degree of distribution, cluster, centrality measures, and efficiency are used to rank the nodes and links in the network (10,11,13,16,17). This kind of analysis only considers the structure of the network without considering the user’s behavior in the calculation procedure.

The most often used approach in the literature is full-scan analysis, which considers the system's performance in both normal and abnormal conditions (6,18,20,23,29,32). This approach simulates removing each link iteratively and measure its impact on the network performance (travel time, generalized cost, flow, etc.) and the links are ranked according to their impact on the values of the investigated measures. According to (8,9), the ranking measures proposed using the full-scan analysis are referred to as traffic-based vulnerability measures. While traffic-based measures are capable of identifying critical links in a network in reliable way (36), their

calculation requires undertaking traffic assignment under all possible disruption scenarios, resulting in computationally infeasible measures for use on large-scale networks.

A few studies have been published trying to incorporate traffic assignment characteristics (e.g., flow, travel time, etc.) into existing topological measures (e.g., centrality measures, efficiency, etc.) and developing new criteria called hybrid measures (9,35,50). This approach aims to reduce computational and time requirements while retaining accuracy in ranking the critical links in transportation networks.

II) Optimization Models

According to the comprehensive research performed by Khademi et al. (51), most of the studies on transportation network vulnerability/resilience include only a single link failure. However, in real-world road network situations, multiple links are typically affected during disruptions, and single link failures can cause misleading when multiple correlated (cascading) and uncorrelated disruptions occur, as they do not capture the network-wise effects of such a large disruption event (40). The significant computational burden is the main issue in systematic nodes/links removal in full-scan vulnerability analysis of a real large-scale network which may only be possible/realistic for single-link/node removal (9,50). Mathematical optimization models are the best approaches for vulnerability analysis of large-size networks in the face of complex disruption scenarios (52). This research proposes an optimization model in a hierarchical game theory platform which is adopted with both topological-based and traffic-based analysis.

There are two main components considered by game theory models which are discussed in this section: the players and the formulation. The players are the different viewpoints of the game each with their own objective which describe as follows. The formulation is how the game is arranged which includes who goes first, how many moves can that player make, etc.

Players of the Game

In transportation networks, there are multiple different viewpoints to consider that collectively determine the performance of the networks. These viewpoints fall into three different categories: decision makers (defender), threats (adversary), and network users. This part of the review is focused on the definition, consideration, and interactions of these three viewpoints.

1. Decision Makers

Decision makers are responsible for the maintenance, expansion, protection, and operation of a transportation network. It is also the responsibility of the decision maker to optimize for the benefit of the network users. This translates into the decision maker pursuing the global good by considering the benefits and detriments to all users simultaneously. Also, decision makers have a large constraint placed upon them in the form of a budget. Budgets limit the number and magnitude of the actions that a decision maker can make. In reference to a transportation network, the actions available to a decision maker include the following: construct a new link, perform maintenance on a link, and expand a link. These actions focus on the building blocks of networks, links, thus the complexity of the problem is dependent upon the number of links that compose the network.

2. Intentional or Unintentional Threats

Adversary to a transportation network can be considered as anything that will negatively impact performance. The two categories, intentional and unintentional, differ in those intentional threats select their impact while unintentional threats are random or must follow certain rules. For example, a terrorist can carefully plan an attack on a specific link of a network while a flood can only affect links that are within the flood plain during periods of heavy rain. This example

highlights those intentional threats are intelligent and can carefully choose actions for the optimal or largest impact on the network.

Intentional Threats

Intentional threats, listed in Table 3-1 are deliberate attacks on a network with a clear goal of disrupting the network. Unlike unintentional threats, intentional threats are intelligent and attempt to exploit known vulnerabilities. Construction on roadways falls into this category because it is an intentional intelligent action that can temporarily lower performance on a network. This also creates a paradox where in order to protect certain infrastructure against vulnerability, construction must create a temporary vulnerability.

Transportation networks are a common target of attacks due to being economic pipelines that are crucial to the movement of people, goods, and services from one place to another. The damage or destruction of transportation infrastructure can have wide-spread detrimental effects, thus making a very desirable target for an attack.

Table 3-1 List of Intentional Threats

Threat	Description
Terrorist Attack (53,54)	A terrorist attack is a very focused and deliberate attack to damage or destroy a particular infrastructure
Construction (55)	Partial or full road closures are very common occurrences when maintaining or improving roadways

Unintentional Threats

Unintentional threats usually pertain to the consequences of human error, or the damage caused by acts of nature. Human errors like negligence and traffic accidents can have drastic consequences for a network. This research distinguishes between weather events (rain, snow,

etc.) and natural disasters (earthquake, hurricane, etc.) by considering that weather events occur often, and natural disasters are rare. Extreme weather events can be classified as natural disasters because they present dangers that are on the same scale as other natural disasters. For example, excessive rainfall can cause flooding that can wash away roadways and excessive snowfall can prevent roadways from being used safely.

Weather Events

Table 3-2 provides a small list of weather events that can be detrimental to a transportation network. All of these events lower the coefficient of friction for the roadway thus making it slippery and more dangerous. Rain will immediately drain off of the road unless it pools which can lead to hydroplaning of vehicles. Snow and ice can pile up thus blocking the roadway until it is removed.

Table 3-2 List of Weather Events

Weather Event	**Description**
Rain (56)	Precipitation in the form of liquid water
Snow and Ice (57,58)	Precipitation in the form of frozen water

Natural Disasters

Natural disasters have been responsible for billions of dollars of damage in the United States. The total cost of U.S. billion-dollar disasters from 2016 to 2020 exceeds $600 billion. These disasters included: hurricanes, droughts, severe local storms, non-tropical floods, winter storms, wildfires, and freezes. There are many other natural disasters (listed in Table 3-3) that are destructive but are not designated as billion-dollar disasters.

Table 3-3 List of Natural Disasters

Natural Hazard	Description
Earthquakes (59,60)	The sudden release of energy in the Earth's crust that creates seismic waves
Volcanic Activity (61)	This can be an eruption or lava flow associated with an active volcano
Sea Level Rise (62)	The gradual rise of sea level over time (8 inches in the past century)
Flooding (60,63)	An overflow of water that submerges land that is typically dry
Tsunamis (63)	A sea wave caused by the displacement of a large volume of a body of water.
Hurricane (64)	A large tropical storm system with high-powered circular winds
Tornado (65)	A funnel cloud of violently rotating winds
Wildfires (65)	A large, destructive fire that spreads quickly
Blizzard (65)	A severe snowstorm with high winds and low visibility

Human Related Events

Humans can make choices that have unintended consequences for the performance of a roadway network. Table 3-4 lists the events that fall under unintended consequences of human actions. In the worst of cases, improper maintenance of a bridge can led to a collapse as was the case for I-35 W in Minnesota. Traffic accidents are much more common than bridge failures with 10.8 million crashes occurring in 2009.

Table 3-4 List of Human Error Events

Human Error	Description
Traffic Accidents (66)	Traffic accidents can result in temporary partial or full road closures leading to unexpected delay in a network.
Improper Maintenance (67)	Improper maintenance can result in failures that can be catastrophic in some cases (Minnesota Bridge)

3. Network Users

There are many different types of network users (cars, trucks, emergency vehicles, buses, etc.), but they all have the same goal of using the network to travel from an origin to a destination. While achieving that goal, there are multiple potential routes to choose from which requires a decision on which to use. There are a number of different objectives that the users can try to maximize or minimize (travel time, gas consumption, user cost, etc.), but the chosen route represents the most valuable to the user. Network users are inherently selfish due to the fact that they only know how their route decision affects themselves without any information available about how that decision may affect others.

Game Theory Formulations

The field of game theory covers a wide variety of applications and thus includes a wide array of formulations to match these applications. The formulations consist of three main parts: communication between the players, order of play, and amount of information. The communication between the players can be considered as cooperative or non-cooperative. Transportation networks are typically non-cooperative where the players cannot make agreements with each other about how they will play the game. The order of play can be simultaneous, all players choose an action at the same time, or sequential, one player chooses an action then another player chooses an action. The amount of information can be considered as perfect or imperfect and refers to the knowledge of the actions of other players in sequential games. Attacks on transportation networks are primarily sequential games and thus the focus of this section is the various formulations of sequential games.

Game theory as a tool to assess the transportation network vulnerability began by Bell (68) who proposed a mixed strategy non-cooperative game with two players: i) the network users who are attempting to find the paths of minimum travel costs, and ii) an evil entity imposing link costs on the user to maximize the expected trip cost. MurrayTuite and Mahmassani (25) developed a bi-level model and considered four different scenarios involving an adversary and the traffic management agency trying to identify the most vulnerable links in the network. To evaluate the vulnerability of a system Lownes et al. (69) used a mixed-strategy stochastic game-theoretical model and applied it to the Sioux Falls network. Their method was designed to incorporate all Origin-Destination (ODs) pairs computational efficient and to design a game between a user seeking minimum cost paths for travel as well as adversary seeking to maximize travel cost by disabling links in the network.

Yates and Sanjeevi (28) developed the shortest path network interdiction problem (bi-level problem) and modeled the network as a two-player game for analyzing attacks on critical infrastructure and a subset of the California highway network was used to test the model. A global optimization framework for identifying the most combination of critical links was presented by Wang et al. (3). Their findings indicate that the crucial combination of vulnerable links is not necessarily connected or even placed in neighborhood of each other. Higgs et al. (27) used a multi-level multi-objective framework to identify vulnerable routes in a network. To tackle the problem of dimensionality, each level was converted to a single objective using the weighted sum technique with weight determination based on heuristic methods. To find the most important sets of links where losing them will lead to the highest total travel cost, Starita (40) formulated a game theoretical model as a bi-level problem and applied it to the roadway networks of Sioux Falls and Berlin. According to their results, when multiple link disruptions are

considered, optimization methodologies outperform existing vulnerability measures assessment techniques.

What Is Missing in the Literature?

To overcome the time-consuming issue of vulnerability evaluation, most of the studies related to the transport network vulnerability/resilience analysis only consider a single link failure. However, in real-road network situations, more than one link is involved during disruptions (70). Another concern in the majority of the vulnerability analysis studies is the capacity reduction level which was first raised by Sullivan et al. (24). The capacity reduction level is defined as the reduction in link's capacity and is expressed as a fraction of the original capacity. In most studies, the vulnerability of a network is assessed for only full disruption of the link (12,18,20,23,34) which results in inaccurate reflection of frequent minor events and day-to-day accidents such as the closure of several lanes in a path due to car accidents or adverse weather.

To address these two main issues in road-way vulnerability analysis, a heuristic solution algorithm focusing on worst-case scenario is presented in this research which is capable of identifying the critical sets of links under different disruption scenarios including both full and partial links closure by using only one traffic assignment. A worst-case scenario is the most critical sets of links with respect to a specific performance criterion, which is modeled as a game between three players. The upper-level player (defender) can be defined as public entity which is responsible for the maintenance and operation of the network. The second level player (adversary) can be defined as anything (or anyone) which can degrade the network performance and is classified into two categories: intelligent and non-intelligent. The lower-level players are road users, whose behavior and rout decision in a congested network are modeled based on the

User Equilibrium (UE) assignment model based on the first Wardrop principle. According to the assumption in Wardrop's first principle, travelers always choose the path with the least travel time, which is calculated through the Bureau of Public Roads (BPR) function (39). These equilibrium constraints can guarantee that no user can improve their travel time by unilaterally changing routes. Since both the first and second level objective functions are the same, a min-max formulation is used to reduce the problem from a tri-level to bi-level problem or interdiction problem (65,71).

Methodology:

In this section the mathematical formulation used to identify and rank the group of critical and vulnerable links in a roadway network is presented. This formulation can assist decision makers in developing an optimal investment strategy to maximize the network's resilience to attacks. The product of traffic flows and travel time has been considered as the system's cost. The presented methodology covers two distinct game frameworks: 1) Adversary-User and 2) Defender-Adversary-User. The Adversary-User configuration optimizes the adversary's strategy and finds the most critical links in the absence of defender action. The configuration of Defender-Adversary-User reduces the adversary's efficiency by defending the network. In both frameworks, the lower level is the UE traffic assignment, which enables the model to account for the effect of congestion on drivers' route choice (39). A bi-level UE based model is used to formulate both games. The bi-level formulation models the relationship between the network manipulated by defender and adversary at the upper-level, and the users at the lower-level problem.

The nomenclature followed by the mathematical formulation for the Bi-Level User Equilibrium (BLUE) are listed as follows.

Nomenclature

Sets	Description
A	Set of links
N	Set of nodes
R	Set of origins
S	Set of destinations
K_{rs}	Set of paths between origin r and destination s
Variables	
x_a	Traffic flow on link $a \in A$
y_a	Binary decision to either do nothing (0) or defend link $a \in A$ (1)
z_a	Binary decision to either do nothing (0) or attack link $a \in A$ (1)
B^D	Number of links that can be defended
B^A	Number of links that can be attacked
$t_a(x)$	Link travel time function
q_{rs}	The demand for travel from origin $r \in R$ to destination $s \in S$
F_k^{rs}	The traffic volume for path $k \in K_{rs}$ between origin $r \in R$ to destination $s \in S$
δ_a^{krs}	The binary path incidence for link $a \in A'$ if it belongs to path $k \in K_{rs}$ between origin $r \in R$ to destination $s \in S$ (1) or not (0)

Mathematical Model for the BLUE:

$\underset{y,z}{\text{Minimize}} \ \sum_{a \in A} x_a t_a(x)$ (Equation 1)

s.t.

$\sum_{a \in A} y_a \leq B^D$ (Equation 2)

$y_a = \begin{cases} 1, \text{if link a is defended} \\ 0, \text{otherwise} \end{cases}$ (Equation 3)

s.t.

$\underset{y,z}{\text{Maximize}} \ \sum_{a \in A} x_a t_a(x)$ (Equation 4)

s.t.

$\sum_{a \in A} z_a \leq B^A$ (Equation 5)

$z_a = \begin{cases} 1, \text{if link a is attacked} \\ 0, \text{otherwise} \end{cases}$ (Equation 6)

s.t.

$\min_x \sum_a \int_0^{x_a} t_a(x) dx$ (Equation 7)

s.t.

$\sum_k f_k^{rs} = q_{rs} \quad \forall r \, R \, and \ s \in S$ (Equation 8)

$f_k^{rs} \geq 0 \qquad \forall k \in k_{rs}, r \in R, s \in S$ (Equation 9)

$x_a = \sum_{k,r,s} \delta_a^{krs} f_k^{rs} \quad \forall a \in \mathrm{A}$ (Equation 10)

Equations (1) through (3) represent the upper-level problem (i.e., defender) within the constraint which limit the number of links that can be defended to a fixed number (equation 2). In equation (3), the decision of the upper-level player is shown to be binary, with 1 indicating that link a is defended and 0 indicating that link a is not defended. In equation (4), the second level player (i.e., adversary) maximizes its own objective function (which in this research it is considered similar to the case with the defender) within the constraints of the total number of links that can be attacked (equation (5)). In equation (6), the decision of the adversary is shown to be binary where 1 is an attack on link a and 0 is no attack on link a. The third and lower-level player (i.e., network users) minimizes the integral of the link travel times in equation (7) within constraints of equation (8) and equation (9) which yields to the user equilibrium. Constraint equation (8) ensures that the sum of traffic flows on the paths between origin *R* and destination *S* is equal to the demand. Constraint equation (9) ensures that the traffic flows on the paths are non-negative. The traffic flow on each link is defined in equation (10) as the sum of the path flows for paths containing that particular link.

Solution Algorithms:

The network interdiction problem is classified as NP-hard problems by Wood (72), where there is no available exact solution. Therefore, different heuristic and meta-heuristic approaches have been introduced by researchers to solve these types of problems. To solve BLUE, we proposed a greedy search based heuristic algorithm by utilizing a subcase of the optimization model developed by Higgs et al. (27) and making locally optimal solutions at each step. At the proposed algorithm in this research which we will refer it from now as Vulnerability Greedy Search Based (VGSB) algorithm, the defender of the network search over the best possible solutions for increasing the resilience of the network and the adversary moves after the defender

and search to find the most critical links on the network which degrading them will lead to highest cost increase in the network. The algorithm builds tentative solutions to defend and attack by using different link selection methods and update the sets at each stage to reach the most promising links. So, at each iteration of the algorithm, a subset of links is selected to be defended by different defended efficiency to simulate full and partial defense in the network. Then, a subset of links is selected to be attacked to simulate both intelligent and non-intelligent adversary. The selected links' capacity will be reduced (by a predetermined percentage) to model both major and minor disruptions, and the total cost of the new network will be estimated using a shortest path assignment method. The algorithm terminates after a predetermined number of iterations has been reached (which varies according to the network's size and PC's computing power). To cover wide variety of attack strategies, four different disruption scenarios have been defined in applying VGSB in identifying critical sets of links. In order to evaluate the accuracy of the proposed solution algorithm, the achieved results are compared with three full-scan analysis measures.

Studied Disruption Scenarios:

To simulate different actions of adversary, four different scenarios are considered. These scenarios are summarized in Table 3-5 and details of each scenario is explained as follows.

Table 3-5 Studied Disruption Scenarios in the Absence of Defender

Scenario's name	Source of Attack		Degree of Closure	Number of disrupted links (DL)
S_{RF}	Random Attack (non-intelligent adversary)		Full Closure	Multiple links (ML)
S_{RP}			Partial Closure	
S_{TF}	Targeted Attack (intelligent adversary)	1: *V/C*	Full Closure	
		2: *BC**		
S_{TP}		3: $T_{FF}BC^*$	Partial Closure	
		4: $T_{C}BC^*$		

Source of Attack:

Both targeted and random attacks are considered in link disruption strategies. In random strategy, based on conducting a Monte Carlo simulation, links will be disrupted randomly (which can model the case of a non-intelligent adversary) while in targeted strategy (which can model the case of an intelligent adversary), links will be disrupted based on the four different rank ordered measures (i.e., volume to capacity ratio and three hybrid measures proposed by Takhtfiroozeh et al. (50)). Therefore, links with higher rank order are more prone for attacks by the adversary and this can be a representer for the intelligent adversary. The four link selection measures used in this research to select sets of links to be attacked based on the defined scenarios are explained as follow.

Link Selection Measures in Targeted Attack

- Link Volume-to-Capacity Ratio Ranking Measure (*V/C*): For each link the V/C ratio is estimated as the ratio of the traffic flow to the capacity of the link.
- Hybrid Link Ranking Measures: Takhtfiroozeh et al. (50) considered traffic equilibrium inputs and outputs in calculating Betweenness Centrality (BC) measure. They modified BC to consider both centrality and traffic attributes in ranking the links, and proposed three hybrid measures (i.e., *BC**, $T_{FF}BC^*$, and T_cBC^*). *BC* (equation (11)) was initially introduced by Freeman (37), and is a topological measure which has been applied to a wide range of graph theory problems. For a link, the value of BC expresses the frequency the link falls on the shortest paths connecting pairs of nodes.

$$\boldsymbol{BC(a)} = \sum_{s,t} \frac{\sigma_{st}(a)}{\sigma_{st}} \qquad \text{(Equation 11)}$$

where $\sigma_{st}(a)$ is the shortest path from node *s* to node *t* that traverses link *a*, and σ_{st} is the number of the shortest paths from node *s* to *t*. The formula, variables, and description of each hybrid measure are presented in Table 3-6.

Table 3-6 Selected Hybrid Ranking Measures

Name	Formula	Variables	Description
Flow Weighted BC (*BC**)	$BC^*_a = F_a * BC_a$	BC_a = Betweenness Centrality of link a F_a=Flow of link a	This measure, makes sure that a links with more centrality and more demand to serve are defined as important links in the network.
Flow Weighted Free Flow Travel Time BC ($T_{FF}BC^*$)	$T_{FF}BC^*_a = F_a * T_{FF}BC_a$	T_a^{FF}=Free Flow Travel Time of link a $T_a^{FF}=\frac{L_a}{FFS_a}$ FFS_a=Free Flow Speed of link a L_a=Length of link a	To capture the UE principle in an uncongested network, in computing the shortest path used in the BC calculation, edges were weighted by their Free Flow Travel Time (FFTT). This measure can be effective in identifying critical links in uncongested conditions. Also, for considering the social efficiency, flow of the links considered as an extra weight in calculating this measure.
Flow Weighted Congested Travel Time BC (T_CBC^*)	$T_CBC^*_a = F_a * T_CBC_a$	T_a^C= Travel Time of link a $T_a^C = T_a^{FF}\left[1+\alpha(\frac{F_a}{C_a})^\beta\right]$ F_a=Flow of link a C_a=Capacity of link a α & β =Model parameters	To capture user behavior in the BC calculation, congested travel time has been used as a weight for links in the shortest path calculation. also flow of the links for considering the social efficiency effect is applied as an extra weight in calculating this measure.

Degree of Closure

To analyze the performance and criticality of the link depending on the attack efficiency, four different capacity reductions (C_r) were considered. C_r = {100%} were considered to simulate full closure due to major events and three different capacity-reduction levels denoted as C_r = {40%, 60%, 80%} were considered to simulate partial closure due to day-to-day disruptions in the roadway network.

Number of Disrupted Components

Most of the studies related to the transport network vulnerability/resilience analysis consider only a single link failure. However, in real road network situations, usually more than one link is affected due to the disruptions. In this regard, scenarios are arranged based on considering different sets of links to be compromised (DL=10, 20, 30, 40, and 50 links).

Studied Defender Strategies

In Defender-Adversary-User framework, to investigate the effect of different strategy that defender might chose to defend the network, two defense levels (partial and full defend) were studied. The effect of 50% defense effectiveness as the partial defense strategy and 100% defense effectiveness (i.e., if a link is fully protected, the attack will have no effect on it) as the full defense strategy were considered. This research assumed that the defender based on the defense budget will protect the specific number of links which recognize by the link selection measure as the top critical links.

Selected Traffic-based Vulnerability Measures for Evaluation Process

For evaluating the presented methodology, the results of BLUE compared with three traffic-based criticality measures (the Network Robustness Index (NRI) (23), Link Importance Measure (7), and Modified Network Robustness Index (NRI^*) (32)) were chosen from the available literature. NRI measures rank the links based on calculating the difference in network's total travel time before and after a link is removed from the network by running traffic assignment in each iteration. While on the other hand, NRI modified, utilizes the difference of product of demand and travel time before and after the link removal from the network as the performance function. IS were derived based on the increase in the generalized cost of travel in degraded networks considering social efficiency by weighting the travel cost by travel demand. A brief description of these three measures is presented next and the formulas of each measure are shown in Table 3-7.

All these three measures use the full scan analysis methodology for ranking links where links are removed one by one, and a performance measure (usually a function of travel time) is calculated in each step, and the links are ranked based on the changes in value of the selected

measure. Most of the published research in roadway vulnerability assessment have used at least one of these three measures as benchmarks (9,36,40) as they are extremely accurate, albeit time consuming and not applicable for full-scan analysis on large-scale networks. Estimation each of the mentioned traffic-based measures requires multiple UE network estimations (as many as the number of network links plus one traffic assignment for the base case of the complete network).

Table 3-7 Selected Traffic-based Criticality Measures and Their Performance Function.

Name of the Measure	**Study**	**Formulation**	**Description**	**Performance Function**
Network Robustness Index (NRI)	Scott et al. (23)	$NRI_a = C_a - C_0$	C_0: network travel time when all links are present in the network. C_a: network travel time when link a is removed	Travel Time
Link Importance (IS)	Jenelius et al. (20)	$Is_a = \frac{\sum_i \sum_{j \neq i} x_{ij} \, (C_{ij}^a - C_{ij}^0)}{\sum_i \sum_{j \neq i} x_{ij}}$	x_{ij}: Travel demand between origin *i* and destination *j* C_{ij}^0: Travel time from origin *i* to destination *j* when all links are present in the network C_{ij}^a: Travel time from origin *i* to destination *j* when link *a* is removed from network	Travel Time × Flow
Modified Network Robustness Index (NRI^*)	Sullivan et al. (24)	$NRI_a{}^* = \sum t_i^a x_i^a - \sum t_i \, x_i$	x_i^a: travel demand on link i when link a is removed and network is re-routed t_i^a : system travel time on link i when link a is removed t_i : base system travel time	Travel Time × Flow

Numerical Experiment

To evaluate the proposed algorithm, the Chicago Sketch transportation network which is commonly used in the literature for testing different algorithms and models for transportation

networks was used. The Chicago sketch network contains 933 nodes, 387 zones, and 2950 links where all its network data are obtained from (43).

Comparison with the traffic-based measures:

Figure 3-1 through Figure 3-5 present the average percentage difference between the BLUE generated system's cost and the cost of NRI, NRI*, and IS for each attack scenario. The total UE system's cost for the three traffic-based measures was determined by sequentially disrupting each link defined in the first 100 critical sets of links according to the priority order identified by BLUE. The Compared costs were normalized by their corresponding base costs, which are defined as the network costs when no link in the network has been attacked.

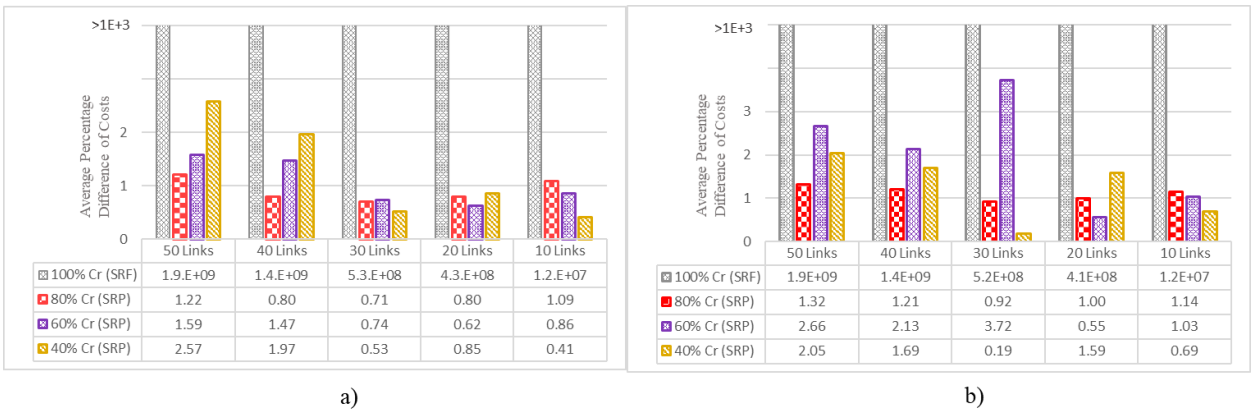


Figure 3-1 Average Percentage Difference for Different Costs under Random Attack Scenarios

a) Average Percentage Difference Between NRI and BLUE Performance Function
b) Average Percentage Difference Between NRI* and BLUE Performance Function
c) Average Percentage Difference Between IS and BLUE Performance Function

The VGSB algorithm does not perform well in the situation of a random attack for full closure, as seen in Figure 3-1. However, the difference between BLUE, NRI, NRI*, and IS performance functions are minimal in the case of partial closure for all DLs (i.e., 10, 20, 30, 40, and 50 links per set). These small differences in the costs indicate that disrupting links classified as critical by BLUE causes as much as cost when they will be disrupted by full-scan analysis methods. Based on these findings, it can be stated that when a non-intelligent adversary with partial link closure is considered, the proposed methodology performs well in identifying the critical sets of links.

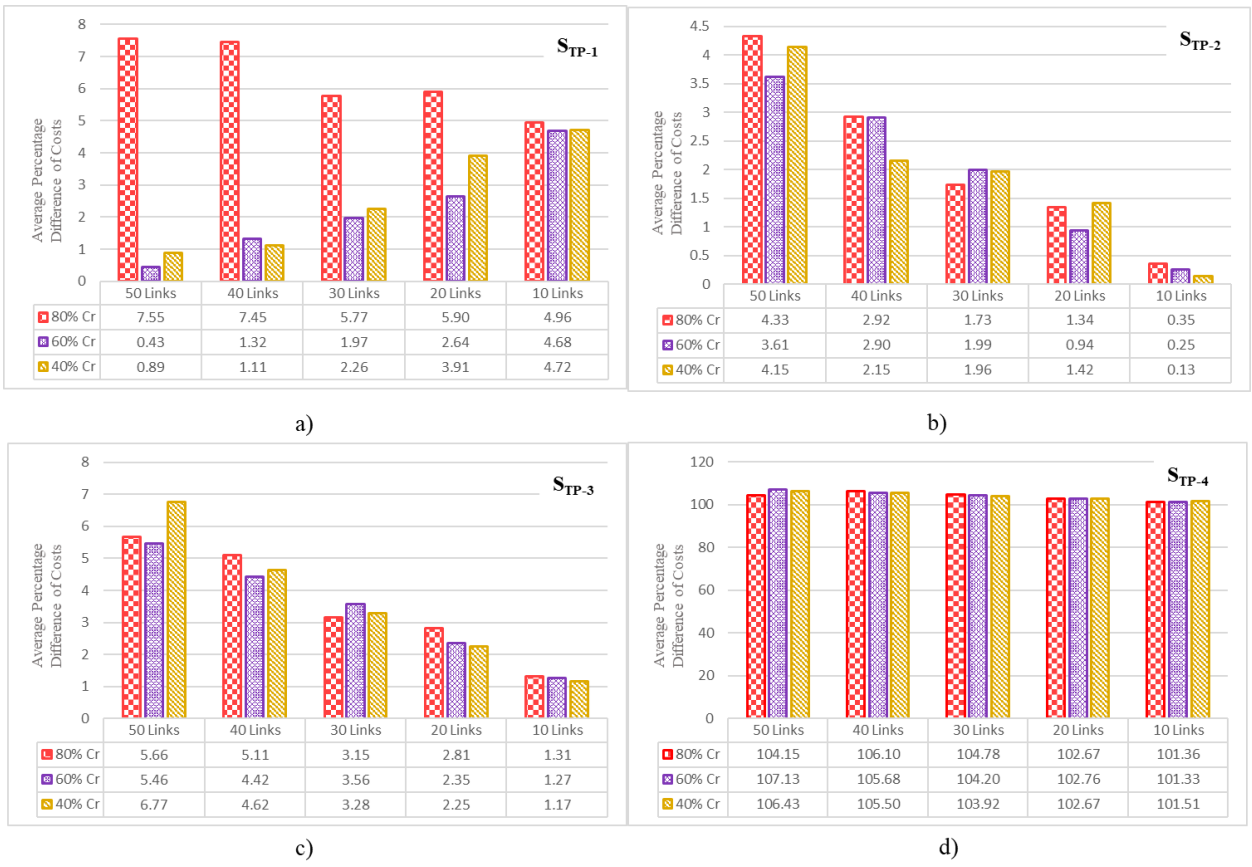


Figure 3-2 Average Percentage Difference Between NRI's and BLUE's Performance Function

a) Scenario $S_{TP\text{-}1}$: Link's Partial Closure, Targeted Attack, Link Selection *V/C* ratio
b) Scenario $S_{TP\text{-}2}$: Link's Partial Closure, Targeted Attack, Link Selection *BC**
c) Scenario $S_{TP\text{-}3}$: Link's Partial Closure, Targeted Attack, Link Selection $T_{FF}BC^*$
d) Scenario $S_{TP\text{-}4}$: Link's Partial Closure, Targeted Attack, Link Selection $T_{C}BC^*$

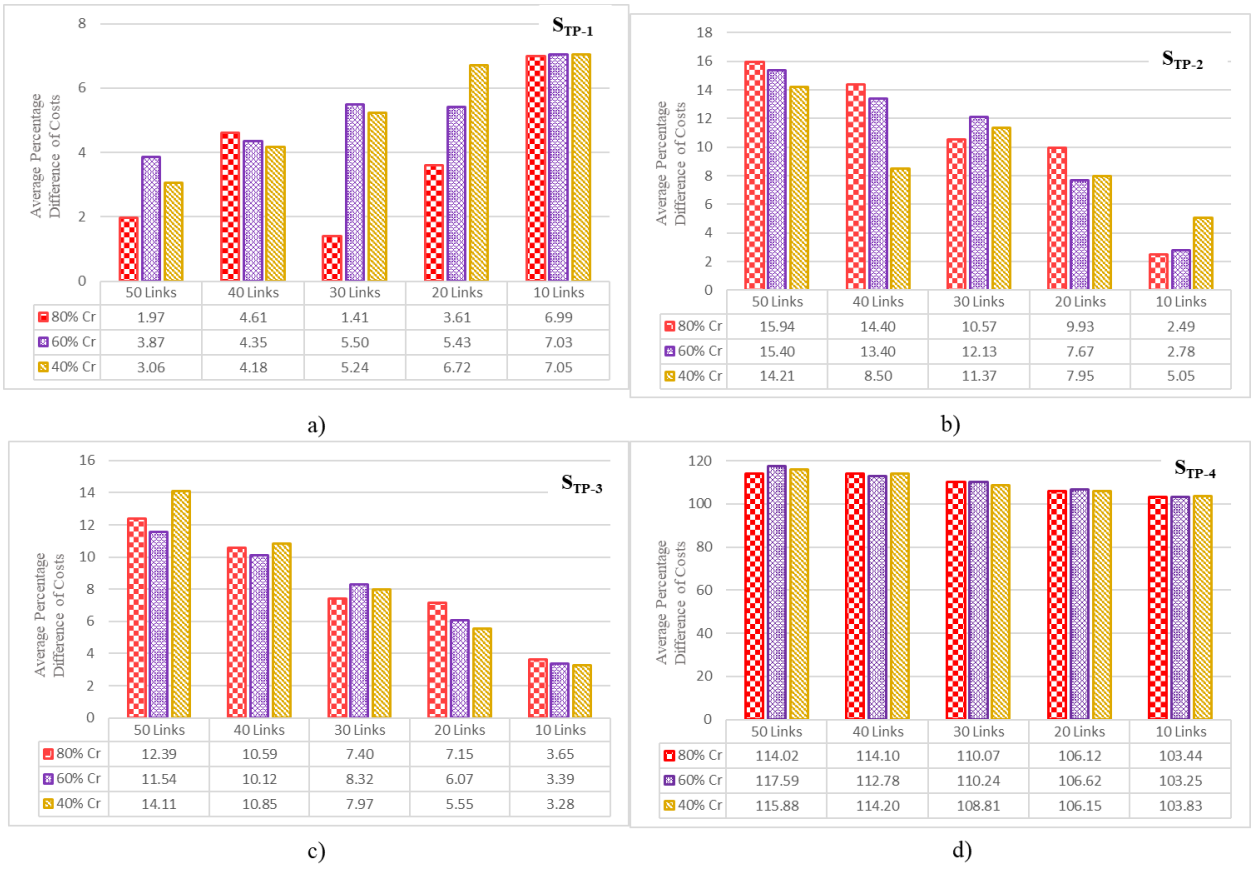


Figure 3-3 Average Percentage Difference Between NRI*'s and BLUE's Performance Function

a) Scenario S_{TP-1}: Link's Partial Closure, Targeted Attack, Link Selection *V/C* ratio
b) Scenario S_{TP-2}: Link's Partial Closure, Targeted Attack, Link Selection *BC**
c) Scenario S_{TP-3}: Link's Partial Closure, Targeted Attack, Link Selection $T_{FF}BC^*$
d) Scenario S_{TP-4}: Link's Partial Closure, Targeted Attack, Link Selection T_CBC^*

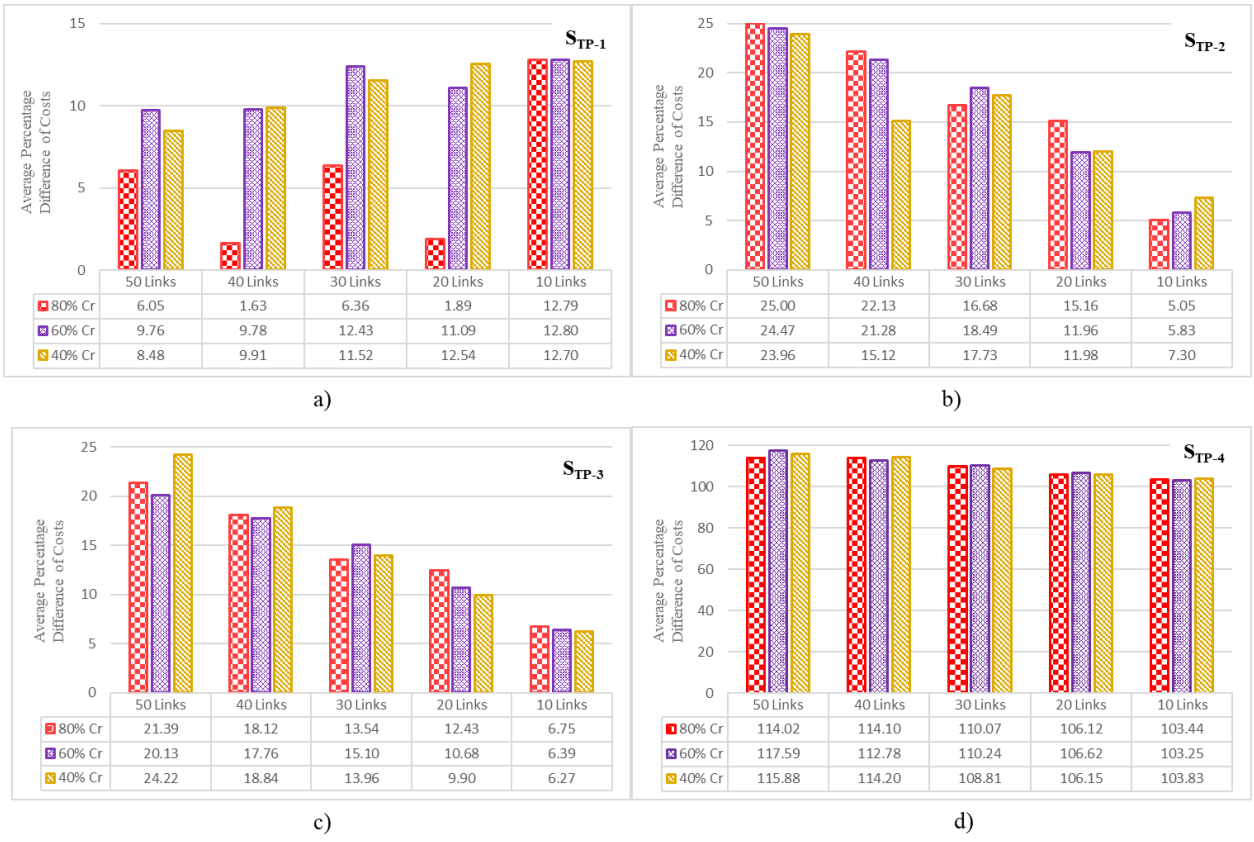


Figure 3-4 Average Percentage Difference Between IS's and BLUE's Performance Function

a) Scenario $S_{TP\text{-}1}$: Link's Partial Closure, Targeted Attack, Link Selection *V/C* ratio
b) Scenario $S_{TP\text{-}2}$: Link's Partial Closure, Targeted Attack, Link Selection *BC**
c) Scenario $S_{TP\text{-}3}$: Link's Partial Closure, Targeted Attack, Link Selection $T_{FF}BC^*$
d) Scenario $S_{TP\text{-}4}$: Link's Partial Closure, Targeted Attack, Link Selection $T_{C}BC^*$

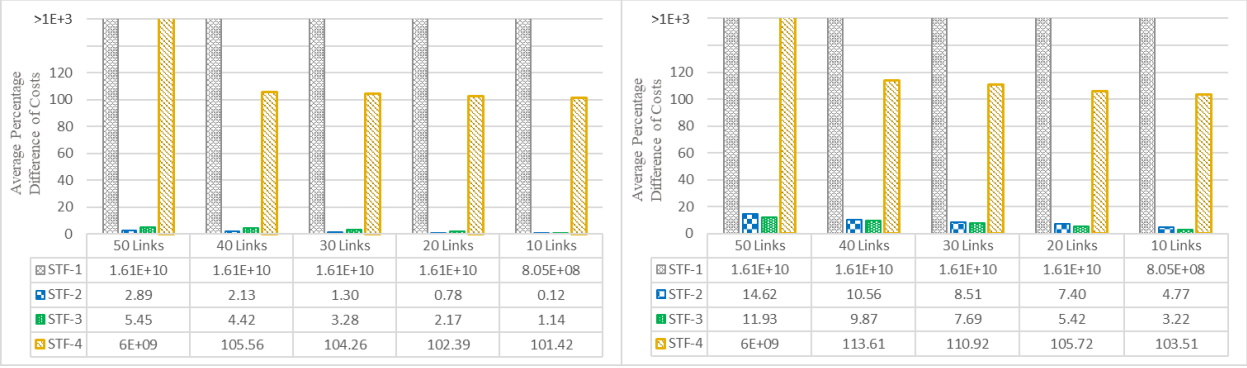


Figure 3-5 Average Percentage Difference for Different Costs under Link's Full Closure and Targeted Attack

a) Average Percentage Difference Between NRI's and BLUE's Performance Function
b) Average Percentage Difference Between NRI*'s and BLUE's Performance Function
c) Average Percentage Difference Between IS's and BLUE's Performance Function

Figure 3-2 through Figure 3-4 illustrate the outcomes of targeted partial closure attacks (40, 60, and 80% capacity reduction), while Figure 3-5 illustrates the results of a targeted full closure attack (100 percent capacity decrease) on various DLs (i.e., 10, 20, 30, 40, and 50 links per set). As seen by the scenario of targeted partial closure, all link selections except $T_C BC^*$ are compatible with the proposed algorithm. When *BC**, $T_{FF}BC^*$, and *V/C* links selection measures are utilized to simulate the intelligence adversary, the cost difference between BLUE's performance function and all three selected vulnerability traffic-based measures (NRI, NRI*, and

IS) is acceptable. By incorporating *BC** into the VGSB, the possibility of attacking central links with higher social efficiency will be increased and similarly, $T_{FF}BC^*$ raises the attack's probability of central links with higher free-flow travel time and higher travel demand. The *V/C* ratio increases the likelihood that more congested links will be attacked by the adversary.

The results of a targeted full-closure attack are depicted in Figure (5). As expected from the partial closure results presented in Figure 3-2 through Figure 3-4, T_CBC^* is not a suitable simulator for the intelligent adversary in the methodology proposed in this research. In comparison to partial closure results, the *V/C* ratio underperforms when simulating complete link closure. This is a significant finding since many agencies define a link's criticality based on its *V/C* ratio under normal operating conditions, while our findings indicate that this measure does not result in appropriate performance in the case of evaluating the network vulnerability using the shortest path concept for major disruption.

*BC** and $T_{FF}BC^*$ hybrid measures are the measures that showed very promising results for both minor and major disruptions, and they are more compatible with the proposed model for detecting the most critical group of links. Since traffic equilibrium inputs and outputs are considered along with the shortest paths concept in calculating these two hybrid measures, therefore, they are recommended as the best-selected link selection measures when modeling the intelligent adversary of the network using BLUE. For a more in-depth discussion about the nature of these measures, the reader is referred to the previous article published by the authors (23) or chapter 2 of this research.

Disrupting a Group of Links Versus Disrupting Multiple Single Links:

Further analysis was performed to evaluate the existing correlation between single critical links and critical group of links in the network vulnerability assessment. To conduct this analysis, links ranking, and the system cost due to disturbing critical sets of links ordered by BLUE and the group of links based on $T_{FF}BC^*$ hybrid measure rank order were compared and the results are presented in Table 3-8 and Figure 3-6. The first two columns of Table 3-8 show the single ranking based on $T_{FF}BC^*$. The third column of this table displays the number of disrupted links per set and the last column presents the BLUE solution where $T_{FF}BC^*$ is used as the link selection obtained with the number of links per set reported in the third column.

Table 3-8 Critical Links According to $T_{FF}BC^*$ and BLUE

Rank	$T_{FF}BC^*$	DL	BLUE (Scenario SF-3)
1	805	1	805
2	761	2	761, 805
3	947	3	761, 947, 805
4	731	4	446, 761, 947, 805
5	801	5	947, 446, 807, 790, 761
6	567	6	731, 807, 947, 761, 802, 790
7	727	7	761, 805, 735, 734, 947, 939, 830
8	734	8	761, 446, 449, 805, 932, 947, 939, 806
9	735	9	947, 801, 446, 761, 931, 805, 939, 806, 932
10	446	10	731, 761, 735, 947, 802, 427, 742, 805, 790, 939

Table 3-8 clearly highlighted difference between the $T_{FF}BC^*$ ranking measure and the BLUE's solution using $T_{FF}BC^*$ for simulation the intelligent adversary. As the number of disrupted links per set increase, this difference will be more visible. In fact, it can be seen that the most identified critical sets of links by the optimization approach are not simply the

combination of the most critical single links. and there is a very complex correlation between links when multiple disrupted links are studying.

The difference between ranking measure and BLUE's solution becomes more apparent when the system's cost is considered in the analysis. In the following analysis, the total system's cost under shortest path assignment is calculated by sequentially disrupting an increasing number of links in each critical set, according to the priority order determined by $T_{FF}BC^*$ ranking. The results are then compared to the network's cost calculated by disrupting critical sets of links determined by BLUE and the comparison is shown in Figure 3-6.

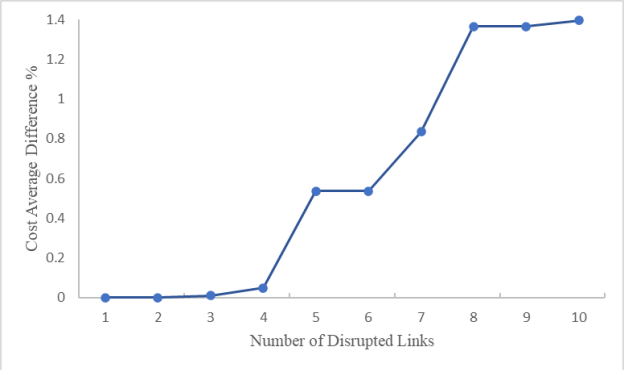


Figure 3-6 Cost Average Difference Between $T_{FF}BC^*$ Hybrid Ranking Measures and BLUE

As the results indicate, when multiple links are disrupted, the ranking method significantly underestimates the vulnerability of the network. As the number of multiple links is increased, the cost difference will be greater. The presented results indicate that the most critical sets of links, those that have the greatest negative effect on the system's total travel cost following an attack, are not simply the combination of the most critical single link and there is a very complex correlation between links when multiple disrupted links are studying.

Defended Network

Figure 3-7 illustrates the effect of defender decision to reduce the network's vulnerability using the proposed methodology. In this study, it was assumed that the defender could defend a limited number of links. To assess the impact of full and partial protection, two levels of defense efficiency were considered (i.e., 50% and 100%). Additionally, the effect of the defense budget was studied by considering various ratios of the number of Defended Links to Attacked Links (DL/AL) in the system (i.e., DL/AL of 1 through 5). It is worth mentioning that the number of possible attacked links is limited to 10 in this figure to save the solver time. However, the same trend is anticipated for the other cases (i.e., 20, 30, or more attached links). Also, since $T_{FF}BC^*$ was recommended as one of the two best link selection measures in attacking strategy, it was used as representative for both defender and adversary to defend and attack the network.

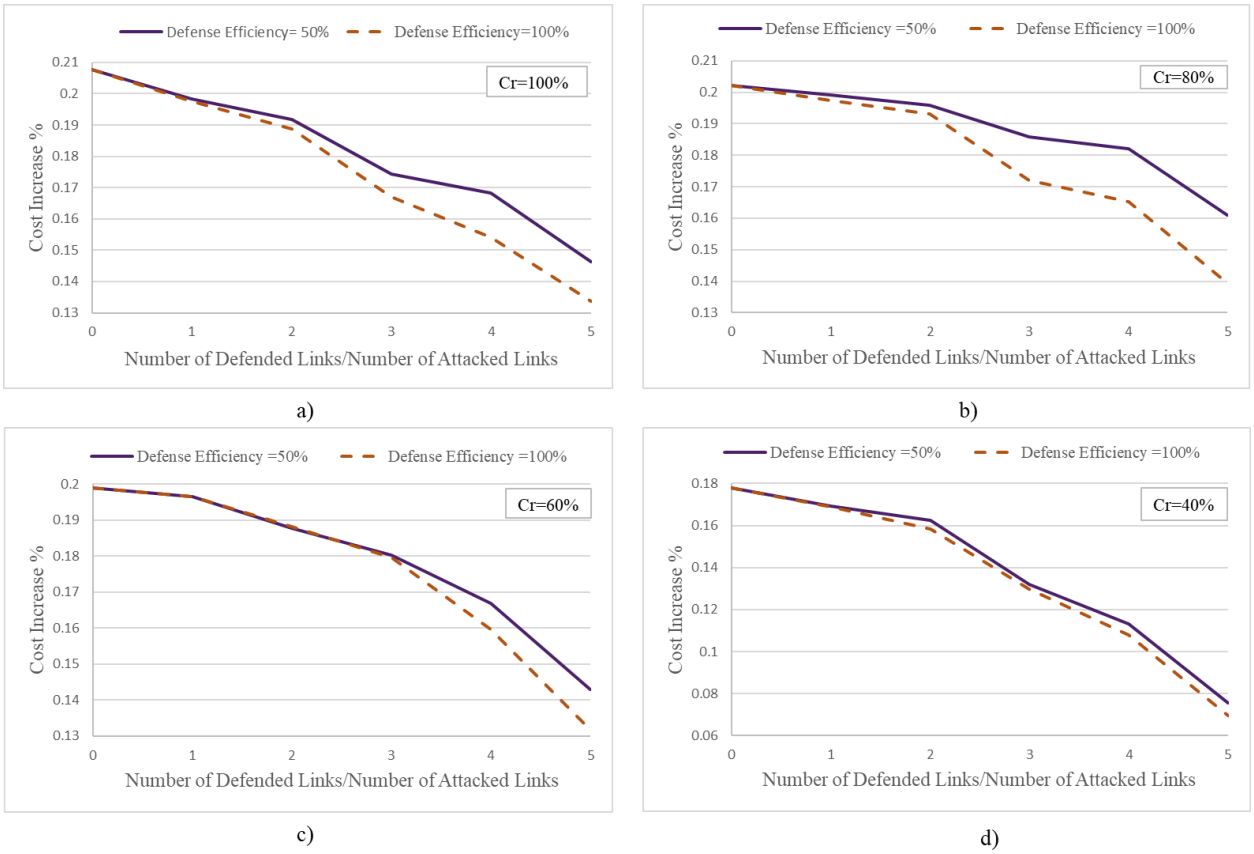


Figure 3-7 Costs Percentage Change for Different Link's Defend Strategies

a) 100% Capacity Reduction of the Attacked Links, Scenario SF-3
b) 80% Capacity Reduction of the Attacked Links, Scenario SP-3
c) 60% Capacity Reduction of the Attacked Links, Scenario SP-3
d) 40% Capacity Reduction of the Attacked Links, Scenario SP-3

As the results demonstrate, defending the links against an adversary can significantly decrease system costs (i.e., vertical ax). However, this improvement is highly dependent on attack efficiency. As can be seen, the difference in defensive efficiency between 100% and 50% is more noticeable when attack efficiency is high (i.e., when Cr = 100% and Cr = 80%). Complete and partial defense strategies have a nearly close effect on reducing the system's cost when the link's capacity is reduced by 40% or 60% (minor disruptions). Additionally, as illustrated in Figure 3-7, the total cost decreases as the number of protected links increases,

although the effect of DL/AL on system cost reduction is highly dependent on attack efficiency as well.

Conclusions

In this research, a model formulation and a heuristic solution algorithm were proposed to assist decision-makers in identifying and ranking vulnerable and critical sets of links of a transportation network. Using a game theory framework and a bi-level formulation, this research identified the most critical sets of links in a roadway network, focusing on both day-to-day and major disruptions. Five distinct link selection measures were used to simulate both the non-intelligent and intelligent adversary's decision to attack the system's links. Also, the effect of defender decisions in defending important links was studied. Unlike most vulnerability modeling approaches found in the literature, which require multiple traffic assignments to assess the network's vulnerability, the methodology developed in this research evaluates networks' vulnerability using only one traffic assignment and can find the worst combination of critical links. As a result, the presented methodology is easily applicable to evaluating roadway networks of any size without excessive computational time or power requirements under different disruption scenarios.

Chicago-Sketch selected as the network for applying the network and three well-known full scan analysis measures (NRI, NRI*, IS) were used to evaluate achieved results. Analysis of the results showed that contrary to popular belief, the volume to capacity ratio of links cannot be considered as accurate measure of a links' criticality in every situation. $T_{FF}BC^*$ and T_CBC^* were the measures showing the best performance in the analysis and more compatible with the presented methodology. These two attack link's selection measures increase the attack

probability of central links with more demand. Additionally, comparison between the multiple links disruption and multiple single link disruptions indicate that the most identified critical sets of links, which after attack have the greatest negative effect on the system's total travel cost, are not simply the combination of the most critical single link. Identifying critical sets of links is highly dependent on the adversary's inelegancy, the attack's selection of links, and the disruption scenario defined in terms of partial or complete link closure. Further analysis accomplished to evaluate the effect of defender decision in defending recognized critical links by decreasing the attack efficiency on these links. In this analysis, different budget constraints were considered for the defender and the effect of these constraints were evaluated in changing the total travel time of the network.

Future research can include the development of a solution algorithm with different objective functions for the two upper players (i.e., defender and adversary), and application of different measures in the selection of candidate links. Additionally, different objective functions for the defender and adversary could be considered, as well as multiple adversaries with distinct sets of objectives. The proposed method was based on a static user equilibrium, which is incapable of accounting for the effects of link interaction and demand uncertainty in traffic assignment. Future research may concentrate on dynamic traffic assignment and/or variable demand.

CHAPTER 4 : IMPLEMENTATION OF THE PROPOSED METHODOLOGIES IN A REAL CASE STUDY

Broward County, in Florida was chosen as the study's testbed location to implementing both proposed methodologies in this research (chapter 2 and 3) in consultation with the Florida Department of Transportation (FDOT) and local transportation agencies. This county in southeast Florida is critical for freight transportation, as it is home to the Port Everglades and the Fort Lauderdale International Airport, as well as the I-95, Florida Turnpike, and I-595.

The main network geometry is a subset of the Southeast Florida Regional Planning Model Version 8 (SERPM 8). This is an activity-based model that has become the state of practice in travel demand forecasting in the largest U.S. metropolitan areas. Personal and commercial demand was estimated using the assigned flows provided by Broward MPO and SE Florida through a well-known Origin Destination Matrix Estimation (ODME) procedure. The TransCAD software (https://www.caliper.com/) was used to implement the ODME procedure. The Broward County network is described in more in-depth details in Table 4-1 and Figure 4-1 Broward County Network Location.

Table 4-1 Broward County Network

Network	No. of Nodes	No. of Links	No. of Origin-Destinations (ODs) pairs
Broward	9,975	24,007	1,653

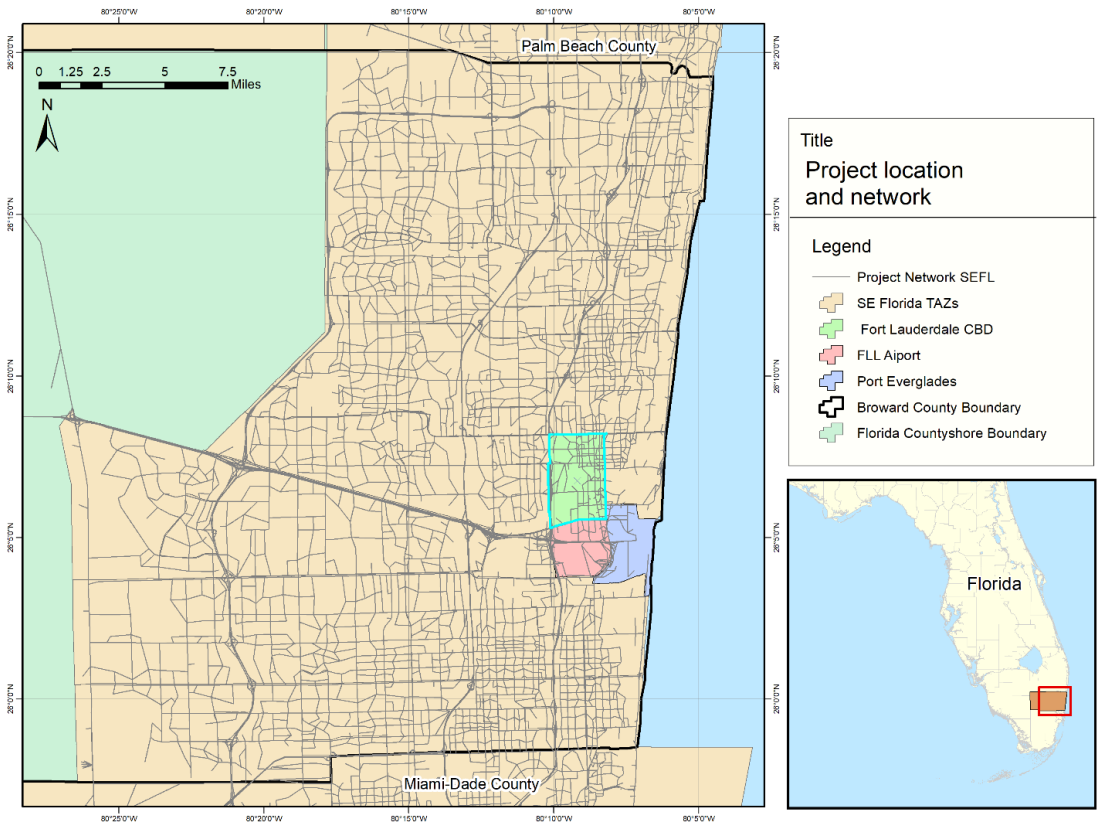


Figure 4-1 Broward County Network Location.

Individual Critical Link

Figure 4-2 through Figure 4-4 present the top 5%, 10%, 15%, and 20% important links identified by each one of the three hybrid measures recommended in Chapter 2 of this research. In these figures, the road classification of the identified critical links showed by using two different colors. The top critical links which are arterial are shown by red color, and the critical links which are non-arterial, have been shown by green. As seen in these figures, the majority of the identified critical links are arterial links. These links carry more flow than non-arterial links,

so disrupting them have a more negative cost effect on the network. Also, these figures show that central links (i.e., links that more shortest paths traverse on them to connect pairs of ODs) are more critical than the others. So, if a link has more demand and is simultaneously more central, it is a more critical link than the others. On the other hand, attacks concentrated around origins and destinations with a high amount of demand in a way that would effectively isolate that origin or destination (i.e., a bridge).

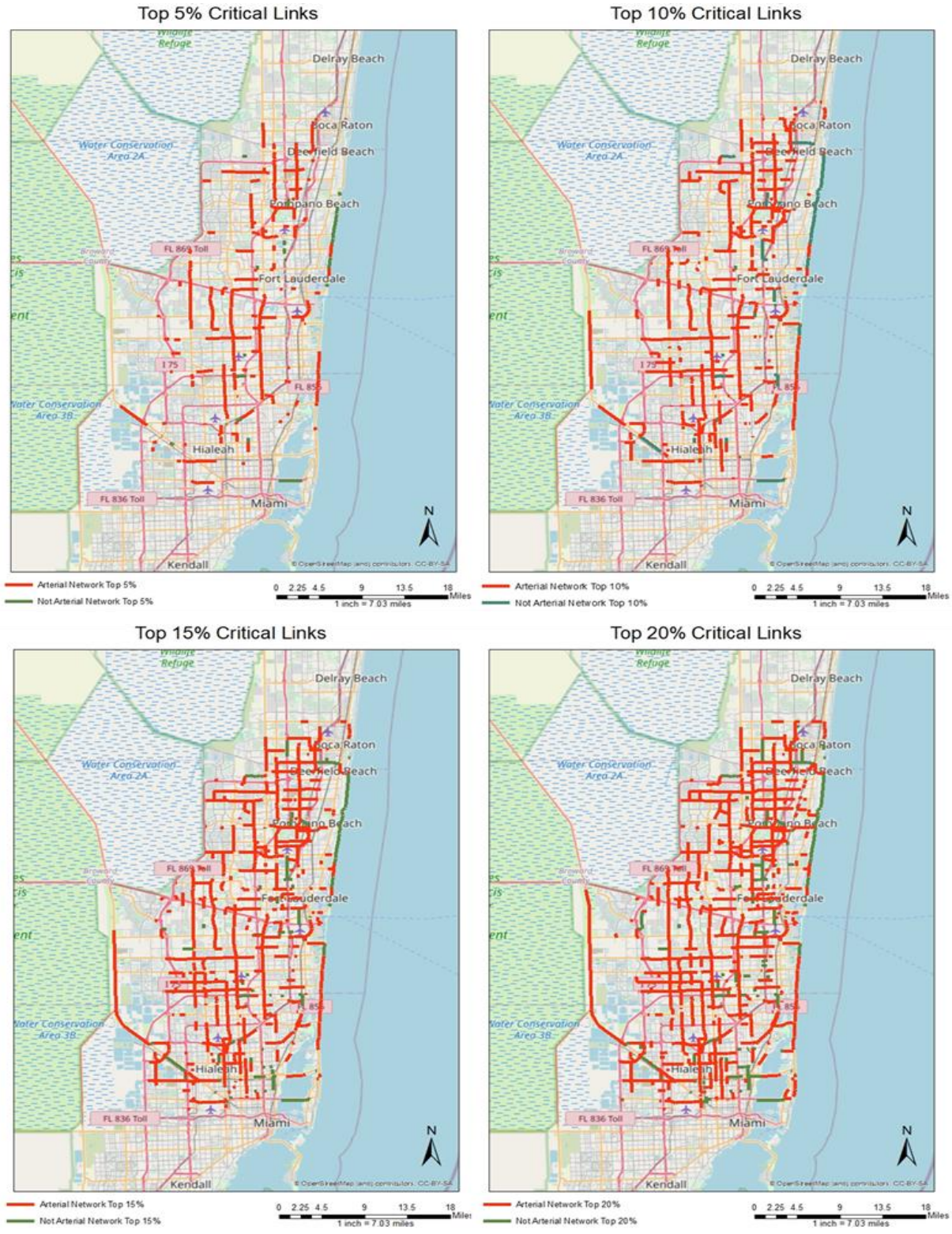


Figure 4-2 Critical links identified by BC^* hybrid measure

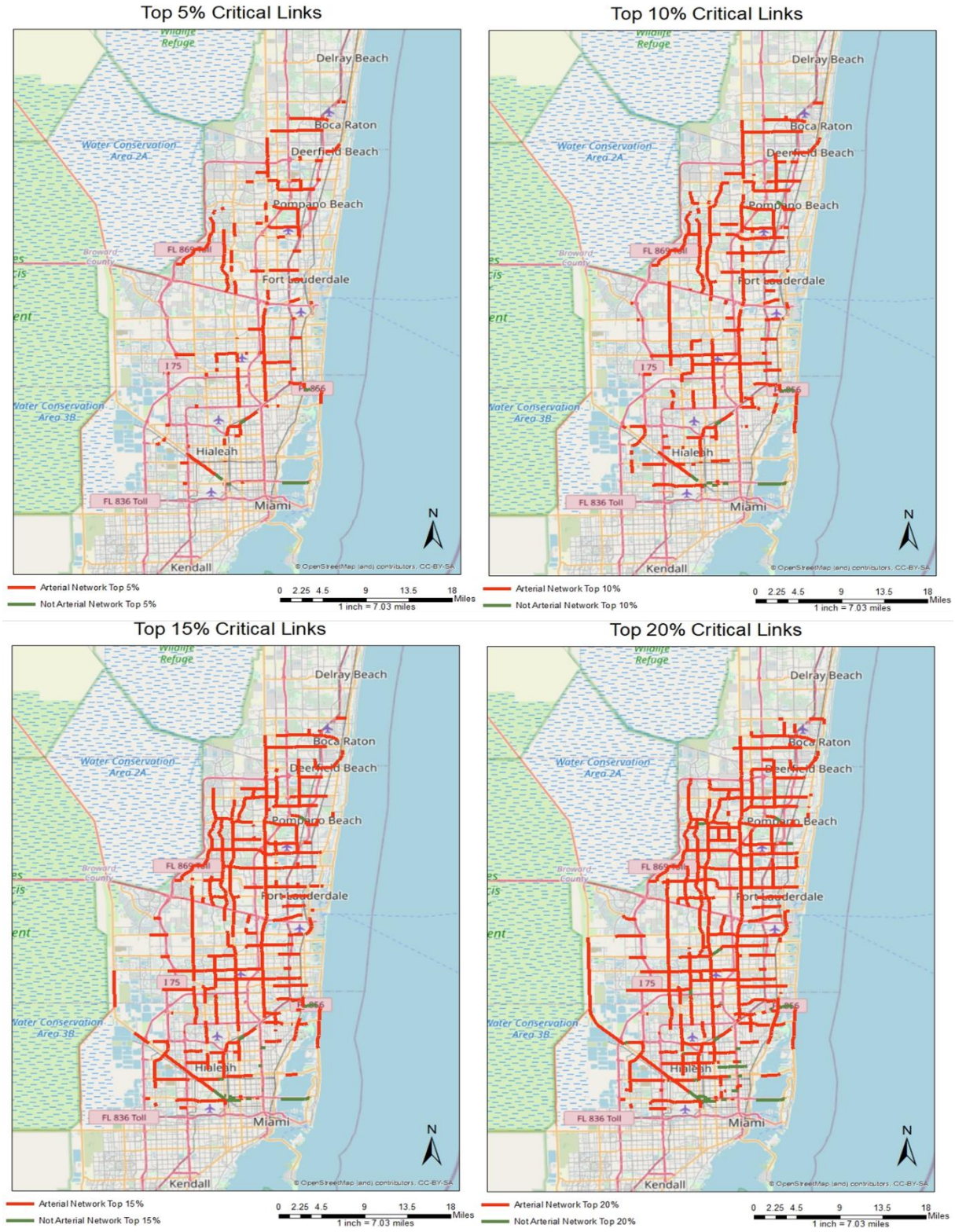


Figure 4-3 Critical links identified by $T_{ff}BC^*$ hybrid measure

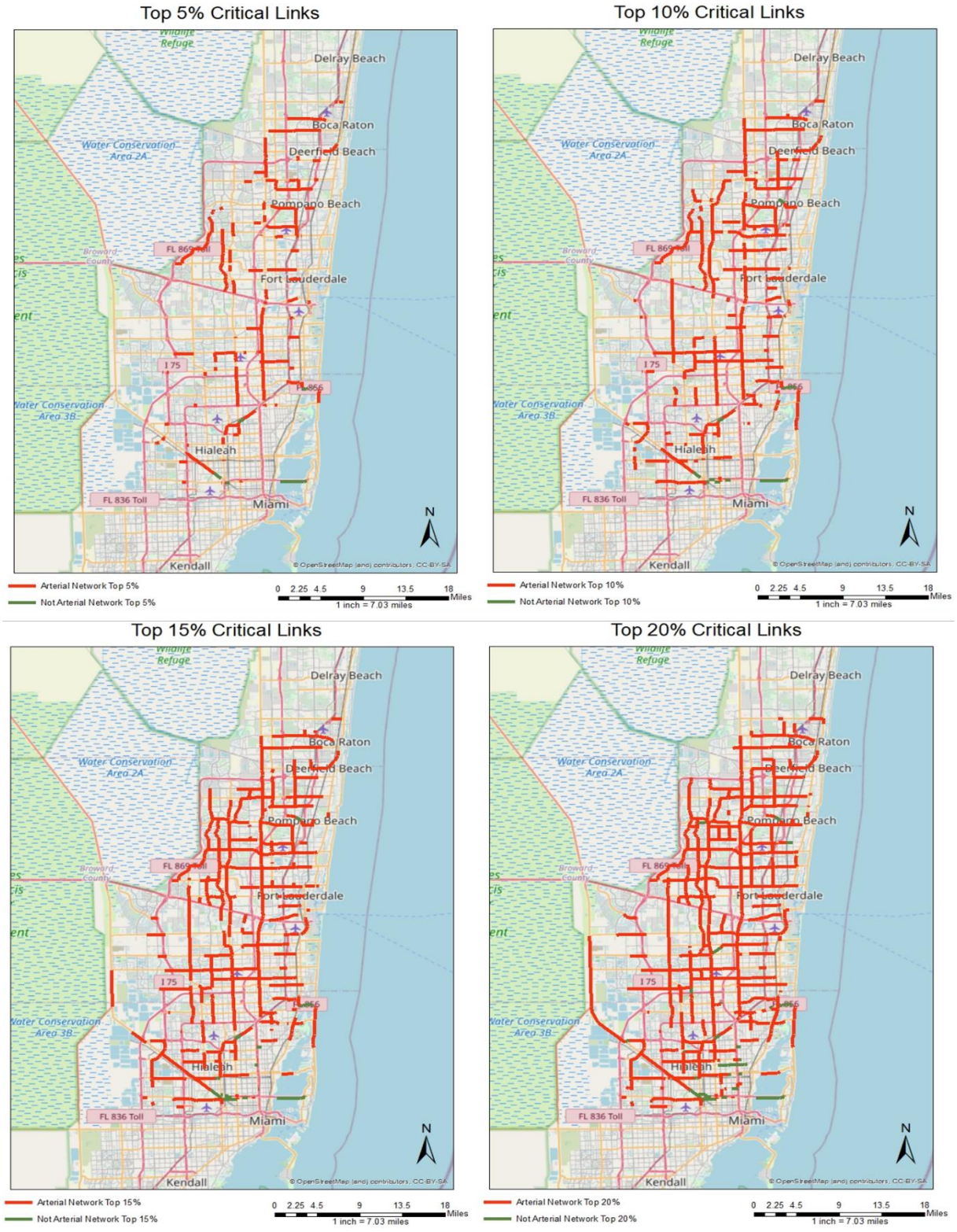


Figure 4-4 Critical links identified by T_cBC^* hybrid

Critical Sets of Links

By implementing the presented mathematical formulation and developed heuristic algorithm presented on chapter 3 of this research on the Broward County network, 10,000 different critical sets of 30 links were identified for each one of the three assumed capacity reduction cases (100%, 80%, and 60% capacity reduction respectively) and for any link that was compromised based on two distinct link selections (i.e., BC^* and $T_{ff}BC^*,$). These sets of links were ranked according to the effect they may have on increasing the cost of travel in the case of attacks. In other words, a set of links is more important than other if attacking it results in the greatest increase in travel time across the network.

As illustrated in Figure 4-5, the most critical subset of links will be altered in response to the attack's efficiency (partial closure vs. full closure of the link). The findings indicated that depending on the severity of the disruption scenario (minor or major), different links in the roadway network could be identified as critical. Even considering different capacity reductions (60 and 80 percent) in partial closure scenarios results in the identification of distinct critical sets of links.

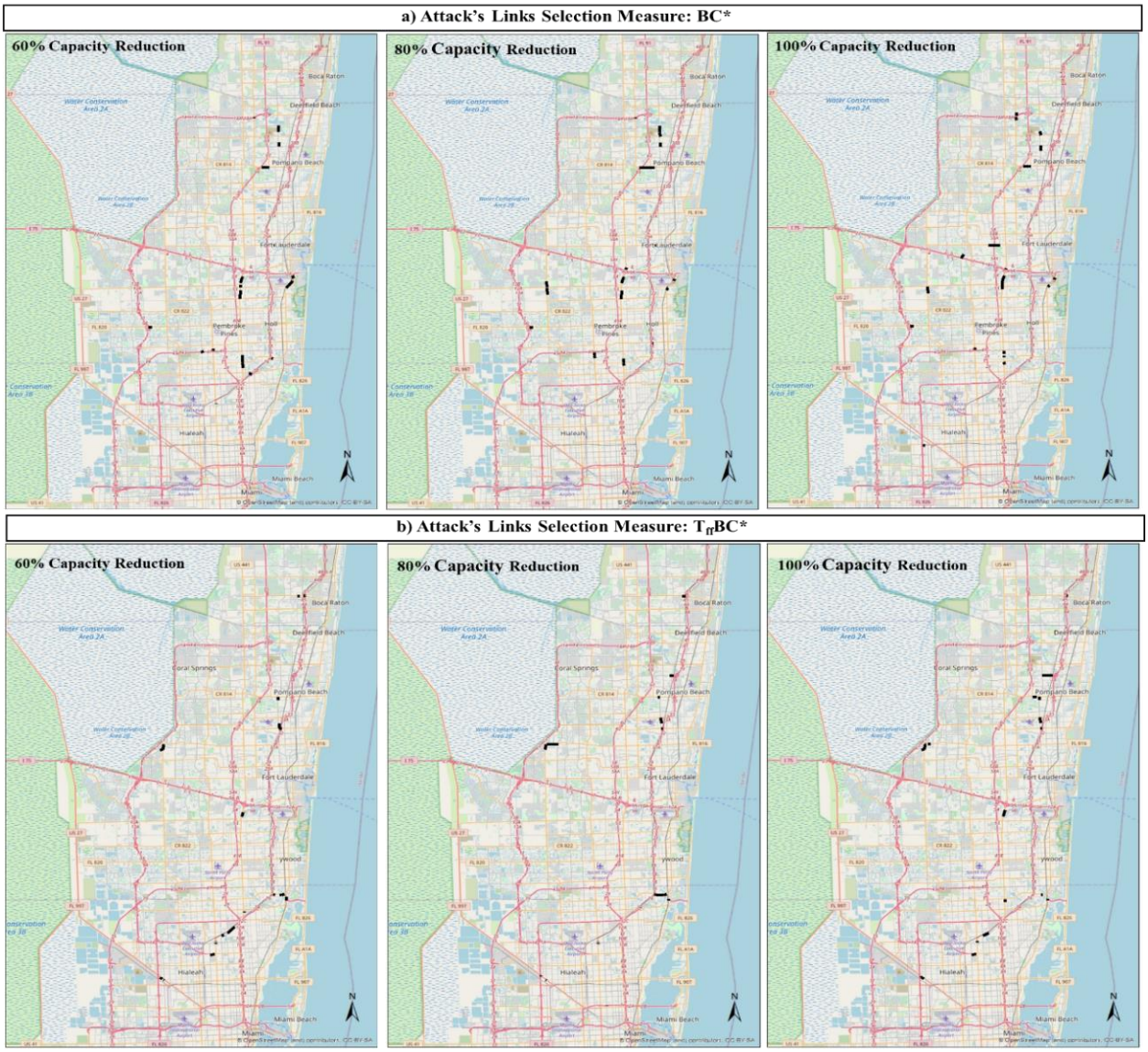


Figure 4-5 First Critical Sets of Links Using Three Different Link Selections Under Different Capacity Reductions: a) *BC**, b) $T_{ff}BC^*$

Figure 4-6 and Figure 4-7 illustrate the probability of attack for each link using all two link selection measures under various capacity reduction scenarios (i.e., 100, 80, and 60 percent). The probability can be assumed as a measure of a link's criticality; it is calculated as the sum of the number of times a link is selected as critical (for all 10,000 sets). Comparing the probability of

attack for each link selection scenario and the top 1% critical links ranking by hybrid measures which are more compatible with BLUE (i.e., $BC^*, T_{ff}BC^*$), it is revealed that the most critical sets of links that when attacked result in the greatest negative effect on the system's total travel cost are not simply a collection of the most single-link failures. Identifying critical sets of links is highly dependent on the adversary's inelegancy, the attack's selection of links, and the disruption scenario defined in terms of partial or complete link closure.

In Figure 4-6, the intelligent adversary's link selection in the BLUE is represented by BC^*. The results in this figure indicate that central links (i.e., links that more shortest paths traverse on them to connect pairs of origin destinations (ODs)) are more critical than others. Thus, if a link has a higher demand and is also more central, it is considered more critical than the others. On the other hand, attacks focused on high-demand origins and destinations effectively isolate those origins and destinations (i.e., a bridge). Additionally, by comparing Figure 4-5(a) to Figure 4-6, it is clear that the first recognized critical sets of links (sets of links whose compromise results in an increase in the network's highest cost) are the links with the highest attack probability. Thus, considering only the firsts recognized sets of links as the most vulnerable links by the proposed algorithm can save decision makers more computational time when assessing the network's vulnerability.

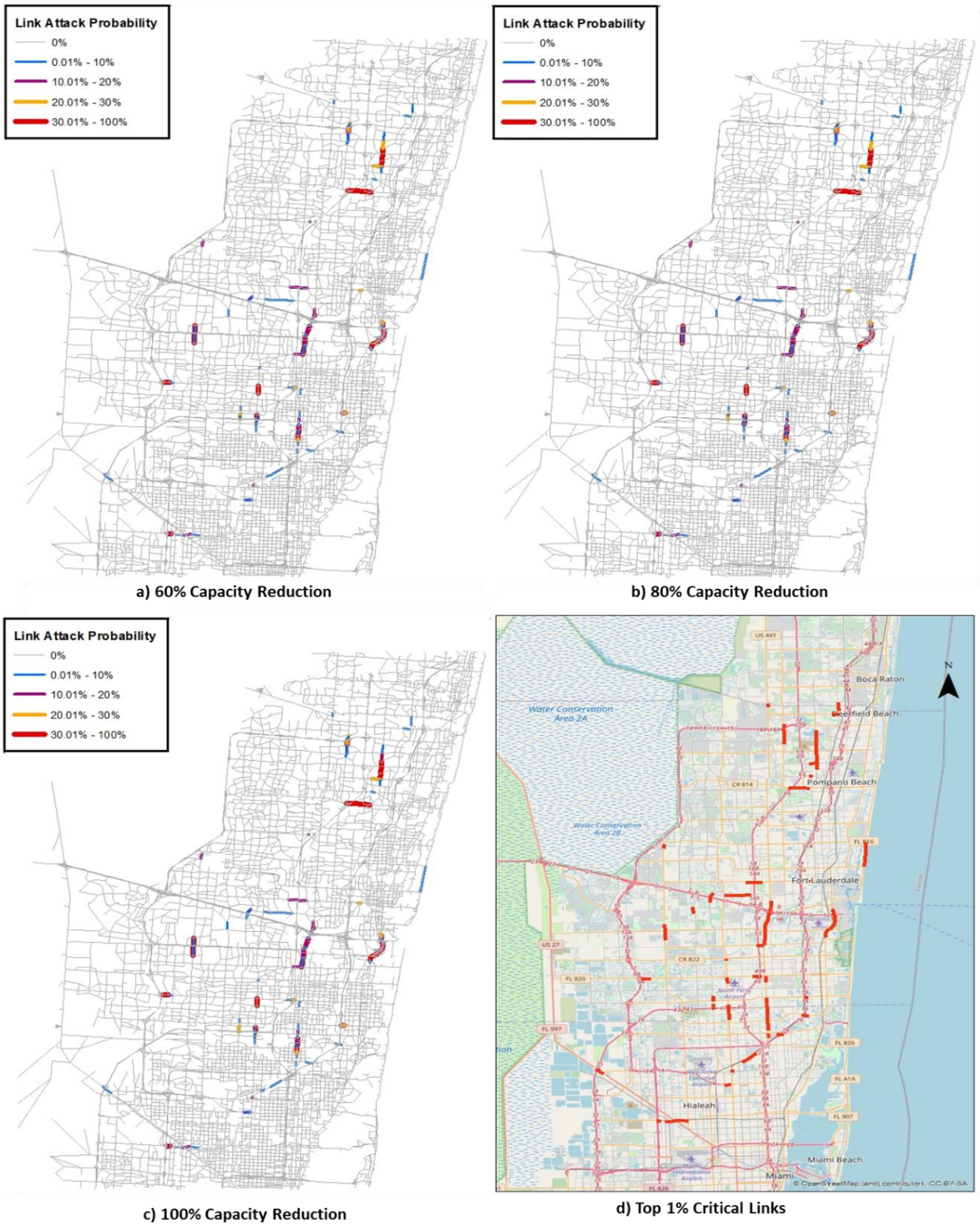


Figure 4-6 Link Attack Probability vs. Top 1% Critical Links for *BC**.

Apart from centrality and social efficiency (i.e., roads with greater demand serve more people and thus achieve additional social and economic benefits, and therefore should be considered more significant), $T_{ff}BC^*$ also consider travel time shortest path (in both congested and uncongested situations) when calculating the network's most critical links. According to $T_{ff}BC^*$ (Figure 4-7), critical links are those which are more central than others, have a higher demand, and require more travel time to commute (in both congested and non-congested situations). The comparison results in Figure 4-5(b) support the conclusion stated in the preceding paragraph that the firsts recognized critical sets of links (sets of links whose compromise results in an increase in the network's highest cost) are the links with the highest attack probability.

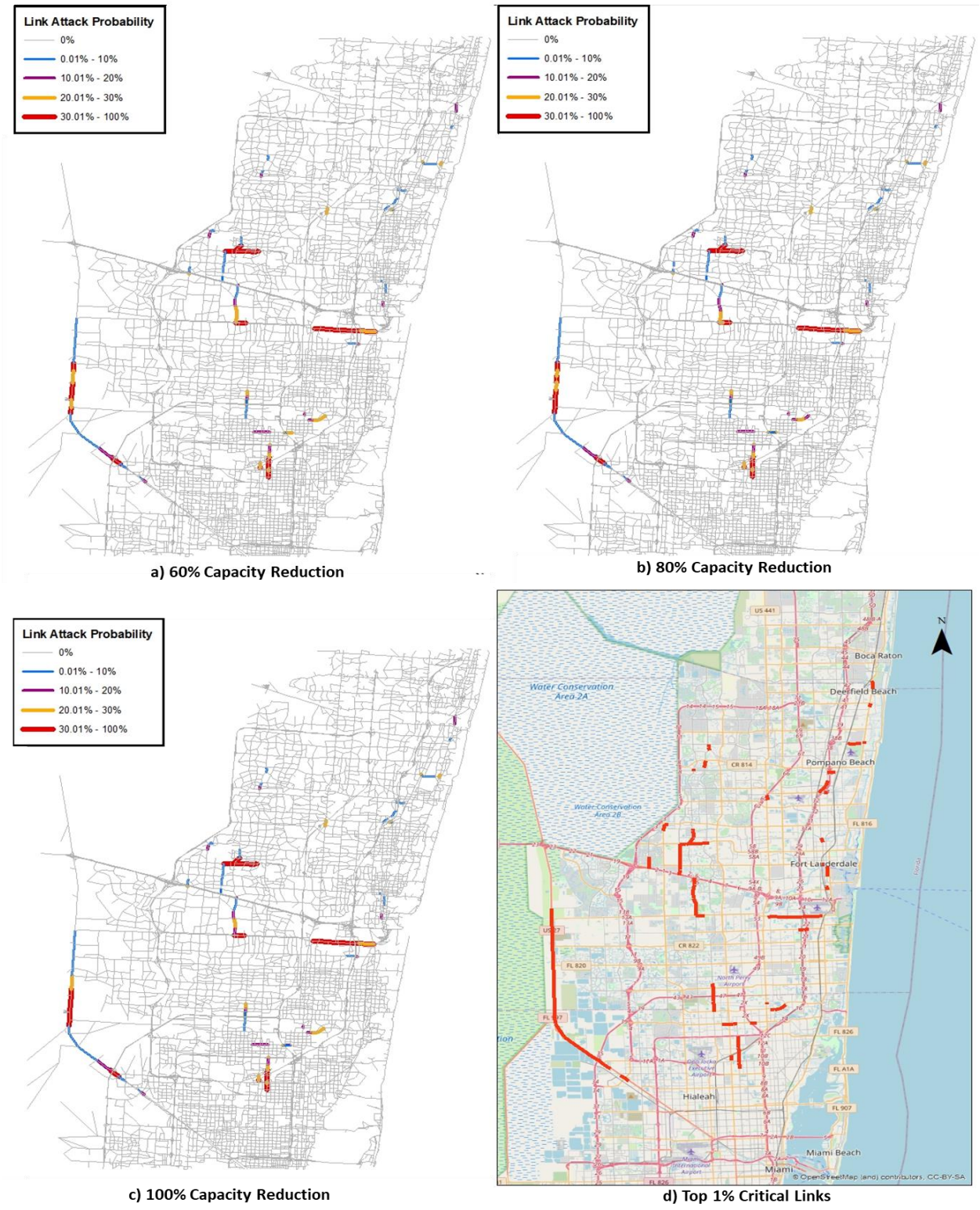


Figure 4-7 Link Attack Probability vs. Top 1% Critical Links for $T_{ff}BC^*$.

CHAPTER 5 : SUMMARY, CONCLUSIONS, AND DIRECTION FOR FUTURE RESEARCH

Prioritizing investment decisions in roadway network infrastructure is a serious obstacle for decision-makers and planning agencies. Transportation networks are subject to a variety of disruptive events that have a significant impact on the travel time of network users. Additionally, limited resources are compelling national, regional, and local governments to prioritize their investments carefully. Thus, planners and decision-makers should employ an efficient and innovative prioritization technique to ensure that significant projects are undertaken and that resources are used efficiently.

In the first part of this research, it was attempted to understand the relative importance of links in a road network and suggested a methodology to rank the links according to structure of the network while combining with several input and output characteristics of the traffic equilibrium. Nine hybrid ranking measures developed as a variants of link Betweenness Centrality (BC) measure. To this matter, various traffic characteristics of the network assigned as link's weight in calculating BC. Links with high betweenness centrality values represent a bridge-like connector between different parts of a network, a failure of which will affect the communication between multiple pairs of nodes through the shortest path. Weighting links adds another dimension of heterogeneity to the network beyond the topological effects. Numerical experiments using three case study networks in three different sizes (i.e., Sioux Falls, Eastern Massachusetts, and Chicago-Sketch), indicated that three of the proposed nine measures provide comparable results

to a full-scan analysis. The proposed hybrid link ranking measures require only one traffic assignment in their calculations which lead to decreasing the computational time significantly compared to the full-scan analysis measures.

Numerical results showed that considering social efficiency in the proposing hybrid measures made their results more reliable. Utilizing social efficiency in calculating BC make sure that if a link has more demand and is simultaneously more central, should be more critical to whole network. In addition to the social efficiency effect, the shortest path travel time effect in both uncongested and congested situations was also important. The recommended hybrid ranking measures identified links which are more central as compared to the others and has higher demand and more travel time require to commute on them in both congested and non-congested situations as the most importing links in the network. Disrupting these links may have more severe damage to the system and can result, resulting in a significant increase in travel costs.

The second section of this research proposed a bi-level mathematical formulation and heuristic solution algorithm to assisted decision makers in identifying and ranking vulnerable and critical sets of links in a transportation network under various disruption scenarios. The presented methodology covers two distinct game frameworks: 1) Adversary-User and 2) Defender-Adversary-User. Five distinct link selection measures were used to simulate both the non-intelligent and intelligent adversary's decision to attack the system's links, and four distinct link capacity reduction measures were used to simulate both major and minor disruptions. Additionally, the effect of defender decisions on defending critical links was investigated. Numerical experiments using a case study network indicated that the proposed methodology provide reliable results to a full-scan analysis. Unlike the majority of vulnerability modeling approaches described in the literature, which require multiple traffic assignments to assess a

network's vulnerability, the methodology developed in this research use only one traffic assignment and can identify the worst combination of critical links. As a result, the methodology presented here is easily applicable to evaluating roadway networks of any size without requiring excessive computational time or power under various disruption scenarios.

The results analysis revealed that the presented methodology produces promising results, particularly when the hybrid measures presented in this research are used to simulate an intelligent adversary. Additionally, contrary to popular belief, the volume to capacity ratio of links cannot be used to accurately determine a link's criticality in all circumstances. More importantly, this research demonstrates that the most identified critical sets of links, which have the greatest negative impact on the system's total travel cost due to an attack, are not simply the combination of the most critical single link. Identification of critical sets of links is highly dependent on the disruption scenario defined by the adversary's inelegancy, the attack's link selection, and the disruption scenario defined in terms of partial or complete link closure. This study demonstrates how presenting a defender can mitigate the adversary's effect on the network. This reduction, however, is highly dependent on the efficiency of the attack and the defense budget constraints. By utilizing the presented methodology, decision-makers can maximize the system's resilience under various disruption scenarios considering their budget constraints.

Both proposed methodologies for ranking single and multiple links described in Chapter 2 and Chapter 3 rely on a static user equilibrium, which cannot capture the effects of link interaction and assignment and/or variable demand uncertainty. Future research could concentrate on implementing dynamic traffic assignment in presenting new hybrid link ranking measures on an individual basis. Additionally, the mathematical formulation presented in Chapter 3 can be expanded to include dynamic traffic assignment in simulating traveler behavior.

Future research can propose new hybrid measures by either modifying an existing topological measure (such as closeness, degree centrality, etc.) by different traffic characteristics or by combining several hybrid measures.

Additional research could include examining different objective functions for the defender and adversary and evaluating candidates' links using a variety of different measures. This study assumed the same objective function for both the defender and adversary had. Considering distinct objective functions for these two players could be an extremely interesting future direction. Additionally, the effect of multiple adversaries with different objective functions on the identification of critical sets of links can be studied. Future research directions may also include expanding the hierarchical bi-level game proposed in this study by incorporating a combination of sets of links and a capacity-enhancing capital investment strategy. Furthermore, links can be attacked with a reduced capacity reduction, as opposed to the case where the defender invests through capacity expansion.

REFERENCES

1. Dehghani MS, Flintsch G, McNeil S. Impact of road conditions and disruption uncertainties on network vulnerability. J Infrastruct Syst. 2014 Sep 1;20(3).
2. Zhou Y, Wang J, Yang H. Resilience of transportation systems: concepts and comprehensive review. IEEE Trans Intell Transp Syst. 2019;20(12):4262–76.
3. Wang DZW, Liu H, Szeto WY, Chow AHF. Identification of critical combination of vulnerable links in transportation networks – a global optimisation approach. Transp A Transp Sci. 2016 Apr 20;12(4):346–65.
4. Lock J, Gelling M. The Tasman bridge disaster - before and after. Aust Road Res. 1976;6(2):9–16.
5. Taylor MAP. Vulnerability analysis for transportation networks. Vulnerability Analysis for Transportation Networks. Elsevier; 2017. 1–258 p.
6. Rupi F, Angelini S, Bernardi S, Danesi A, Rossi G. Ranking links in a road transport network: A practical method for the calculation of link importance. Transp Res Procedia. 2015;5:221–32.
7. Liu W, Song Z. Review of studies on the resilience of urban critical infrastructure networks. Reliab Eng Syst Saf. 2020;193:106617.
8. Mattsson LG, Jenelius E. Vulnerability and resilience of transport systems - A discussion of recent research. Transp Res Part A Policy Pract. 2015;81:16–34.
9. Almotahari A, Yazici MA. A link criticality index embedded in the convex combinations solution of user equilibrium traffic assignment. Transp Res Part A Policy Pract. 2019 Aug 1;126:67–82.
10. Sohn J. Evaluating the significance of highway network links under the flood damage: An accessibility approach. Transp Res Part A Policy Pract. 2006 Jul;40(6):491–506.
11. Demšar U, Špatenková O, Virrantaus K. Identifying critical locations in a spatial network with graph theory. Trans GIS. 2008;12(1):61–82.
12. Knoop VL, Snelder M, van Zuylen HJ, Hoogendoorn SP. Link-level vulnerability indicators for real-world networks. Transp Res Part A Policy Pract [Internet]. 2012;46(5):843–54. Available from: http://dx.doi.org/10.1016/j.tra.2012.02.004
13. Duan Y, Lu F. Robustness of city road networks at different granularities. Phys A Stat Mech its Appl. 2014 Oct 1;411:21–34.
14. Latora V, Marchiori M. Efficient behavior of small-world networks. Phys Rev Lett. 2001 Nov 5;87(19):198701-1-198701–4.
15. Porta S, Crucitti P, Latora V. The network analysis of urban streets: A dual approach. Phys A Stat Mech its Appl. 2006 Sep 15;369(2):853–66.
16. Taylor MAP, Sekhar SVC, D'Este GM. Application of accessibility based methods for vulnerability analysis of strategic road networks. Networks Spat Econ. 2006 Sep;6(3–

4):267–91.

17. Furno A, Faouzi NE El, Sharma R, Cammarota V, Zimeo E. A Graph-based Framework for Real-time Vulnerability Assessment of Road Networks.

18. Cantillo V, Macea LF, Jaller M. Assessing Vulnerability of Transportation Networks for Disaster Response Operations. Networks Spat Econ [Internet]. 2019;19(1):243–73. Available from: https://doi.org/10.1007/s11067-017-9382-x

19. Chen A, Yang C, Kongsomsaksakul S, Lee M. Network-based acessibility measures for vulnerability analysis of degradable transportation networks. Networks Spat Econ. 2007;7(3):241–56.

20. Jenelius E, Petersen T, Mattsson L-G. Importance and exposure in road network vulnerability analysis. Transp Res Part A Policy Pract. 2006;40(7):537–60.

21. Jenelius E, Mattsson L-GG. Road network vulnerability analysis of area-covering disruptions: A grid-based approach with case study. Transp Res Part A Policy Pract. 2012 Jun;46(5):746–60.

22. Jenelius E, Mattsson L-GG. Road network vulnerability analysis: Conceptualization, implementation and application. Comput Environ Urban Syst. 2015 Jan 1;49:136–47.

23. Scott DM, Novak DC, Aultman-Hall L, Guo F. Network Robustness Index: A new method for identifying critical links and evaluating the performance of transportation networks. J Transp Geogr. 2006;14(3):215–27.

24. Sullivan JL, Novak DC, Aultman-Hall L, Scott DM. Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: A link-based capacity-reduction approach. Transp Res Part A Policy Pract. 2010 Jun;44(5):323–36.

25. Murray-Tuite PM, Mahmassani HS. Methodology for determining vulnerable links in a transportation network. Transp Res Rec. 2004 Jan 1;1882(1):88–96.

26. Bell MGH, Kanturska U, Schmöcker JD, Fonzone A. Attacker-defender models and road network vulnerability. Philos Trans R Soc A Math Phys Eng Sci. 2008 Jun 13;366(1872):1893–906.

27. Higgs B, Golias MM, Mishra S. Multi-Level Multi-Objective Vulnerability Assessment of Transportation Networks. 2017.

28. Yates J, Sanjeevi S. A length-based, multiple-resource formulation for shortest path network interdiction problems in the transportation sector. Int J Crit Infrastruct Prot. 2013 Jun 1;6(2):107–19.

29. Chen A, Yang C, Kongsomsaksakul S, Lee M. Network-based accessibility measures for vulnerability analysis of degradable transportation networks. Networks Spat Econ. 2007;7(3):241–56.

30. Taylor MAP. Critical transport infrastructure in urban areas: Impacts of traffic incidents assessed using accessibility-based network vulnerability analysis. Growth Change.

2008;39(4):593–616.

31. Nagurney A, Qiang Q. A Transportation Network Efficiency Measure that Captures Flows, Behavior, and Costs With Applications to Network Component Importance Identification and Vulnerability. Ssrn. 2007;1–22.

32. Sullivan JLL, Novak DCC, Aultman-Hall L, Scott DMM. Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: A link-based capacity-reduction approach. Transp Res Part A Policy Pract. 2010 Jun;44(5):323–36.

33. Luathep P, Sumalee A, Ho HW, Kurauchi F. Large-scale road network vulnerability analysis: A sensitivity analysis based approach. Transportation (Amst). 2011;38(5):799–817.

34. El-Rashidy RA, Grant-Muller SM. An assessment method for highway network vulnerability. J Transp Geogr [Internet]. 2014;34:34–43. Available from: http://dx.doi.org/10.1016/j.jtrangeo.2013.10.017

35. Gauthier P, Furno A, El Faouzi NE. Road network resilience: how to identify critical links subject to day-to-day disruptions. Transp Res Rec. 2018;2672(1):54–65.

36. Li F, Jia H, Luo Q, Li Y, Yang L. Identification of critical links in a large-scale road network considering the traffic flow betweenness index. PLoS One. 2020 Apr 1;15(4):1–23.

37. Freeman LC. A set of measures of centrality based on betweenness. Sociometry. 1977;40(1):35–41.

38. Dijkstra EW. A note on two problems in connexion with graphs. Numer Math. 1959;1(1):269–71.

39. Sheffi Y. Urban transportation networks: equilibrium analysis with mathematical programming methods. In 1985.

40. Starita S, Scaparra MP. Assessing road network vulnerability: A user equilibrium interdiction model. J Oper Res Soc. 2020;0(0):1–16.

41. Berdica K. An introduction to road vulnerability: What has been done, is done and should be done. Transp Policy. 2002;9(2):117–27.

42. Spearman C. The proof and measurement of association between two things. Am J Psychol. 1904;15(1):72–101.

43. Stabler, B., H. Bar-Gera, Sall. E, Stabler B, Bar-Gera H, Sall E. Transportation networks for research core team [Internet]. 2020. Available from: https://github.com/bstabler/TransportationNetworks.

44. Kumar A, Peeta S. Slope-based path shift propensity algorithm for the static traffic assignment problem. Int J TRAFFIC Transp Eng. 2014 Sep;4(3):297–319.

45. U.S. Department of Transportatio B of TS. Transportation Statistics Annual Report 2020. Washington, DC; 2020.

46. Report A. Statistics 2016 Annual Report. U.S. Department of Transportation, Bureau of Transportation Statistics, Transportation Statistics Annual Report 2017 (Washington, DC: 2017).; 2017.

47. Sugishita K, Asakura Y. Vulnerability studies in the fields of transportation and complex networks: a citation network analysis. Public Transp. 2021;13(1):1–34.

48. Wang Z, Chan APC, Yuan J, Xia B, Skitmore M, Li Q. Recent advances in modeling the vulnerability of transportation networks. J Infrastruct Syst. 2015;21(2):1–9.

49. Faturechi R, Miller-Hooks E. Measuring the performance of transportation infrastructure systems in disasters: A comprehensive review. J Infrastruct Syst. 2015;21(1).

50. Takhtfiroozeh, H; Golias, M; Mishra S. Topological-Based Measures with Flow Attributes to Identify Critical Links in a Transportation Network. Transp Res Rec. 2021;(March):03611981211013039.

51. Khademi N, Balaei B, Shahri M, Mirzaei M, Sarrafi B, Zahabiun M, et al. Transportation network vulnerability analysis for the case of a catastrophic earthquake. Int J Disaster Risk Reduct. 2015 Jun 1;12:234–54.

52. Takhtfiroozeh, Hana; Machado, A; Golias, M. Hourdos, J; Evangelos, K; Mishra S. Identifying Critical and Vulnerable Freight Routes in the State of Florida. In: Transportation Research Board, Washington DC.; 2021.

53. Bricha N, Nourelfath M. Critical supply network protection against intentional attacks: A game-theoretical model. Reliab Eng Syst Saf. 2013;119:1–10.

54. Lu Q, George B, Shekhar S. Capacity constrained routing algorithms for evacuation planning: A summary of results. In: International symposium on spatial and temporal databases. Springer; 2005. p. 291–307.

55. Clegg R. Empirical studies on road traffic response to capacity reduction. Transp traffic theory. 2007;17:155–78.

56. Golob TF, Recker WW. Relationships among urban freeway accidents, traffic flow, weather, and lighting conditions. J Transp Eng. 2003;129(4):342–53.

57. Dalziell E, Nicholson A. Risk and impact of natural hazards on a road network. J Transp Eng. 2001;127(2):159–66.

58. Berdica K, Mattsson L-G. Vulnerability: a model-based case study of the road network in Stockholm. In: Critical infrastructure. Springer; 2007. p. 81–106.

59. Kim Y, Kang W-H, Song J. Assessment of seismic risk and importance measures of interdependent networks using a non simulation-based method. J Earthq Eng. 2012;16(6):777–94.

60. Luathep P, Suwanno P, Taneerananon P. Identification of critical locations in road networks due to disasters. In: Proceedings of the Eastern Asia society for transportation studies. 2013. p. 206.

61. Jenelius E. Large-scale road network vulnerability analysis. KTH; 2010.

62. Lu Q-C, Peng Z-R. Vulnerability analysis of transportation network under scenarios of sea level rise. Transp Res Rec. 2011;2263(1):174–81.

63. Abounacer R, Rekik M, Renaud J. An exact solution approach for multi-objective location–transportation problem for disaster response. Comput Oper Res. 2014;41:83–93.

64. Sherali HD, Carter TB, Hobeika AG. A location-allocation model and algorithm for evacuation planning under hurricane/flood conditions. Transp Res Part B Methodol. 1991;25(6):439–52.

65. Smith AB, Katz RW. US billion-dollar weather and climate disasters: Data sources, trends, accuracy and biases. Nat hazards. 2013;67(2):387–410.

66. Elvik R. How much do road accidents cost the national economy? Accid Anal Prev. 2000;32(6):849–51.

67. Xie F, Levinson D. Evaluating the effects of the I-35W bridge collapse on road-users in the twin cities metropolitan region. Transp Plan Technol. 2011;34(7):691–703.

68. Bell MGH. A game theory approach to measuring the performance reliability of transport networks. Transp Res Part B Methodol. 2000;34(6):533–45.

69. Rahman A, Lownes NE, Ivan JN, Fiondella L, Rajasekaran S, Ammar R. A game theory approach to identify alternative regulatory frameworks for hazardous materials routing. In: 2012 IEEE conference on technologies for homeland security (HST). IEEE; 2012. p. 489–94.

70. Xu X, Chen A, Yang C. An optimization approach for deriving upper and lower bounds of transportation network vulnerability under simultaneous disruptions of multiple links. Transp Res procedia. 2017;23:645–63.

71. Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces (Providence). 2006;36(6):530–44.

72. Wood RK. Deterministic network interdiction. Math Comput Model. 1993;17(2):1–18.