Improving resilience of freight networks in West Tennessee

Prepared by:

Principal Investigator

Mihalis M. Golias, Ph.D.

Associate Professor, Dept. of Civil Engineering,

University of Memphis, 104C Engr. Sc. Bldg., 3815 Central Avenue, Memphis, TN 38152

Tel: 901-678-3048, Fax: 901-678-3026, Email: mgkolias@memphis.edu

Co-Principal Investigators

Sabya Mishra, Ph.D., P.E.

Assistant Professor, Dept. of Civil Engineering, University of Memphis,

112D Engr. Sc. Bldg., 3815 Central Avenue, Memphis, TN 38152

Tel: 901-678-5043, Fax: 901-678-3026, Email: smishra3@memphis.edu

Shahram Pezeshk, Ph.D., P.E.

Professor, Dept. of Civil Engineering, University of Memphis,

112D Engr. Sc. Bldg., 3815 Central Avenue, Memphis, TN 38152

Tel: 901-678-4727, Fax: 901-678-3026, Email: spezeshk@memphis.edu

Researchers

Karlis Pujats

Graduate Research Assistant, Dept. of Civil Engineering, University of Memphis

302 Engineering Administration Bldg., 3815 Central Avenue, Memphis, TN 38152

Email: kpufats@memphis.edu

November 8, 2018

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-CFL/TD-0x-00x		

4. Title and Subtitle	5. Report Date
Improving resilience of freight networks in West Tennessee	September 2018
	6. Performing Organization Code
7. Author(s) Golias, M., Mishra, S., Pezeshk S., Pujats K.	8. Performing Organization Report No.
9. Performing Organization Name and Address University of Memphis 3851 Central Avenue Memphis, TN 38152	10. Work Unit No. (TRAIS) 11. Contract or Grant No.
12. Sponsoring Agency Name and Address Tennessee Department of Transportation Long Range Planning Division 505 Deaderick St., Nashville, TN 37243-0344	13. Type of Report and Period Covered 14. Sponsoring Agency Code HFTS-16.4

15. Supplementary Notes

COTR: First & Last name, FHWA CFLHD; Advisory Panel Members: List First & last names. This project
was funded under the FHWA Federal Lands Highway Technology Deployment Initiatives and Partnership
Program (TDIPP). Or the Coordinated Technology Implementation Program (CTIP).

16. Abstract

This project developed models and tools of freight network vulnerability and resilience that capture both long/medium range pre- and post-disruption network conditions. This research used the demand/supply of the passenger and freight road network of the greater Memphis metropolitan area, an important freight hub in the nation’s transportation system and of significant importance to the Midwest region of the U.S. Deliverables include a report on state of the art and practice of network vulnerability and resilience, a GIS based tool and a mathematical model to identify vulnerable freight links and routes, and a mathematical based tool to identify investment options to improve and maximize resilience of the passenger and/or freight network in TN. These products can be used by TDOT, regional, and local public agencies to further improve their respective freight planning processes.

17. Key Words	18. Distribution Statement
Improving resilience of freight networks in West Tennessee	No restriction. This document is available to the public from the sponsoring agency at the website http://www.cflhd.gov.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	167	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

DISCLAIMER

This research was funded through the State Research and Planning (SPR) Program by the Tennessee Department of Transportation and the Federal Highway Administration under RES #:2016-36, Research Project Title: Improving resilience of freight networks in West Tennessee.

This document is disseminated under the sponsorship of the Tennessee Department of Transportation and the United States Department of Transportation in the interest of information exchange. The State of Tennessee and the United States Government assume no liability of its contents or use thereof.

The contents of this report reflect the views of the author(s) who are solely responsible for the facts and accuracy of the material presented. The contents do not necessarily reflect the official views of the Tennessee Department of Transportation or the United States Department of Transportation.

EXECUTIVE SUMMARY

With freight networks acting as economic pipelines that distribute goods throughout a region, disruptions to the network can have widespread consequences. Thus, the vulnerability and resilience of freight networks are extremely important considerations. The complexity of these elements, multiple measures of performance (e.g., mobility can be measured in terms of speed, response time, evacuation time), interactions between them, and the interdependency of various types of networks (e.g., risk for loss of electric power increases vulnerability of the roadway network) necessitates simultaneous optimization of multiple objectives. Characterizing risks within a network can be complex and include time dependent (i.e., planning, tactical, operational, real time) and time changing objectives such as shortest routes, congestion and safety of a route, clearance time, total distance traveled, and link connectivity to multiple paths. Vulnerable routes in a network are best identified through engagement of multiple stakeholders with different roles, risk thresholds, and objectives.

Goals and Objectives: This project developed models and tools of freight network vulnerability and resilience that capture both long/medium range pre- and post-disruption network conditions. This research used the demand/supply of the passenger and freight road network of the greater Memphis metropolitan area, an important freight hub in the nation's transportation system and of significant importance to the Midwest region of the U.S. Deliverables include a report on state of the art and practice of network vulnerability and resilience, a GIS based tool to identify vulnerable freight links and routes, and a tool to identify investment options to improve and maximize resilience of the freight network in TN. These products can be used by TDOT, regional, and local public agencies to further improve their respective freight planning processes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Vulnerabilities of transportation networks have been widely studied in recent years and are gaining even more attention with the growing number of threats (e.g., climate change, man-made attacks). Research in this area can vary drastically (in mathematical formulations, assumptions made, objective functions used) due to the vague meaning and various interpretations of the term vulnerability. There are also other terms with definitions and interpretations akin to the term vulnerability like robustness, resiliency, and reliability. Transportation networks are open to a wide variety of threats that can be divided into two main categories: intentional and unintentional. The former are deliberate and intelligent attacks on a network with a clear goal of disrupting the network and attempt to exploit known vulnerabilities. Transportation networks are a common target of such attacks due to being economic pipelines crucial to the movement of people, goods, and services. The damage or destruction (partial or full loss of capacity of a link or path) of transportation infrastructure can have wide-spread detrimental effects, thus making a very desirable target for intentional attacks. Unintentional threats usually pertain to the consequences of human error, insufficient maintenance, or damage caused by acts of nature. Human errors like negligence and traffic accidents can have drastic consequences to the network's performance and ability to accommodate traffic. Weather events can also be detrimental to a network and can indirectly reduce capacity (i.e., lower travel speeds with lower densities due to increased driver reaction times). Natural disasters like earthquakes, volcanic activity, flooding, tsunamis, hurricanes, etc. have been responsible for billions of dollars of damage in the United States alone.

From 1980 to 2011, there have been 133 disasters designated as billion dollars disasters (total damages more than one billion dollars). Humans can also make choices that have unintended consequences to the performance of a roadway network as well. In the worst of cases, improper maintenance of the infrastructure (e.g., bridges) can lead to a complete loss of capacity (as was the case for the collapse of a bridge on I-35 W in Minnesota). Traffic accidents are much more common than infrastructure failure with 10.8 million crashes occurring in the United States in 2009. In 2010, the economic cost of crashes totaled $242 billion and if quality-of-life is considered the total value of societal harm was $836 billion.

1.1 Project Scope

Transportation networks are by nature vulnerable to natural and man-made disasters (or incidents). The concept of vulnerability focuses on three elements: a) degree of loss and damage, b) degree of exposure, and c) degree of resilience. The complexity of each element and its components, the multiple measures of performance for each (e.g., mobility can be measured with speed, response time, evacuation time, etc. depending on the incident), interactions between them, and the interdependency of various physical and other types of networks (e.g., risk for loss of electric power increases vulnerability of the roadway network) necessitates simultaneous optimization of multiple objectives. The objective of this project is to develop models and tools of freight network vulnerability and resilience that capture both operational/real time and long/medium range pre- and post-disruption network conditions.

The rest of the report is organized as follows. The next chapter presents a brief summary the literature that has been published on the topic of transportation resilience to date. The third chapter presents the methodology and models that were developed to identify the critical and vulnerable links within a network. The fourth chapter presents the methodology and models developed to rank the critical and vulnerable links and paths within a network. The fifth chapter presents the ArcGIS toolbox that was developed as part of this research to support application of the models and solution algorithms developed as part of this project. The last chapter concludes the report and provides future research directions.

CHAPTER 2: LITERATURE REVIEW

This section of the report presents a summary of the literature on the following three areas: (1) vulnerability/resilience, (2) game theory frameworks, and (3) optimization algorithms. The vulnerability/resilience part of the literature review is divided into three sections structured around the three questions that (Kaplan and Garrick, 1981) associate with vulnerability. The game theory part of the literature review is divided into two sections. The first section is a general introduction to the application of game theory to various problems. The second section defines the players that exist in a transportation network and the research that has examined the actions of these players. The optimization part of the review will discuss the solution algorithms presented in the literature to solve problems of transportation link vulnerability/resilience estimation.

2.1 Vulnerability/resilience of roadway networks

Research on the vulnerability and resilience of systems in general (not only transportation networks), has been an area of increasing research. Unfortunately, due to various interpretations of the terms by researchers and practitioners the published articles can vary drastically. In addition, other terms relating to vulnerability and resilience (e.g., robustness, reliability) have been used interchangeably in the literature. According to (Kaplan and Garrick, 1981) to define vulnerability one must ask and answer the following questions: 1) What can happen, 2) How likely is it that the event will happen, and 3) What are the consequences?

With regards to the first question, and in the case of transportation networks, a wide variety of threats exist and can be grouped into two main categories based on the cause of the incident: i) intentional and ii) unintentional. Intentional threats, listed in Table 2-1, are attacks on a network with a clear goal of disrupting the operations. Such threats are considered as intelligent and, in most of the cases, attempt to exploit known vulnerabilities of the transportation network (e.g., a bridge that connects two major urban areas). 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 2-1: List of Intentional Threats

Threat	Description
Terrorist Attack (Bricha and Nourelfath, 2013; Latora and Marchiori, 2005; Lu et al., 2005)	A terrorist attack is a very focused and deliberate attack to damage or destroy an infrastructure
Construction (Clegg, 2007)	Partial or full road closures are very common occurrences when maintaining or improving roadways

On the other hand, unintentional threats are the results of either human error or acts of nature. Human errors like negligence and traffic accidents can have drastic consequences to the operations of a network. The literature review distinguishes between weather events (rain, snow, etc.) and natural disasters (earthquake, hurricane, etc.) by considering that weather events occur often while 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. Tables 2-2 through 2-5 summarize a list of weather, natural disaster, human related, and generic events that increase the vulnerability and reduce resilience of transportation networks.

Table 2-2: List of Weather Events

Weather Event	Description
Rain (Golob and Recker, 2003)	Precipitation in the form of liquid water
Snow and Ice (Berdica and Mattsson, 2007; Dalziell and Nicholson, 2001)	Precipitation in the form of frozen water

Table 2-3: List of Natural Disasters

Natural Hazard	Description
Earthquakes (Abounacer et al., 2014; Kim et al., 2012a, 2012b; LUATHEP et al., 2013a; Oppenheim, 1977; Poljansek et al., 2012; Wu and Duenas-Osorio, 2013)	The sudden release of energy in the Earth's crust that creates seismic waves
Volcanic Activity (Erik Jenelius, 2010)	This can be an eruption or lava flow associated with an active volcano
Sea Level Rise (Lu and Peng, 2011)	The gradual rise of sea level over time (8 inches in the past century)
Flooding (Abounacer et al., 2014; LUATHEP et al., 2013a)	An overflow of water that submerges land that is typically dry
Tsunamis (Abounacer et al., 2014)	A sea wave caused by the displacement of a large volume of a body of water.
Hurricane (Sherali et al., 1991)	A large tropical storm system with high-powered circular winds
Tornado (Smith and Katz, 2013)	A funnel cloud of violently rotating winds
Wildfires (Smith and Katz, 2013)	A large, destructive fire that spreads quickly
Blizzard (Smith and Katz, 2013)	A severe snowstorm with high winds and low visibility

Table 2-4: List of Humen Error Events

Human Error	Description
Traffic Accidents (Elvik, 2000)	Traffic accidents can result in temporary partial or full road closures leading to unexpected delay in a network.
Improper Maintenance (Xie and Levinson, 2011)	Improper maintenance can result in failures that can be catastrophic in some cases (Minnesota Bridge)

Table 2-5: List of Generic Events

Event	Description

Full closure of one link (Berdica and Mattsson, 2007)	Studies in this category focus on the effects generated by the closure of a single roadway link
Full closure of multiple links (Jenelius and Mattsson, 2012)	Studies in this category focus on the effects generated by the closure of multiple roadway links
Partial closure of one link (Berdica and Mattsson, 2007)	Studies in this category focus on the effects of closing only part one link (lane closure)
Partial Closure of Multiple Links (Berdica and Mattsson, 2007)	Studies in this category focus on the effects of closing only part of multiple links (lane closures)
Increased Traffic Volume (Berdica and Mattsson, 2007)	Studies in this category focus on the performance of a network using higher than normal traffic volumes (future traffic growth)

With regards to the second question (i.e., how likely is that an event will happen) two measures have been commonly used in the literature to provide an answer: time periods of occurrence and probability of occurrence. The former measure is usually associated with weather events and earthquakes and can easily be converted to probabilities while the latter is case based and can vary greatly over time (e.g., the probability of an earthquake or a volcano eruption increases with time; the probability of an intentional attack on a network can fluctuate based on different geopolitical conditions). The authors would like to note that the quantity and accuracy of information available is key to determining the probability associated with a specific threat (intentional or otherwise) and decision makers have a very difficult task considering all the different threats and their probabilities while making a decision that will have consequences on the performance of a network.

The final question (i.e., what are the consequences) is usually answered through the estimation of the impacts to the transportation network users. In most cases these impacts are averaged or combined (e.g., mean total travel time increase, total travel delay) as an event will not impact all users in the same manner. Combination can include weights to differentiate between the different groups of uses (e.g., passenger VS freight).

There are two different types of measures used to evaluate transportation networks: (1) link and (2) network measures. Link measures only reflect the characteristics or influence of a single link while network measures reflect the performance or characteristics of an entire network. Most of the network measures are an aggregation of a link measure for all links on the network.

Both measures can be divided into four subcategories: (1) mobility, (2) accessibility, (3) reliability, and (4) resilience. Mobility measures focus on how easy or difficult is to travel through the network. Accessibility refers to the connectivity of the network. Reliability, a derivative of mobility, refers to the fluctuations of mobility. Finally, resilience is usually a comparison of all three measures before and after an event. Tables 2-6 and 2-7 summarizes the link and network measures for each subcategory that have been found in the published literature. The first column provides the measure, the second column provides the formula used to estimate the measure, and the third column provides the definition of the variables used in column two. Table 2-7 has a fourth column that indicates the desired direction of optimization (if the measure is used as part of a decision-making support tool).

Table 2-6: Link Performance Measures

Measures	Function	Definitions
	Mobility	
Congestion Index (Zhang and Lomax, 2008)	$CI = \frac{t_c}{t_f}$	t_cIs the travel time under congested traffic conditions $t_f$is the travel time under free-flow conditions
User Lost Time (YANG and QIAN, 2012)	$tt - t_f$	tt is the travel time $t_f$is the travel time under free-flow conditions
Travel Time (United States., 1964)	$S_a(v_a) = t_a\left(1 + 0.15\left(\frac{v_a}{c_a}\right)^4\right)$	$S_a(v_a)$ is the average travel time for a vehicle on link *a* t_a is the free flow travel time on link *a* per unit of time v_a is the volume of traffic on link *a* per unit of time c_a is the capacity of link *a* per unit of time
Travel Distance (Berdica and Mattsson, 2007)	$segment\ length$	
Travel Speed (Berdica and Mattsson, 2007)	$\frac{segment\ length}{tt}$	tt is the travel time
Travel Rate (Berdica, 2002; Pratt and Lomax, 1996)	$\frac{tt}{segment\ length} = (speed^{-1}) - 1$	tt is the travel time
Speed of Person Movement (Berdica, 2002; Pratt and Lomax, 1996)	$Passenger\ vol. \times average\ travel\ speed$	
Corridor Mobility Index (Berdica, 2002; Pratt and Lomax, 1996)	$\frac{Speed\ of\ Person\ Movement}{Standard\ Value}$	
	Accessibility	
Serviceability (Berdica, 2002)	Probability that link/route/network will be utilized during a given time period	
Accessibility (Chen et al., 2007; LUATHEP et al., 2013b;	Average travel time to locations or percentage of locations within a pre-specified time	

Luathep et al., 2011; Taylor et al., 2006)		
Reliability		
Delay Rate (Berdica, 2002; Pratt and Lomax, 1996)	$(atr - dtr) = \frac{(att - dtt)}{length}$	atr is the actual travel rate dtr is the desired travel rate att is the actual travel time dtt is the desired travel time
Total Delay (Berdica, 2002; Pratt and Lomax, 1996)	$dr \times people\ vol. \times length = (att - dtt) \times people\ vol.$	att is the actual travel time dtt is the desired travel time
Relative Delay Rate (Berdica, 2002; Pratt and Lomax, 1996)	$\frac{dr}{dtr} = \frac{atr}{dtr} - 1$	dr is the delay rate atr is the actual travel rate dtr is the desired travel rate
Delay Ratio (Berdica, 2002; Pratt and Lomax, 1996)	$\frac{dr}{atr} = 1 - \frac{dtr}{atr}$	dr is the delay rate atr is the actual travel rate dtr is the desired travel rate
Resilience		
Redundancy Importance -Flow (E. Jenelius, 2010)	$RI_{flow}(k;l) = (f_k^l - f_k^0)$	*l*,*k* are links f_k^0 is the base case flow on link *k* f_k^l is the flow on link *k* when link *l* is closed
Redundancy Importance-Impact (E. Jenelius, 2010)	$RI_{impact}(k;l) = \left(\Delta T_k^l - \Delta T^l\right)$	*L*,*k* are links ΔT^l is the base case ΔT_k^l is the total impact of closure of link *l* to link *k*
Robustness (Scott et al., 2006; Sullivan et al., 2010)	$q_a = c_a - c$ $c = \sum_a t_a x_a$ $c_a = \sum_a t_a x_a \delta_a$	q_a is the network robustness index c_a is the cost of removing link *a* *c* is the cost of the base case t_a is the travel time of link *a* x_a is the flow of link *a* δ_a is the presence of link *a* in the network (1 if present 0 otherwise)
Disruption Index (Murray-Tuite and Mahmassani, 2004)	$D_a = \sum_{r,s} M_a^{r,s}$ $M_a^{r,s} = \chi_a^{r,s} V_a^{r,s}$ $\chi_a^{r,s} = \left(\frac{x_a^{r,s}}{q^{r,s}}\right)$	D_a is the disruption index of link *a* *r* is the origin index *s* is the destination index

	$V_a^{r,s} = \begin{cases} 1.0 \;\; if\; k^{r,s} > K^{r,s} \\ 1.0 - \sum_{j=1}^{k^{r,s}} g_j^{r,s} \frac{X_{a,j}}{x_a^{r,s}} \; otherwise \end{cases}$ $g_j^{r,s} = \left(\frac{C_j^{r,s}}{\rho h_j}\right)\left(\frac{T_j^0}{\tau_j}\right)$ $C_j^{r,s} = \min_{l \in L_j} c_l \left(\frac{\mathrm{x}_l^{r,s}}{\sum_{r',s'} \mathrm{x}_l^{r',s'}}\right)$	$M_a^{r,s}$ is the vulnerability index for link *a* evaluated for O-D flow from *r* to *s* $\chi_a^{r,s}$ is the coefficient of $V_a^{r,s}$ $V_a^{r,s}$ is the initial vulnerability index $\mathrm{x}_a^{r,s}$ is the flow on link *a* from *r* to *s* $q^{r,s}$ is the total demand from *r* to *s* $k^{r,s}$ is the number of alternate paths needed to accommodate $x_a^{r,s}$ $K^{r,s}$ is the total number of paths connecting *r* and *s* *j* is the path index $g_j^{r,s}$ is the utility of alternate path *j* $X_{a,j}$ is the amount of flow on *a* to be accommodated by alternate path *j* $C_j^{r,s}$ is the excess capacity on path *j* available to *r,s* h_j is the bottleneck link of path *j* ρ_l is the maximum service rate of link *l* T_j^0 is the free flow path travel time for path *j* τ_j is the marginal path travel time c_l is the excess capacity of link *l* *r′,s’* is an O-D pair with flow on link *a* L_j is the set of links on path *j*
Impact Area Vulnerability Index (Chen et al., 2012)	$VUL_a^l = \frac{E_0(G_a) - E_a(G_a)}{E_0(G_a)}$ $E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	VUL_a^l is the impact area vulnerability index *l* is the traveler type *a* is the link index $E_0(G_a)$ is the network efficiency of impact area G_a under normal conditions

		$E_a(G_a)$ is the network efficiency of impact area G_a after the closure of link *a* *r* is the origin index *s* is the destination index *I* is the traveler type q_{rs} is the mean travel demand between *r* and *s* u_i^{rs} is the proportion of type *I* travelers from *r* to *s* π_i^{rs} is the minimum travel time budget between *r* and *s* for type *I* travelers
Importance-Cost Based (Jenelius et al., 2006)	$Importance_{net}^{dem}(k) = \frac{\sum_i \sum_{j \neq i} x_{ij}(c_{ij}^{(k)} - c_{ij}^{(0)})}{\sum_i \sum_{j \neq i} x_{ij}}, k \in E^{nc}$	x_{ij} is the travel demand from node *i* to node *j* $c_{ij}^{(k)}$ is the cost of travel from node *i* to node *j* when link *k* is closed $c_{ij}^{(0)}$ is the cost of travel from node *i* to node *j* when no link is closed E^{nc} is the set of non-cut links
Importance - Demand Based (Jenelius et al., 2006)	$Importance_{net}^{uns}(k) = \frac{\sum_i \sum_{j \neq i} u_{ij}^{(k)}}{\sum_i \sum_{j \neq i} x_{ij}}, k \in E$ $u_{ij}^{(k)} = \begin{cases} x_{ij} \; if \; c_{ij}^{(k)} = \infty \\ 0 \; if \; c_{ij}^{(k)} < \infty \end{cases}$	x_{ij} is the travel demand from node *i* to node *j* $u_{ij}^{(k)}$ is the unsatisfied demand from node *i* to node *j* when link *k* is closed $c_{ij}^{(k)}$ is the cost of travel from node *i* to node *j* when link *k* is closed *E* is the set of all links
Passenger Betweeness Centrality (Cats and Jenelius, n.d.)	$PBC(e) = \frac{\sum_{o \in S_{OD}} \sum_{d \in S_{OD}} E[\lvert N_{ode}(\sigma_0, t_s, \tau_s) \rvert]}{\sum_{o \in S_{OD}} \sum_{d \in S_{OD}} E[\lvert N_{od}(t_s, \tau_s) \rvert]}$	*e* is the link *o* is the origin *d* is the destination σ_0 is the baseline scenario t_s is the start time τ_s is the end time *N* is the number of passengers
Vulnerability Index (Dehghanisanij et al., 2013; Knoop	$I^1 = \frac{q}{(1 - \frac{q}{C})}$ $I^2 = \frac{1}{T_b}$	I_i^n is the *n*th criteria for link *i* q_i is the flow on link *i* C_i is the capacity of link *i*

et al., 2012; Tampere et al., 2007)	$I^3 = I_i^1 * \vartheta(q - 2500)$ $I^4 = I^1 \times q$ $I_i^5 = I_i^2 \times q_i \times \sum I_j^1$ $I_i^6 = I_i^3 \times q_i \times \sum I_j^1$ $I_i^7 = \sum I_j^1$ $I^8 = \frac{q}{C}$ $I^9 = q_i - C_i^b$	C_i^b is the remaining capacity at blocking T_b is the time it takes for the tail of the queue to reach the upstream junction
Network Robustness Index (Scott et al., 2006)	$NRI_k = \sum_i t'_i \times v'_i - \sum_i t_i \times v_i$	k Is the link blocked $t'_i$is the travel time of link i when link $k$is blocked v'_i is the traffic volume of link i when link $k$is blocked $t_i$is the travel time of link i when no links are blocked v_i is the traffic volume of link i when no links are blocked

Table 2-7: Network Performance Measures

Measures	**Function**	**Definitions**	**Direction of Optimization**
Mobility			
Total Travel Time	$\sum_{i=1}^{n} tt_i * x_i$	tt_i is the travel time on link *i* x_i is the flow on link *i* n is the number of links	Minimize
Total User Lost Time	$\sum_{i=1}^{n} \left(tt_i - tt_f\right) * x_i$	tt_i is the travel time on link *i* tt_f is the free flow travel time on link *i* x_i is the flow on link *i* n is the number of links	Minimize
Average Travel Time (David L Alderson et al., 2011; Berdica and Mattsson, 2007)	$\frac{\sum_{i\in O,j\in D} t_{ij}x_{ij}}{\sum_{i\in O,j\in D} x_{ij}}$	t_{ij} is the travel time between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Minimize
Average Trip Length (Berdica and Mattsson, 2007)	$\frac{\sum_{i\in O,j\in D} d_{ij}x_{ij}}{\sum_{i\in O,j\in D} x_{ij}}$	d_{ij} is the travel distance between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Minimize
Average Travel Speed (Berdica and Mattsson, 2007)	$\frac{\sum_{i\in O,j\in D} s_{ij}x_{ij}}{\sum_{i\in O,j\in D} x_{ij}}$	s_{ij} is the travel speed between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Minimize
Congested Travel (Berdica, 2002; Pratt and Lomax, 1996)	$\sum(congested\ segment\ length \times people\ vol.)$		Minimize
Accessibility			
Percentage of Highway	$L_t = \frac{L_O}{L_T} \times 100\%$	L_t is the percentage of total length of	Maximize

Operational (Zhang et al., 2010)		highway that is open in the network L_O is the total length of highway that is open in the network L_T is the total length of highway in the network	
Percentage of Travel Speed Below Acceptable Speed (Zhang et al., 2010)	$T_u = \frac{T_U}{T_T} \times 100\%$	Acceptable travel speed = 0.85*speed limit T_u is the percentage of vehicles traveling under the acceptable travel speed T_U is the number of vehicles traveling under the acceptable travel speed T_T is the total number of vehicles in the network	Minimize
Reliability			
L-M Network Efficiency Measure (Nagurney and Qiang, 2007)	$E(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}$	*n* is the number of nodes in the network d_{ij} is the shortest path between node *i* and node *j*	Maximize
Network Efficiency Measure (Nagurney and Qiang, 2007)	$\varepsilon = \varepsilon(G,d) = \frac{\sum_{w \in W} \frac{d_w}{\lambda_w}}{n_W}$	λ_w is the cost on the shortest path for OD pair *w* d_w is the demand for OD pair *w* n_W is the number of OD pairs	Maximize
Network Efficiency (Chen et al., 2012)	$E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	*r* is the origin index *s* is the destination index *i* is the traveler type q_{rs} is the mean travel demand between *r* and *s*	Maximize

		u_i^{rs} is the proportion of type *i* travelers from *r* to *s* π_i^{rs} is the minimum travel time budget between *r* and *s* for type *i* travelers	
	Resilience		
Fraction of Satisfied Demand (Miller-Hooks et al., 2012)	$\propto = E\left(\frac{\sum_{w\in W} d_w}{\sum_{w\in W} D_w}\right) = \left(\frac{1}{\sum_{w\in W} D_w}\right) \cdot \left(\sum_{w\in W} d_w\right)$	d_w is the post-disaster demand D_w is the pre-disaster demand	Minimize

2.2 Network vulnerability/resilience and game theory

This subsection of the report summarizes the game theory frameworks that have been adopted by researchers and published in the literature to model network vulnerability. As it is well known, the field of game theory covers a wide variety of applications, but any type of application will consist of the following three components: i) communication between the players, ii) order of play, and iii) amount of information. The communication between the players can be considered as cooperative or non-cooperative and transportation networks typically fall into the latter category as players cannot make agreements with each other about how they will play the game although they can make safe assumptions as to the objective that the other player(s) is trying to optimize. The order of play can be simultaneous, where all players choose an action at the same time, or sequential, where each player chooses an action after/before another player. The amount of information that is available to the players can be considered as perfect or imperfect and refers to the knowledge of the actions of other players.

In the case of transportation networks, the use of sequential games has been primarily adopted to model the dynamics of the interactions between the decision maker, the user, and a possible network interruption event. For the purposes of this research we focus on one large area of interest commonly referred to as decision maker-user games. In this research we do not consider games of the attacker-defender (Bell et al., 2008) or defender-attacker-defender (David L. Alderson et al., 2011) type (although the former can be approximated by the framework used in this research if we consider that the attacker-defender game is a zero-sum game). The rational for not considering these games is that the response of the user, which is critical in a transportation network is considered fixed (i.e., does not change with the choice of the defender or attacker) and is thus outside the scope of this research. One could estimate the response of the user for each possible feasible move of the defender and attacker but that would result in an intractable problem.

Decision maker-user games are two level hierarchical games that begin with the former player choosing an investment (or change) in the network. On the second level, the users see the network conditions and react by changing their choice of travel (including departure time, mode choice, and/or travel path choice). The user behavior is usually modeled as a traffic assignment problem and is used to evaluate the network performance. Note, that in most cases departure times and mode choice are not considered unless the decision maker is dealing with a real-time problem (e.g., evacuation). The complexity of these games lies in the estimation of the pay-off matrix which requires a significant number of traffic assignment problems to be solved. These types of models have been widely used (Farahani et al., 2013) in investment decision making (i.e., tolling systems, capital investment, operational changes) but can be easily used in estimating the vulnerability of a network and its resilience by adding capacity reduction as an option for the decision maker (i.e., how will a network behave if a subset of links is removed from the network).

2.3 Solution algorithms

It has been well recognized in the literature that modeling transportation networks with the objective or goal of identifying vulnerable links is a computationally intensive problem (see for example (Higgs et al., 2017, 2016; Poorzahedy and Rouhani, 2007a; Wang et al., 2015)). Most problem formulations resulted in NP-Complete or NP-Hard problems that require hybrid solutions algorithms where a traffic assignment algorithm is required to be executed multiple times (as also discussed in the previous subsection).

Research that has been published to date (to the authors knowledge) in the areas of game theory and network vulnerability (and network design in general) resulted in the development and use of custom-made (meta)heuristic algorithms or the use of simulation to deal with the complexity issue and address uncertainty. Table 2-8 presents a review of metaheuristics approaches from the literature for these types of problem. Note, that even though the list in Table 2-8 is not exhaustive, the algorithms follow the typical (random) descent search that is very commonly used in optimization to address the issue of solving NP problems. Most algorithms developed and published in the literature adopt a sequential approach where at set of links (selected randomly or based on a set of a-priori criteria e.g., total volume, number of paths a link belongs to etc.) are selected and removed from the network (or their capacity is reduced) followed by the solution of a traffic assignment for the new network to estimate the various performance measures. In most of the cases, the traffic assignment is performed at the macroscopic level as doing so at the meso- or microscopic level becomes intractable. A description of the traffic assignment algorithms is beyond the scope of this research and we refer for more details for these solutions algorithms to (Barceló, 2010).

Table 2-8: Metaheuristic algorithms examples

Single solution based metaheuristics	Descent local search (LS)		(Patriksson and Rockafellar, 2002)
	Simulated Annealing (SA)		(Parvaresh et al., 2014; Zhao and Zeng, 2006)
	Tabu Search (TS)		(Flisberg et al., 2009; Mouskos, 1991; Parvaresh et al., 2014; Poorzahedy and Rouhani, 2007a)
Population-based metaheuristics	Evolutionary algorithms:	Genetic Algorithms (GA)	(Cao et al., 2013; Mathew and Sharma, 2006; Sharma and Mathew, 2011)
		Evolutionary Strategies (ES)	(Dimitriou and Stathopoulos, 2009)
	Ant Colonies (AC)		(Gallo et al., 2012; Yun-peng et al., n.d.)
	Scatter Search (SS)		(Gallo et al., 2012, n.d.)
	Particle Swarm Optimization (PSO)		(Karami and Guerrero-zapata, 2015)
	Surrogate models		(de Araújo et al., 2015)
	Hybrid meta-heuristics		(Miandoabchi et al., 2013; Poorzahedy and Rouhani, 2007b)

CHAPTER 3: CRITICAL AND VULNERABLE LINK IDENTIFICATION

In this task the research team developed and implemented a framework that can assist decision makers in identifying and ranking vulnerable and critical links of a transportation network. In this research we define a link as critical if a change in its capacity results in a high increase of total travel time for the whole network. On the other hand, a vulnerable link is defined as a link that will experience the highest increase in total travel time (as compared to a base case of normal operating conditions) when a critical link is compromised. This definition does not exclude a link of being both a critical and vulnerable link.

Given the complexity of the problem the research team developed three heuristic-based approaches to identify critical and vulnerable links on roadway transportation networks that can handle real life networks. The first two approaches are based on user response and traffic equilibrium principles (i.e., the network design problem) while the third one is based on the network topology and characteristics. All three approaches can be considered as surrogates to solving a full network design problem that is not practical (due to the complexity and solution time) for real life networks.

The first heuristic-based approach (from now on referred to as Greedy Search Based heuristic or GSB) ranks each link based on a weighted combination of user defined attributes (e.g., car flows, truck flows, capacity, Volume to Capacity (VC) Ratio etc.). Once the links have been ranked a User Equilibrium (U.E.) traffic assignment is performed with a reduced capacity (defined by the user) for the top *n* links (*n* is provided by the user) in isolation and/or in combination to evaluate the new state of the transportation network. This approach can be considered as a surrogate for an attacker that does not have the capability of formulating and solving the network design problem. It is thus safe to assume that such an attacker would target links with the highest flow and/or capacity. As we will see in the results presented in the next subsection, such lack of knowledge leads to ineffective attacks.

The second heuristic-based approach is based on assumption that the importance of link depends on the number of k-shortest path it belongs to. In this research parameter k is an input from the user and thus multiple link ranking can be identified for multiple values of k. More detail is provided in Appendix A where the GIS tools are described with accompanying examples. This approach can be considered as a surrogate for an attacker similar to that considered in the first heuristic but also has no knowledge on traffic data and/or network attributes that may affect traffic conditions. It is assumed that the attacker can obtain data for the network location (which is the basic information required for this heuristic) from open data sources (e.g., Google Maps, the freight analysis framework website etc.).

The third, and the final, heuristic-based approach assumes the presence of an intelligent attacker that has full knowledge of the network state (e.g., number of lanes, capacity, demand) and also the capability of formulating and solving a network design problem to identify which links should be compromised (i.e., capacity reduction), to maximize the total travel time experienced by all the users.

3.1 Traffic Assignment Algorithm

In this research the U.E. traffic assignment was performed using the Slope-based Path Shift-propensity Algorithm (SPSA) developed by (Kumar and Peeta, 2014). SPSA was proposed to devise a traffic assignment algorithm capable of generating a precise solution at moderate computational effort while maintaining simplicity of execution for practice. It is an iterative algorithm and its convergence is theoretically proven. It uses the concepts of the path shift-propensity factor and the sensitivity of path costs with respect to path flows in the flow update process. The path shift-propensity factor is defined as the difference between the cost of a path and the cost of the cheapest path for the related Origin-Destination (O-D) pair. The slope of the path cost function is used as the measure of sensitivity of path costs with respect to path flow. The SPSA algorithm starts with an all-or-nothing (AON) assignment or a warm start using a previously known approximate solution as initialization. If the initial solution does not satisfy the convergence criteria, then the SPSA flow update process is initiated. The SPSA equilibrates one O-D pair at a time in a sequential manner. The equilibration process updates path flows to decrease the cost differences of paths with non-zero flows between an O-D pair. For this purpose, it divides the set of paths between an O-D pair into two subsets: a set of costlier paths and set of cheaper paths. Then flows are shifted from the set of costlier paths to the set of cheaper paths. It uses a line search to decide the optimal step size, which determines the extent of flow shifts along the move direction. The move direction is determined by the vector of path shift-propensity factors and the slopes of the path cost function. The sequential approach helps achieve faster convergence, but it may introduce an order bias leading to solution noise. This issue is tackled partially by updating the path sets simultaneously for all the O-D pairs before commencing the flow shifts for the O-D pairs at each iteration. In this sense SPSA combines merits of simultaneous and sequential approaches. The simultaneous path set update also helps to decrease the computational cost, especially for large-scale networks. Once an O-D pair is equilibrated using the SPSA flow update mechanism, then the next O-D pair in the sequence is brought into the equilibration process. Once all the O-D pairs are equilibrated, the convergence criterion is checked. If it is satisfied, the algorithm is terminated, else the next iteration is initiated. The convergence criterion adopted in this research is a relative gap (Rgap) of 1.0E-6. Rgap defines the distance of the solution from the optimum.

Here it is imperative to mention an important limitation from an implementation perspective arising due to non-uniqueness of the UE path flows. UE path flows are theoretically non-unique. Different solution algorithms can result in different path flows. Even multiple runs of the same solution algorithm with significantly different initialization can result in a new path flow solution. Changes in the UE path flow solution can affect the value of the third I.F. This issue can be handled by using a central solution in the UE solution space that is considered as representative of the entire solution space, for example by using a maximum entropy user equilibrium (MEUE) or entropy weighted user equilibrium (EWUE) solution for the UETAP (Kumar and Peeta, 2015). We have used SPSA for solving the UETAP for simplicity as the focus of the research is on demonstrating the proposed methodology. The issues arising due to non-uniqueness of the path flow solution of UETAP can be resolved by post-processing the SPSA solution (Kumar and Peeta, 2015; Rossi et al., 1989) or by switching SPSA with another solution algorithm (e.g. TAPAS (Bar-Gera, 2010) , SOLA (Florian and Morosan, 2014)). However, for simplicity, in this research, this issue has been dealt partially by using SPSA with a warm start. SPSA is initialized through a warm start using the path flow solution from the previous iteration to improve consistency between the solutions of two consecutive iterations.

Next, we present a sample of the results (figures 3-1 through 3-32) obtained from the all three heuristics to showcase the capabilities of the software produced and the methodology. Figures presented in this chapter show the top critical links identified by the first and third heuristics for twelve cases of capacity reduction and number of links attacked. (three different capacity reductions of 100%, 90% and 80% for any link that was compromised and four cases of different number of links that could be compromised i.e., 5, 10, 15 and 20 links). For the second heuristic the top 5, 10, 15, and 20 links based on the k-shortest path (demand weighted and unweighted) are presented. More figures can be produced by using the geodatabase that is available with this report. Note, that the links shown are the ones appearing at the top of the list. Other sets of links that can result in similar (or even the same) network conditions do exist. In Chapter 4, a model and methodology are presented to account for all the possible sets of links to be attacked and estimate the probability that a link will be attacked.

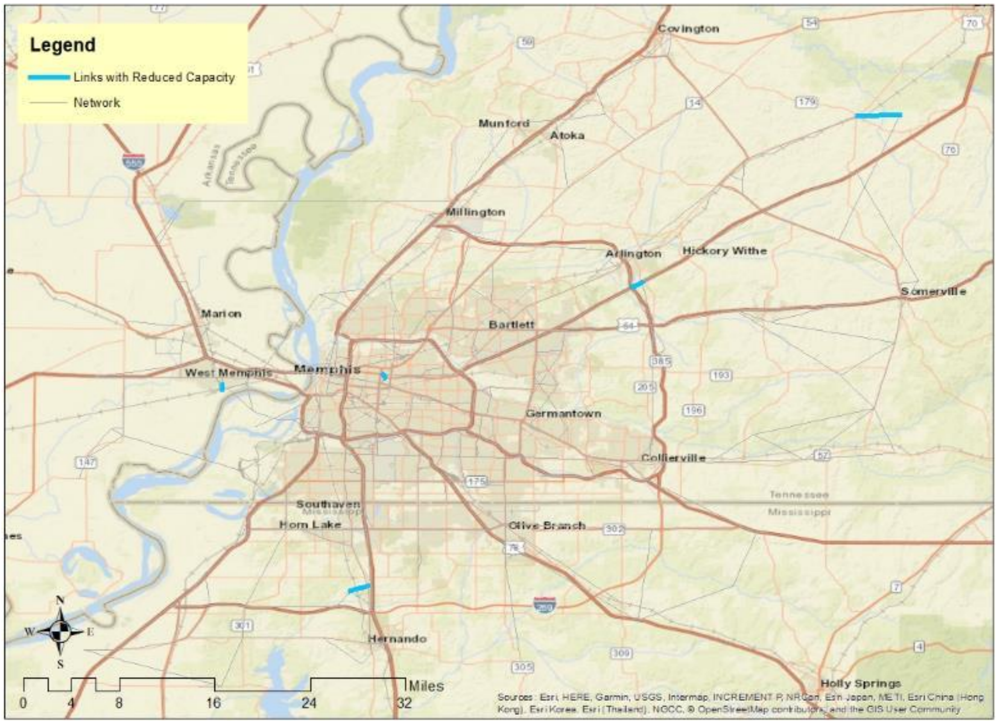


Figure 0-1. Case 1: GSB Based Top 5 Critical Links.

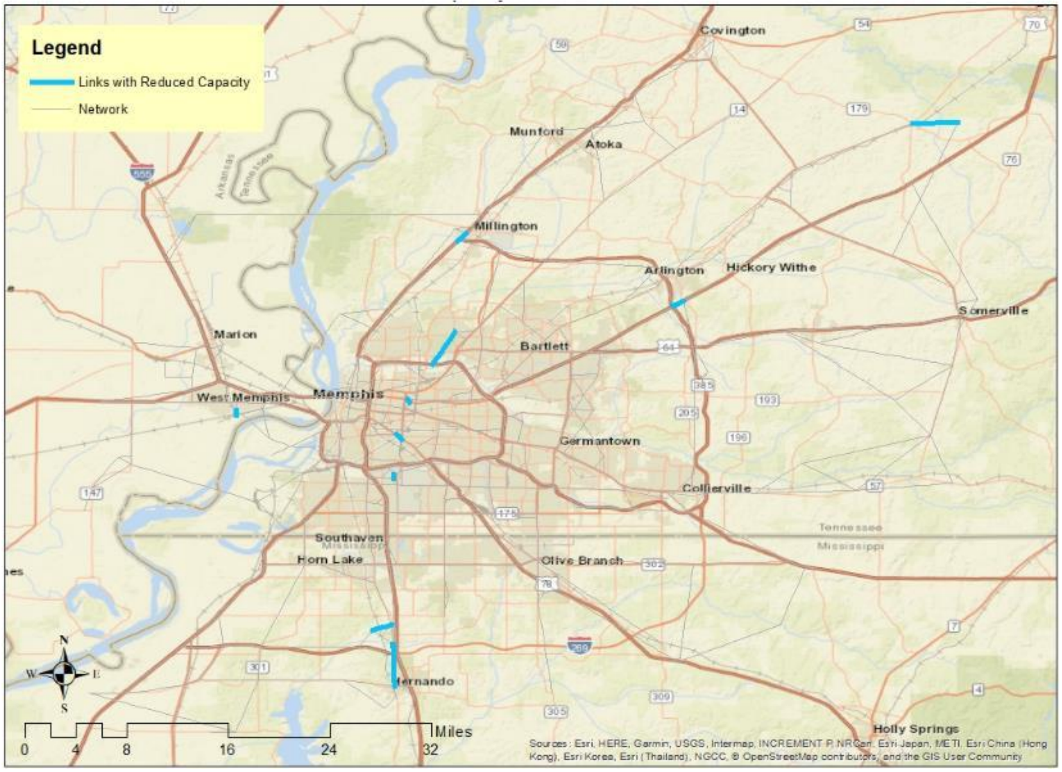


Figure 0-2. Case 2: GSB Based Top 10 Critical Links.

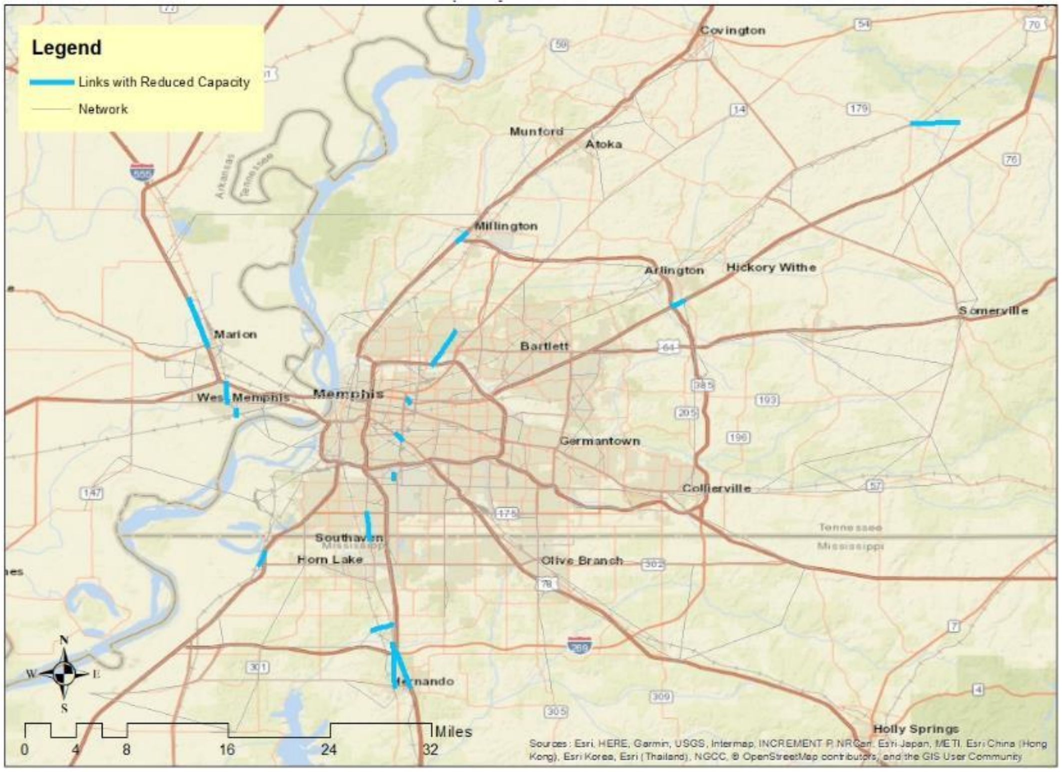


Figure 0-3. Case 3: GSB Based Top 15 Critical Links.

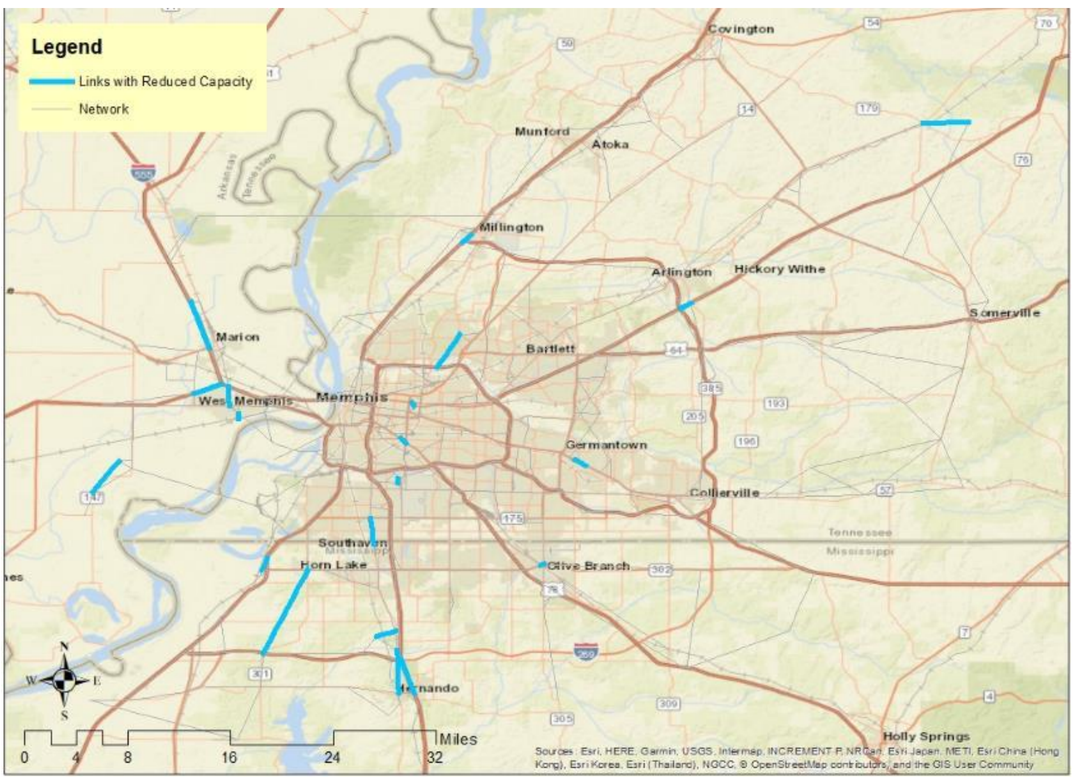


Figure 0-4. Case 4: GSB Based Top 20 Critical Links.

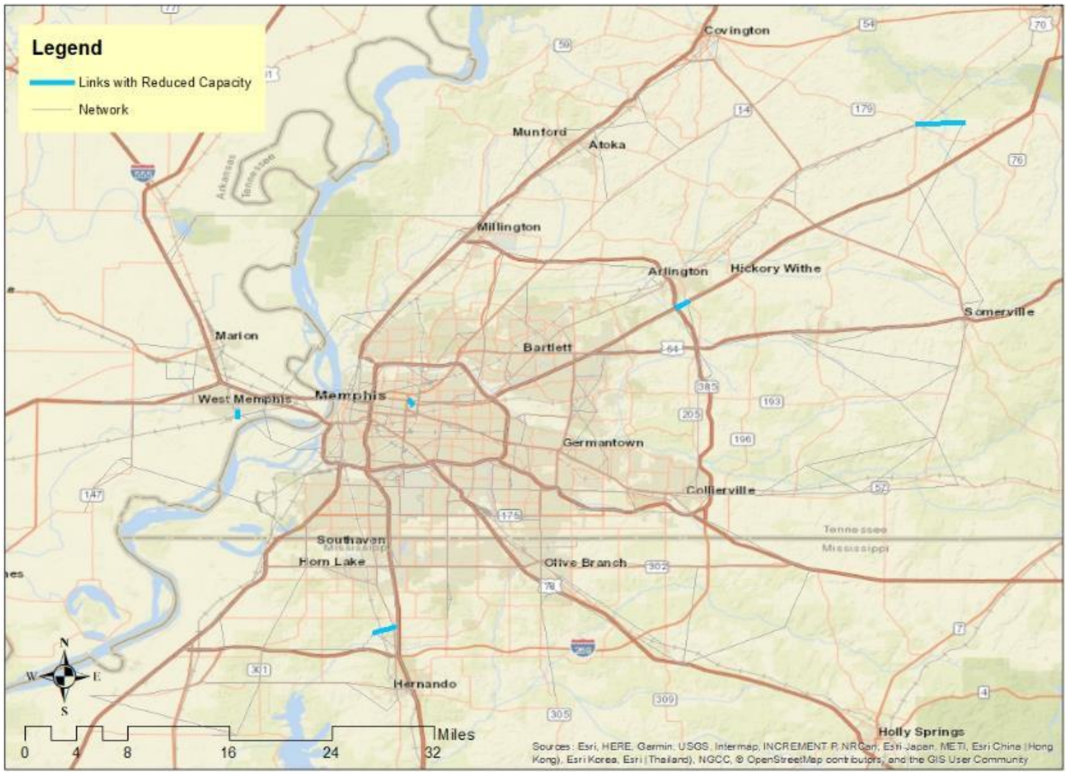


Figure 0-5. Case 5: GSB Based Top 5 Critical Links.

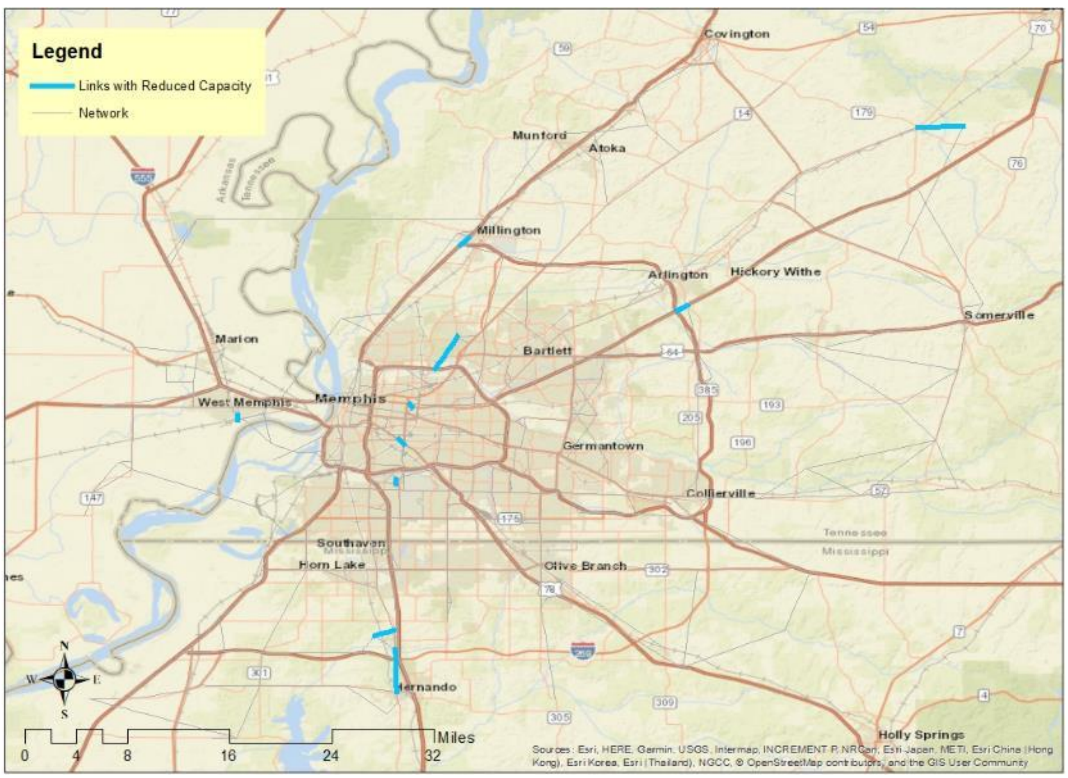


Figure 0-6. Case 6: GSB Based Top 10 Critical Links.

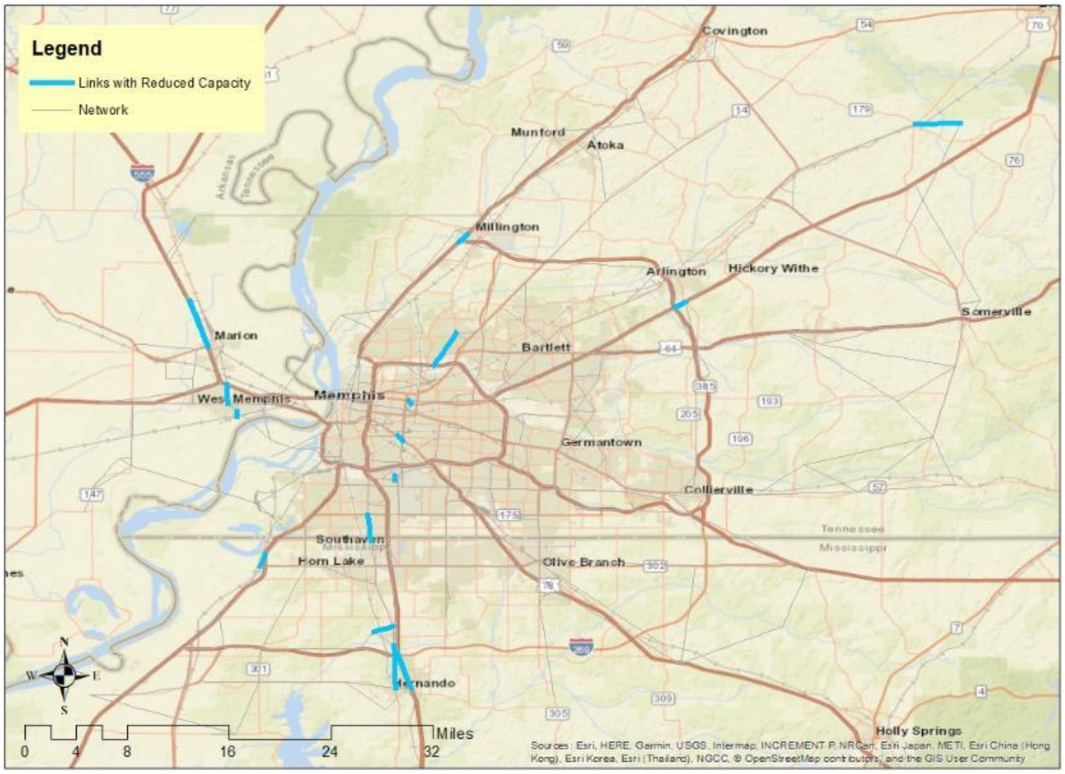


Figure 0-7. Case 7: GSB Based Top 15 Critical Links.

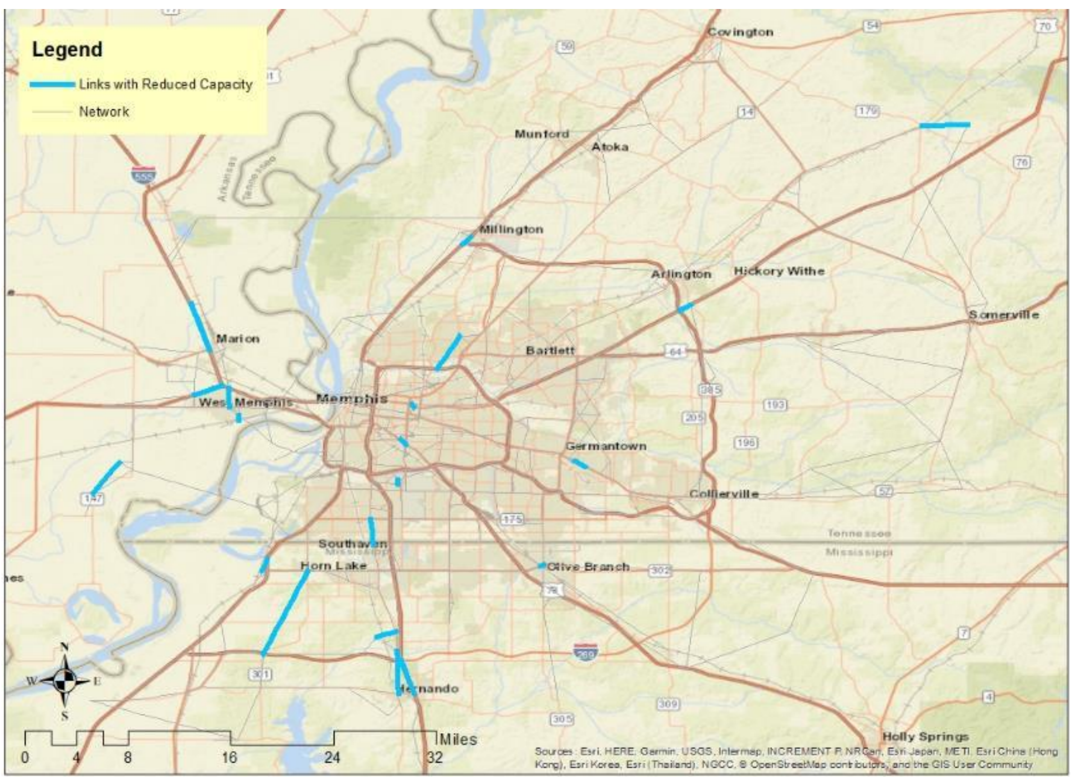


Figure 0-8. Case 8: GSB Based Top 20 Critical Links.

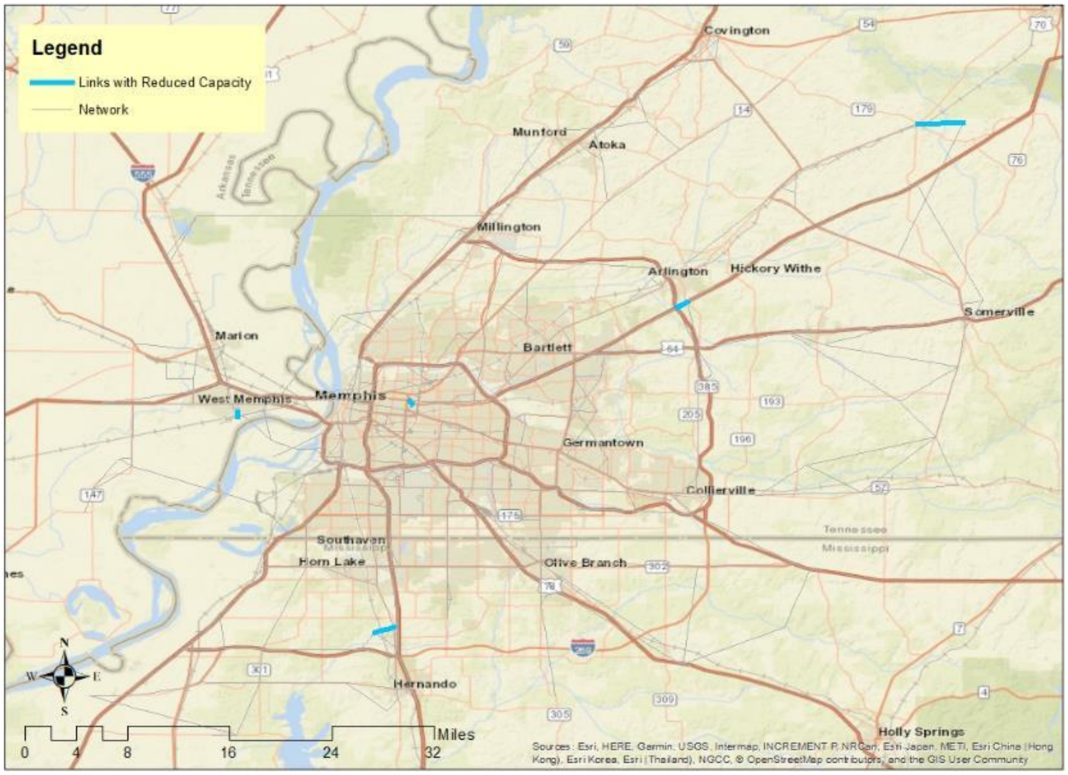


Figure 0-9. Case 9: GSB Based Top 5 Critical Links.

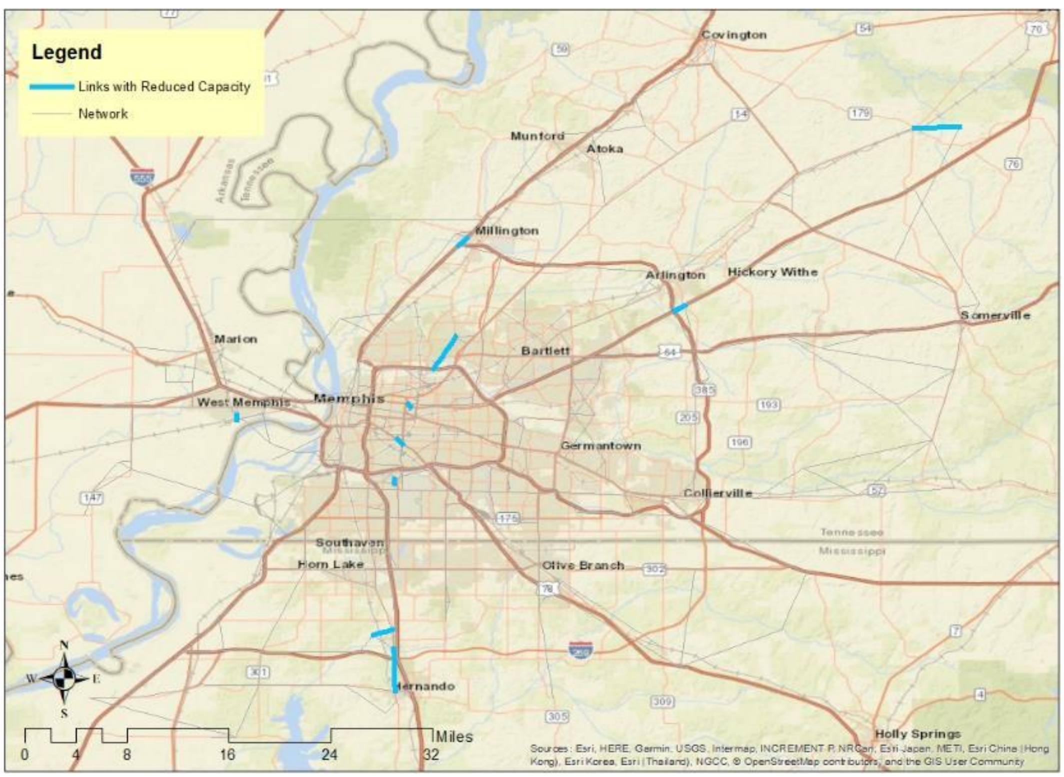


Figure 0-10. Case 10: GSB Based Top 10 Critical Links.

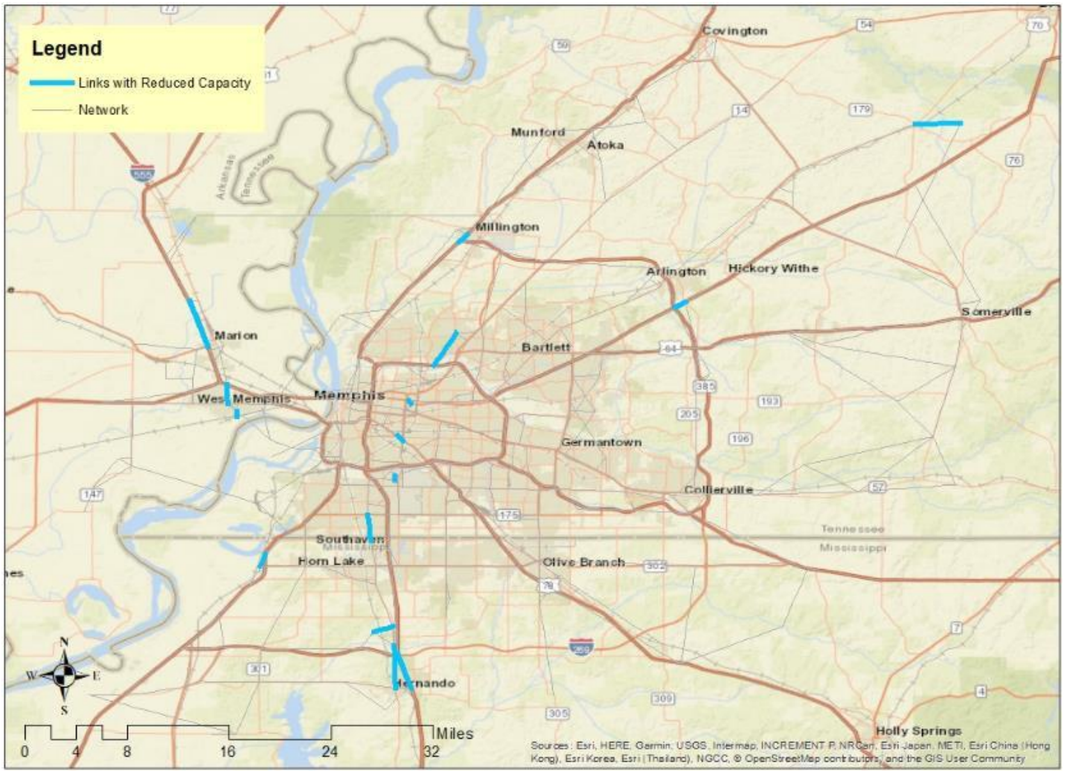


Figure 0-11. Case 11: GSB Based Top 15 Critical Links.

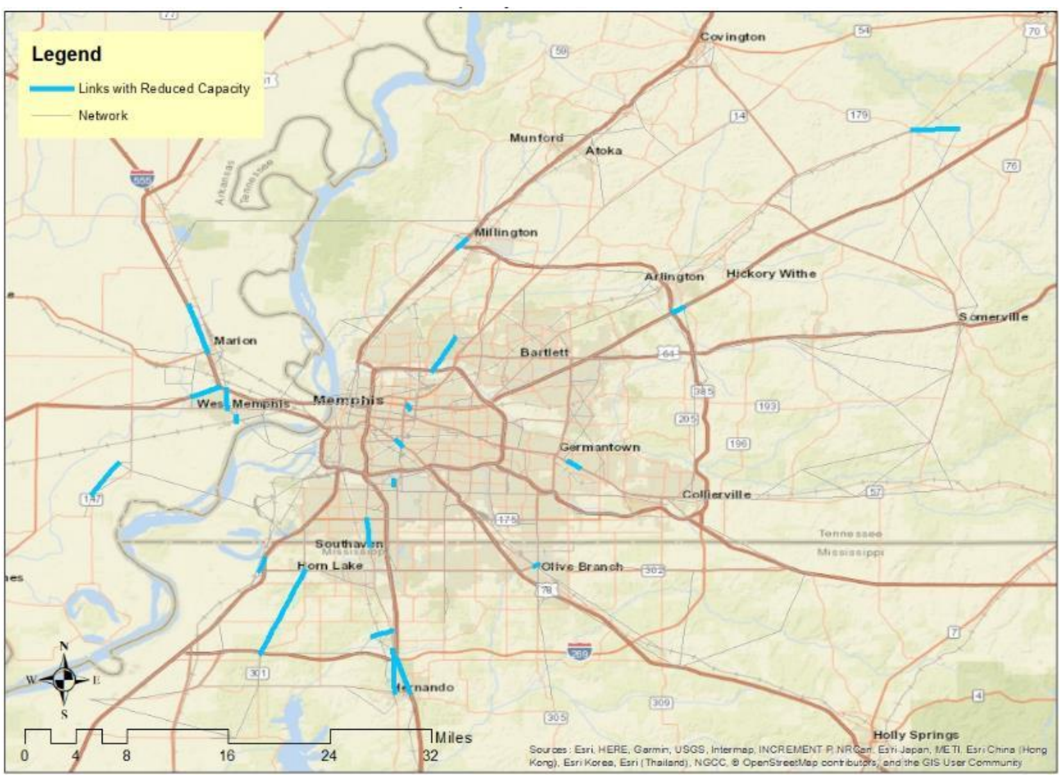


Figure 0-12. Case 12: GSB Based Top 20 Critical Links.

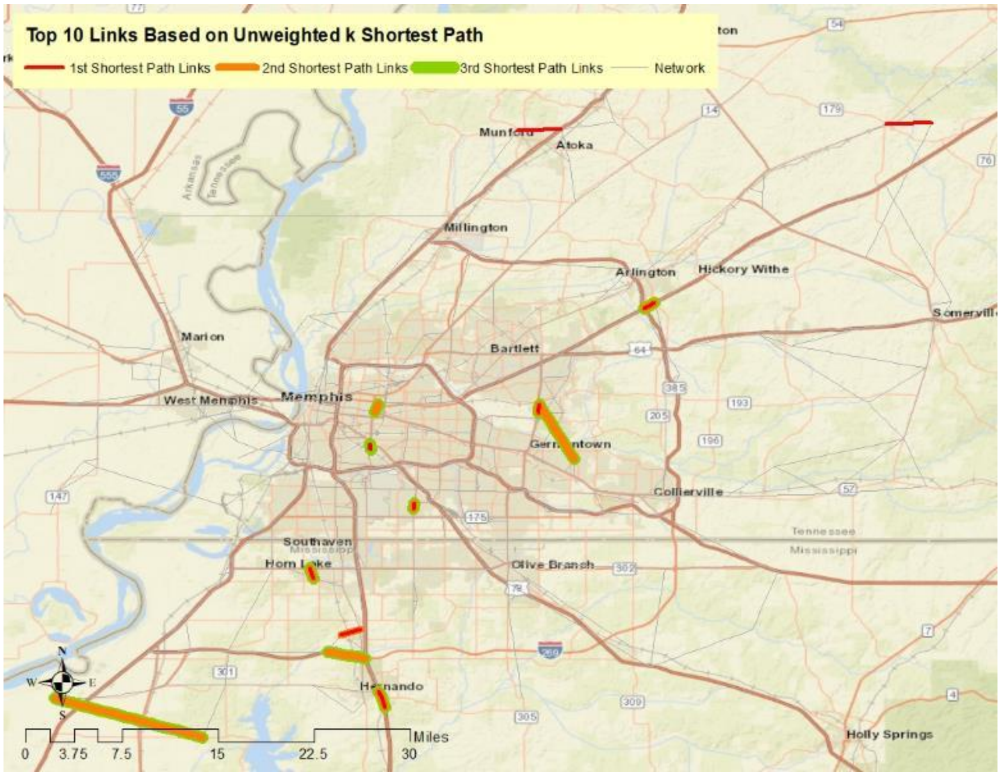


Figure 0-13. Top 10 Links Based on Unweighted k Shortest Path.

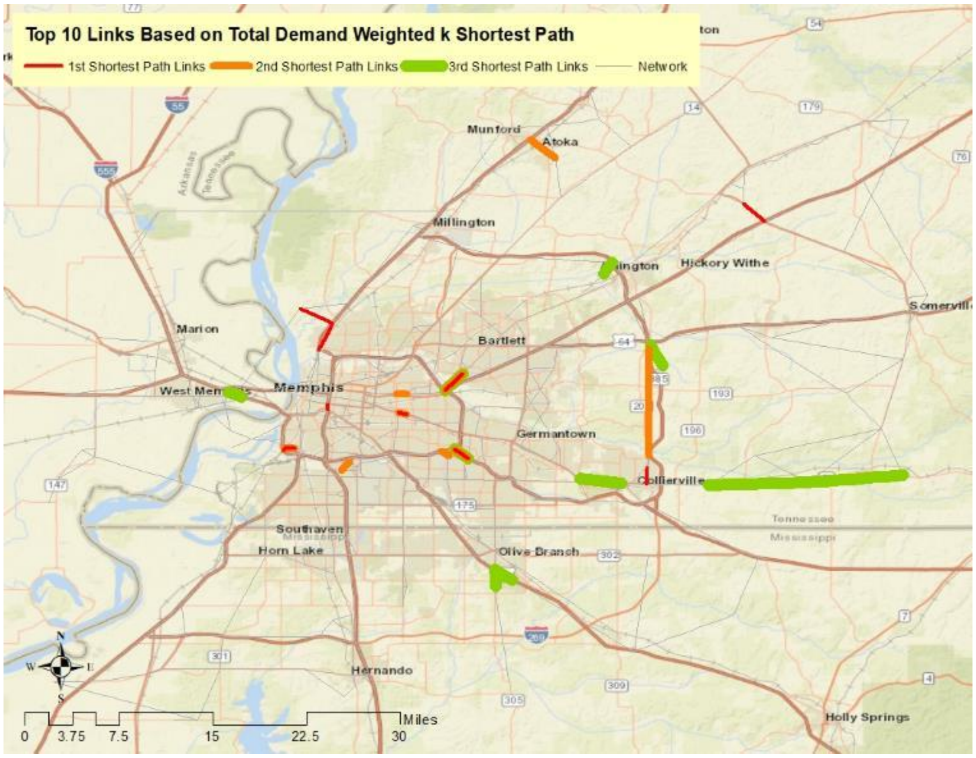


Figure 0-14. Top 10 Links Based on Demand Weighted k Shortest Path.

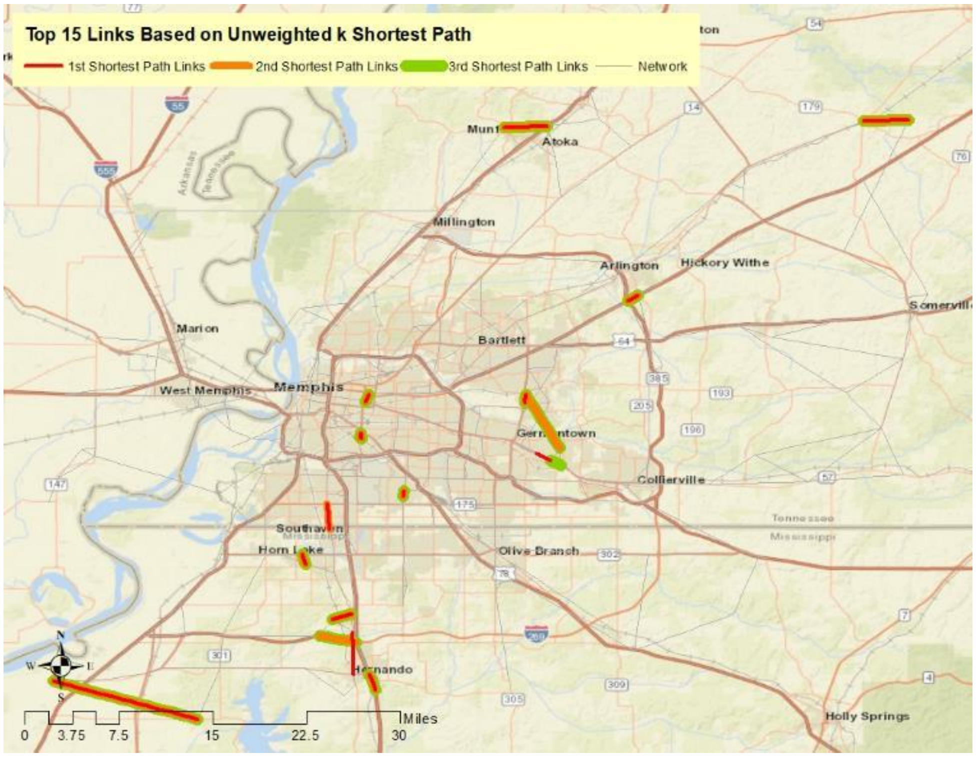


Figure 0-15. Top 15 Links Based on Unweighted k Shortest Path.

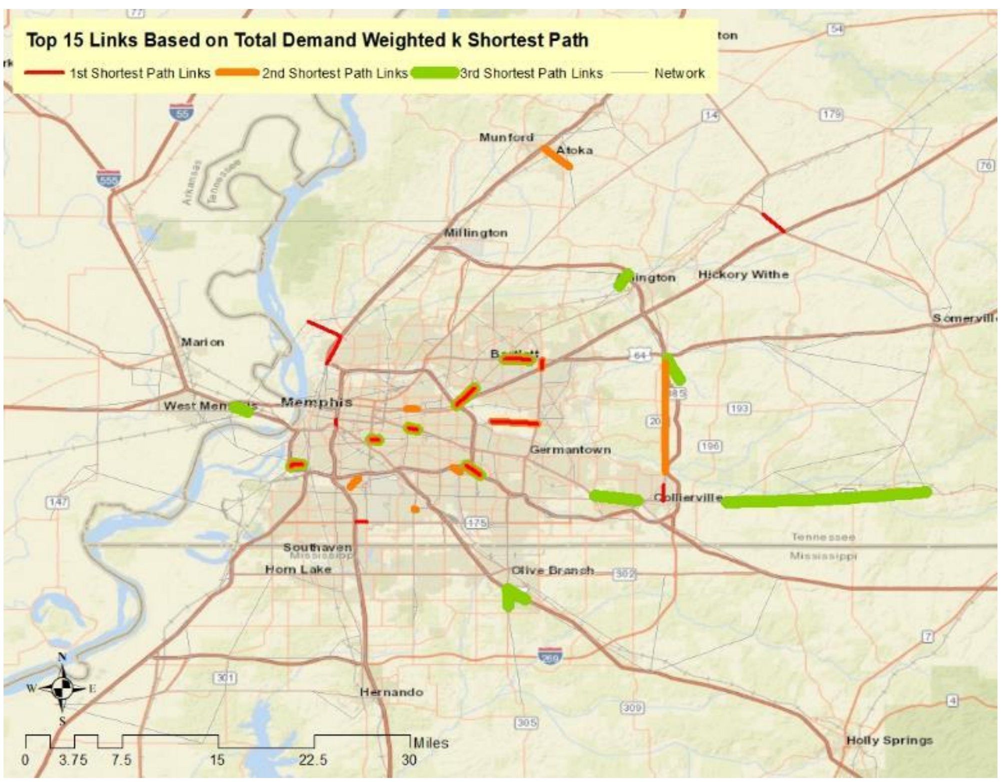


Figure 0-16. Top 15 Links Based on Demand Weighted k Shortest Path.

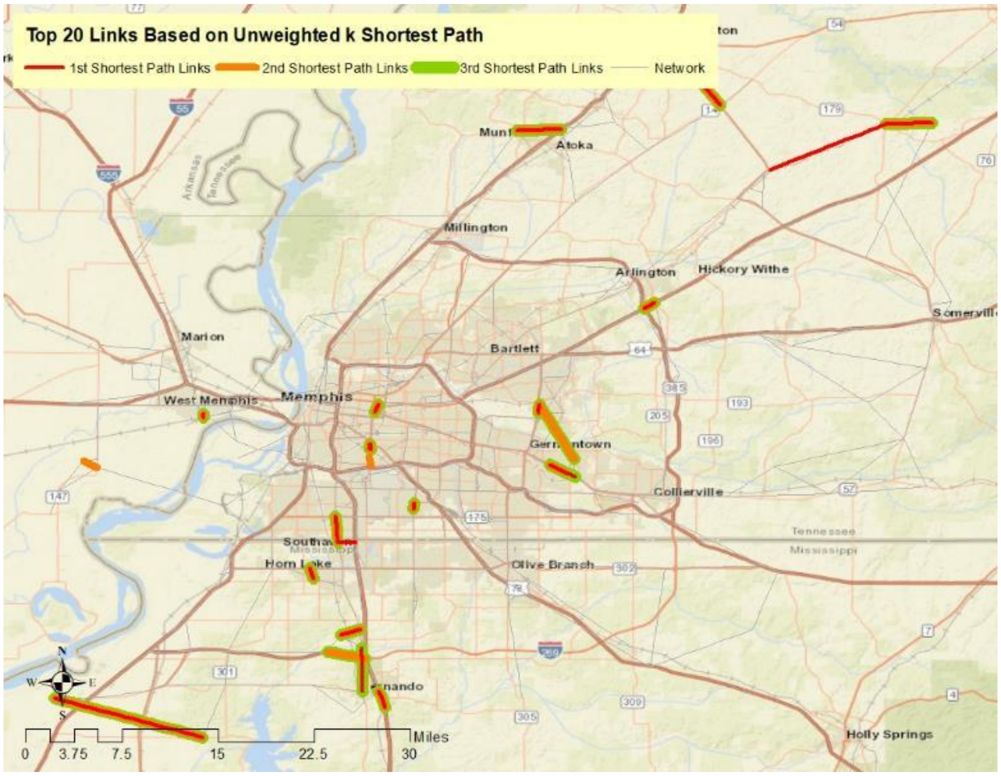


Figure 0-17. Top 20 Links Based on Unweighted k Shortest Path.

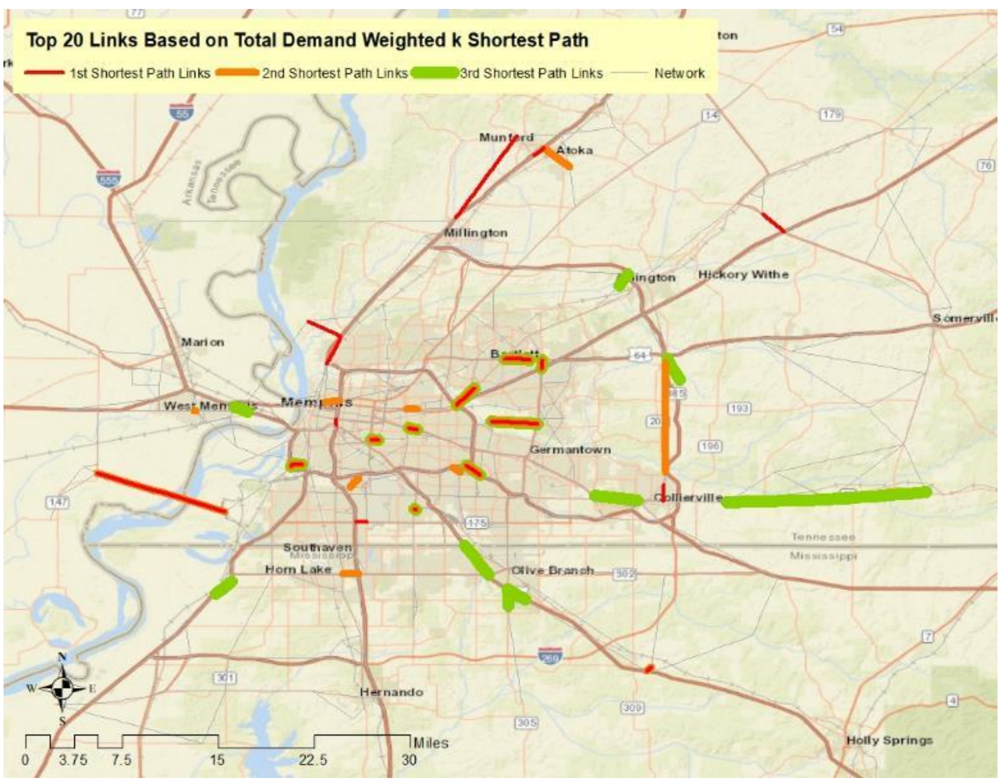


Figure 0-18. Top 20 Links Based on Demand Weighted k Shortest Path.

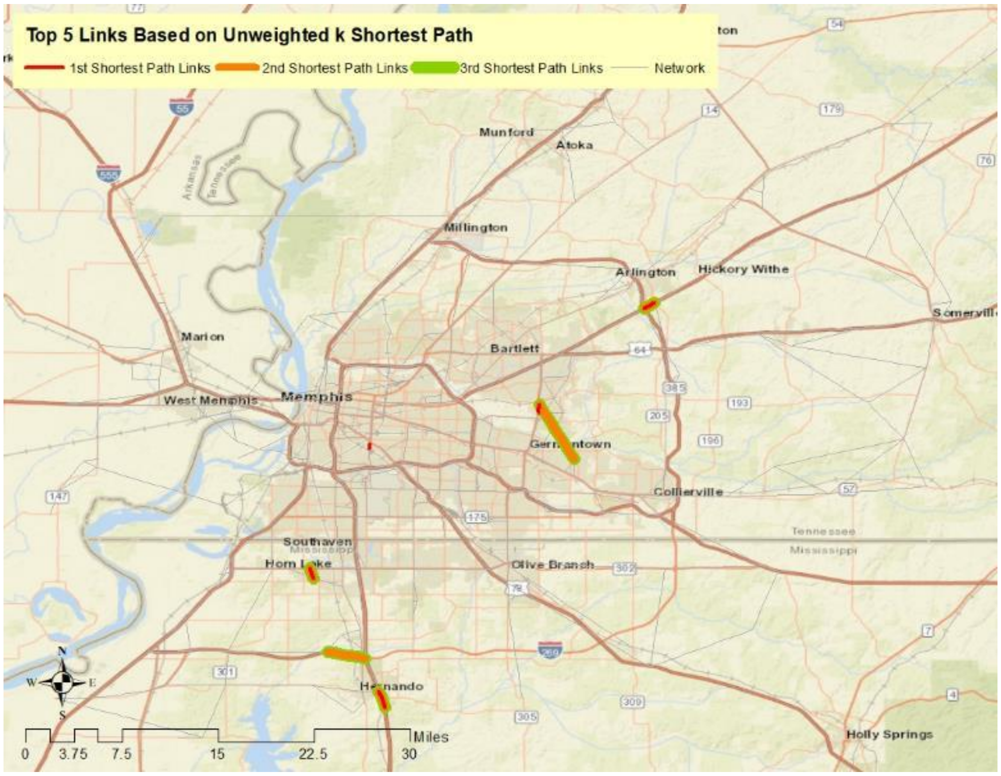


Figure 0-19. Top 5 Links Based on Unweighted k Shortest Path.

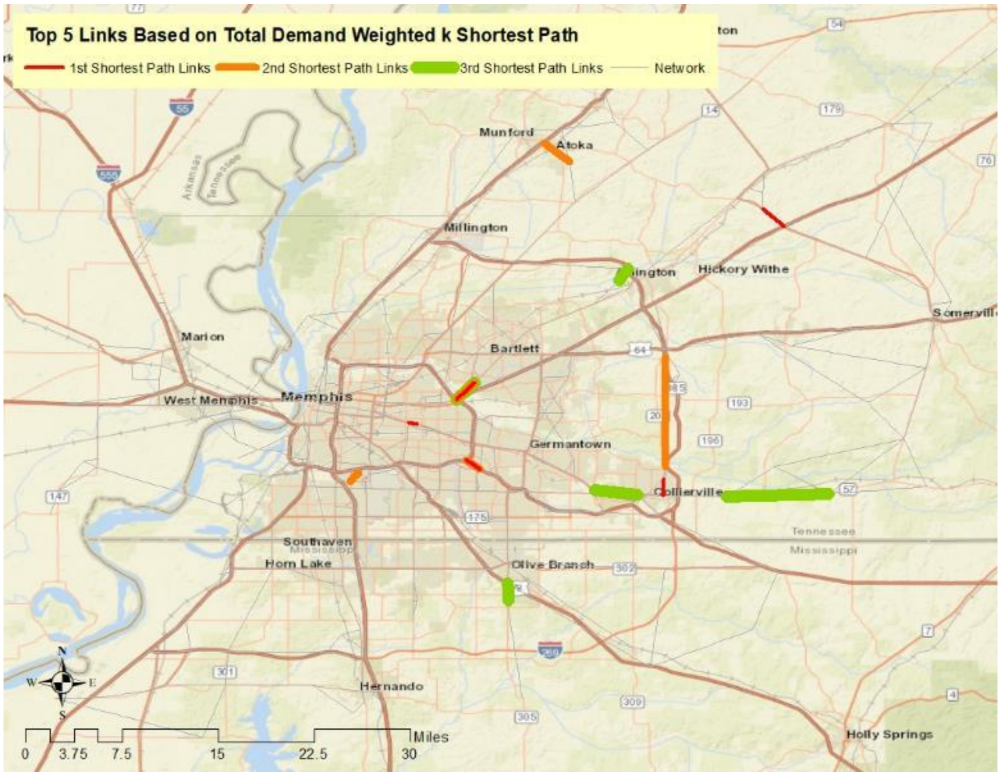


Figure 0-20. Top 5 Links Based on Demand Weighted k Shortest Path.

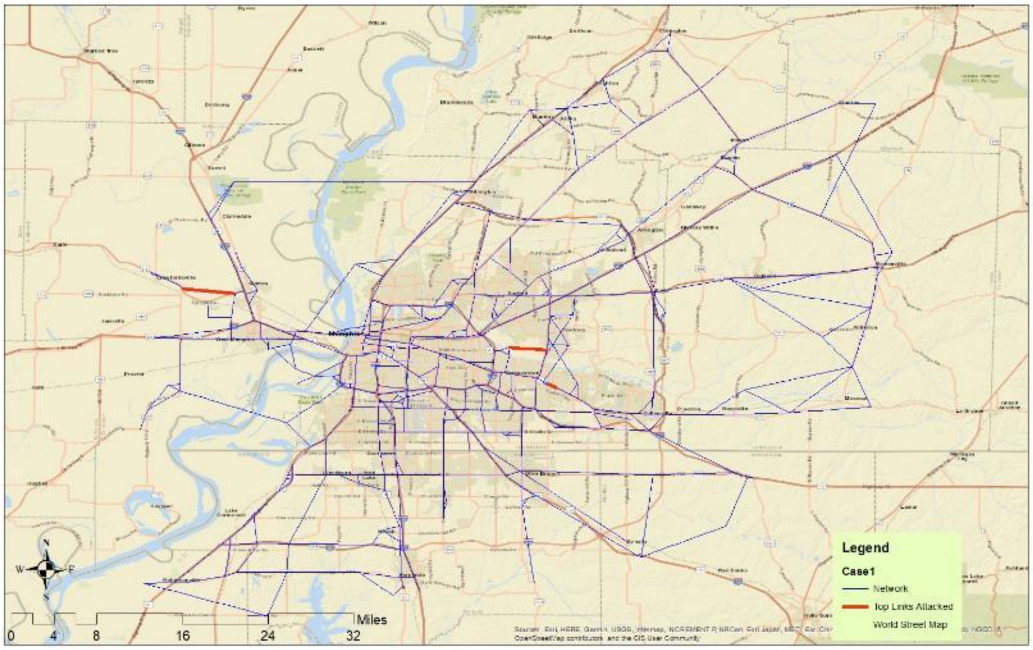


Figure 0-21. RSH Top 5 Links Attacked: Case 1.

Figure 0-22. RSH Top 10 Links Attacked: Case 2.

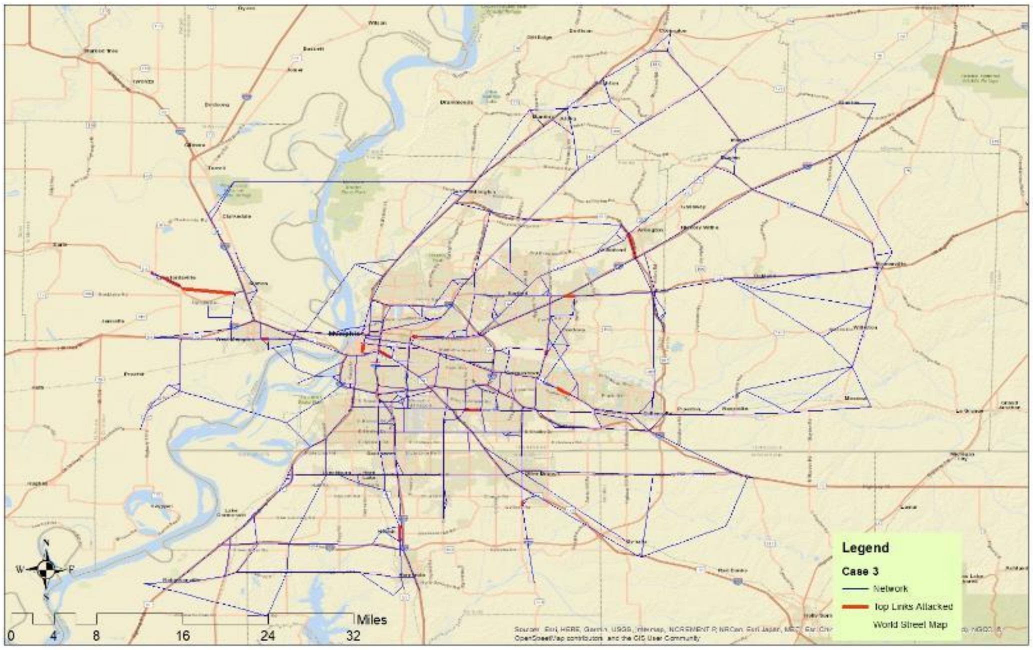


Figure 0-23. RSH Top 15 Links Attacked: Case 3.

Figure 0-24. RSH Top 20 Links Attacked: Case 4.

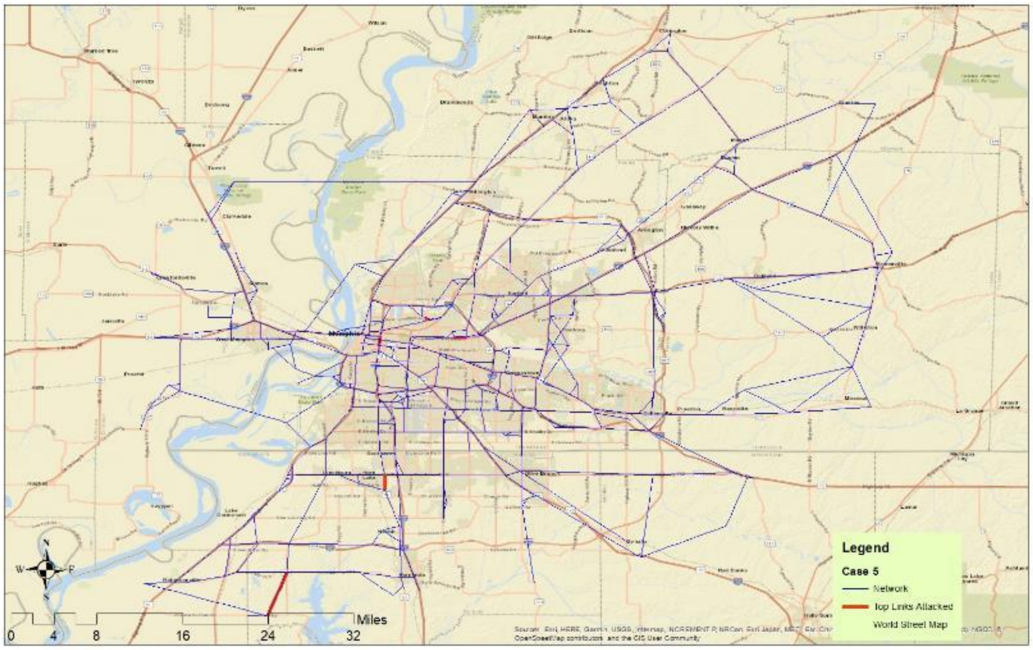


Figure 0-25. RSH Top 20 Links Attacked: Case 5.

Figure 0-26. RSH Top 20 Links Attacked: Case 6.

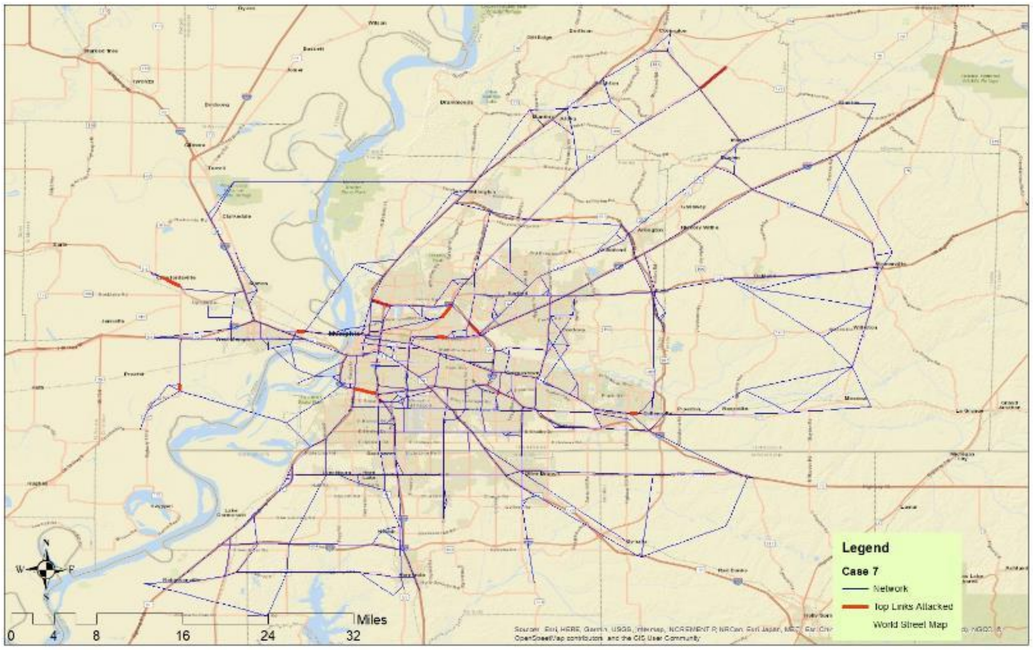


Figure 0-27. RSH Top 20 Links Attacked: Case 7.

Figure 0-28. RSH Top 20 Links Attacked: Case 4.

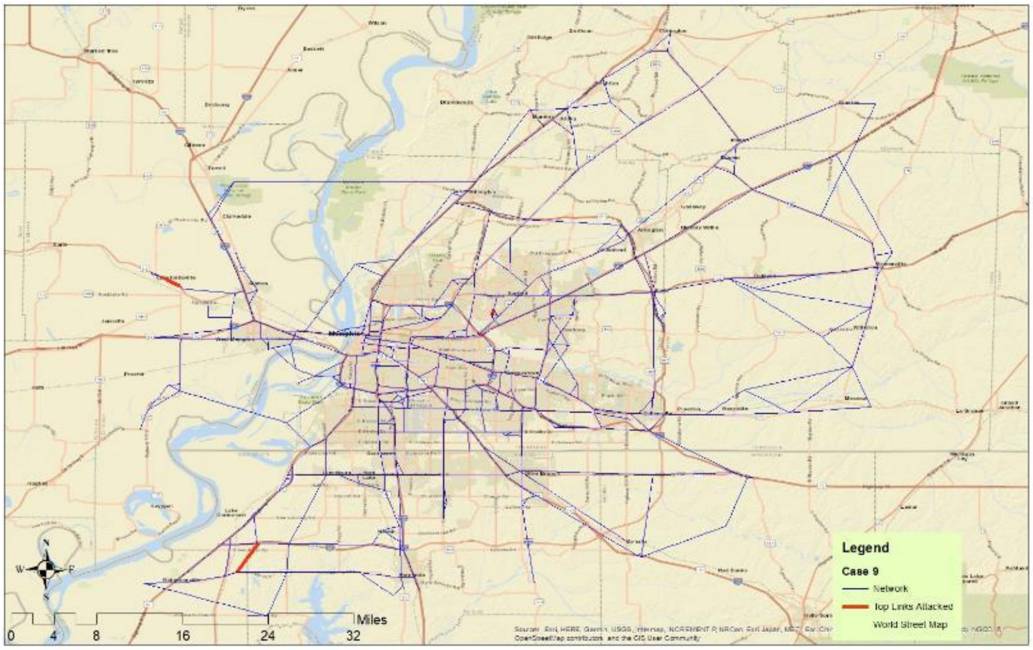


Figure 0-29. RSH Top 5 Links Attacked: Case 9.

Figure 0-30. RSH Top 10 Links Attacked: Case 10.

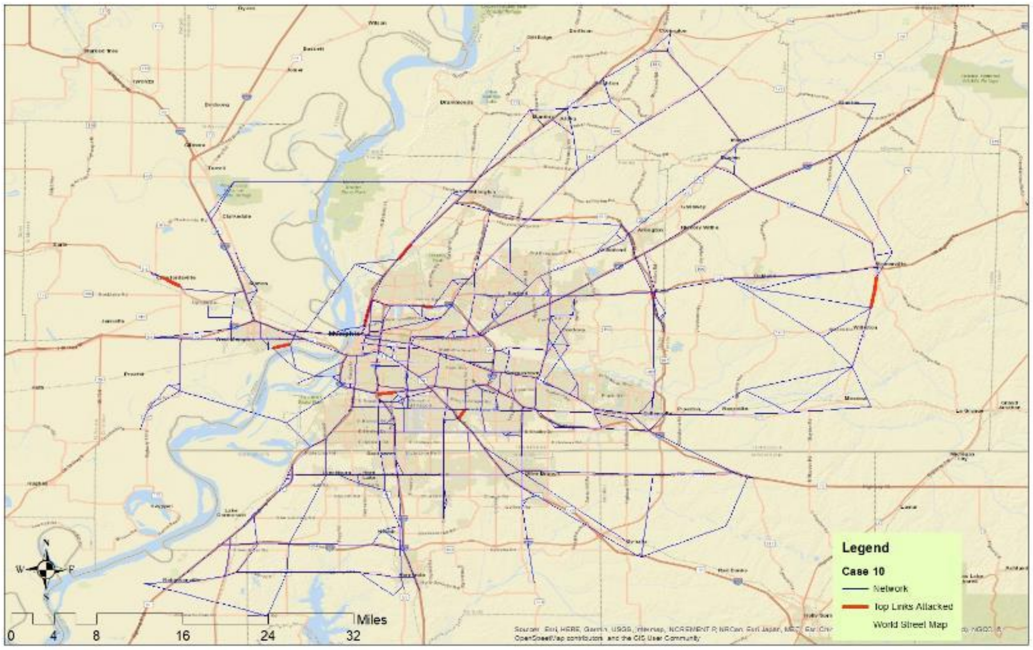


Figure 0-31. RSH Top 15 Links Attacked: Case 11.

Figure 0-32. RSH Top 20 Links Attacked: Case 12.

CHAPTER 4: CRITICAL AND VULNERABLE LINK RANKING

In this chapter we present the methodology developed to help decision makers with formulating an optimal investment plan to maximize network resilience against attacks on the network. The model presented in this section does not use any input from the tools developed in Chapter 3. Instead it uses a mathematical formulation (presented) next that utilizes a game theory framework to identify how many and which links need to be protected by the decision maker in case of an attacker presence. The model can be implemented by introducing knowledge about the attacker. For example, if the attacker is a natural event the links to be attacked can be links that are more likely to fail due to the event. In the case of a man-made attack, the defender may assume limited knowledge of the network by the attacker and consider as candidate links for attack specific functional class links (e.g., freeways or highways).

In this research, we assume that the decision maker can protect more links than the attacker can compromise. The proposed mathematical formulation assumes multiple objectives for both the decision maker and the attacker (Golias and Higgs, 2016) but only one is used in the numerical examples (the most common one). More details are provided in the numerical experiments and results section. Due to the complexity of the solution algorithm the mathematical model presented herein was not implemented in ArcGIS as is uses two software that require commercial licenses, to develop GUI (Graphical User Interface) and DLL (Dynamic Linked Libraries) that can be introduced into ArcGIS, that the research team do not possess. The research team invested a significant amount of effort in developing heuristic solution algorithms using freeware software, but the results were not promising, and a decision was made to use the commercial software. Next, we present the nomenclature, followed by the mathematical model and results.

Nomenclature

Variable	Meaning
O	Set of objective functions
M	Set of modes
x_{am}	Traffic flow on link a by mode m

y_a	Binary decision to either do nothing (0) or attack link a (1)
z_a	Binary decision to either do nothing (0) or defend link a (1)
$G_i(x,y,z)$	Objective function $i \in O$ of the upper level player (defender)
$F_j(x,y,z)$	Objective function $j \in O$ of the upper level player (defender)
c_a^D	Cost to defend link a
c_a^{IA}	Cost to attack link a
B^D	Number of links that can be defended
B^{IA}	Number of links that can be attacked
$t_a(x,y,z)$	The travel time function
q_{rsm}	The demand for travel from origin r to destination s by mode *m*
f_k^{rsm}	The traffic volume for path k between origin r to destination s by mode *m*
δ_a^{krs}	The binary path incidence for link a if it occurs on path k between origin r to destination s (1) or not (0)

4.1 Mathematical model formulation

The formulation for the multi-level multi-objective game theory framework is presented below.

$$\min_{x,y,z}\{G_i(x,y,z)\} \tag{1}$$

s.t.

$$\sum_a z_a c_a^D \le B^D \tag{2}$$

$$z_a = \begin{cases} 1, if\ link\ a\ is\ protected\ by\ the\ defender \\ 0, otherwise \end{cases} \tag{3}$$

s.t.

$$\max_{x,y}\{F_j(x,y,z)\} \tag{4}$$

s.t.

$$\sum_a y_a c_a^{IA} \le B^{IA} \tag{5}$$

$$y_a = \begin{cases} 1, if\ link\ a\ is\ attacked\ by\ the\ attacker \\ 0, otherwise \end{cases} \tag{6}$$

$$\min_x \sum_a \int_0^{x_a} t_a(x,y,z)dx \tag{7}$$

s.t.

$$\sum_k f_k^{rsm} = q_{rsm} \qquad \forall r,s,m \tag{8}$$

$$f_k^{rs} \ge 0 \qquad \forall k,r,s \tag{9}$$

$$x_{am} = \sum_{k,r,s} \delta_a^{krs} f_k^{rsm} \qquad \forall a, m \tag{10}$$

$$\delta_a^{krs} = \begin{cases} 1, if\ link\ a\ is\ on\ path\ k \\ 0, otherwise \end{cases} \tag{11}$$

In equation (1) the upper level player (i.e., defender) minimizes objective *i* within the constraints of the total number of links that can be defended (2). In equation (3) the decision of the upper level player is shown to be binary where 1 is protection of link a and 0 is no protection of link a. In equation (4), the second level player (i.e., attacker) maximizes its own objective function *j* (which can be the same as 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 attacker is shown to be binary where 1 is an attack of link a and 0 is no attack on link a. The third and lower level player (i.e., network users) minimize the integral of the link travel times in equation (7) within constraints equation (8) and equation (9) which yields the user equilibrium. Constraint equation (8) ensures that the sum of the 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 of paths that contain that link.

4.2 Numerical examples and results

For this research project the Shelby County, TN Freight Analysis Framework 4 (FAF4) network was used as a case study for the numerical examples. A snapshot of the network can be seen in Figure 4-1. Car and truck demand was estimated using the assigned flows provided by FAF4 through a well-known Origin Destination Matrix Estimation (ODME) procedure. The TransCAD software (https://www.caliper.com/) was used to implement the ODME procedure. As previously discussed, in this research we utilized the most common objective used by MPOs, SDOTs and in general transportation planners, engineers and modelers: i.e., the total travel time experienced by all users in the network. The developed models are flexible and can utilize various other objectives with some modifications to the formulation and solution algorithms (e.g., Vehicle Miles Travelled).

Figure 4-1. Shelby County, TN FAF4 Network.

The numerical experiments consisted of three different capacity reductions of 100%, 90% and 80% for any link that was compromised and four cases of different number of links that could be compromised i.e., 5, 10, 15 and 20 links. In total 12 different cases where tested and results are shown in table 4-1. The objective function of both the defender and the attacked were assumed to be equal to the total travel time of all users. The first column of Table 4-1 shows the ratio of the number of links protected to the number of links attacked. The remaining columns show the change of the total traveled time for the compromised network as compared to the base case network (i.e., the network where all links operate at their full capacity). For example, for the first instance and for Case 5, if the defender does not protect any links (i.e., NPL/NLA=0) then after an attack that reduces the capacity of five links by 10% the total travel time will increase by approximately 152%.

Results in Table 4-1 showcase that the network is extremely vulnerable for the four first instances where the attacker can compromise a link to the extreme (i.e., remove the link completely from the network by reducing its capacity by 100%). For example, and for case 1, the defender would need to protect 50 links to obtain an operational network (that would still experience a 12% total travel time increase as compared to the base case network.

Another observation from the results shown in Table 4-1, is that for all instances and cases, the network performance decreases with the increase of the links attacked and capacity reduction. This trend is an indication of the accuracy of the model and solution accuracy and it is to be expected. Another interesting observation is that the change in the networks performance as compared to the base case does not always show a strong correlation as we introduce the defender. In other words, as we increase the ratio of the number of links protected to attacked, the network does not result in a worst or better state necessarily between the cases. There maybe two main reasons for these results: i) the solution algorithm was not able to find the global optimal solution (which in realistic cases would be infeasible due to the complexity of the problem), and ii) the well-known issue with transportation networks known as the Braess paradox where an increase in capacity results in a decrease of the networks performance. Unfortunately, there is little that can be done to address either of these two issues (at least with today's computational power and existing solution algorithms) for real life size networks like the one used in this research.

As part of this chapter, and from results obtained by the optimization model, the research team performed an analysis to identify the most critical links (i.e., links that will be attacked and need to be protected) and the vulnerable paths (i.e., paths with the highest cost increase) for the top five origin-destination pairs affected by an attack on the top ten most critical link sets. A summary of the results of this analysis is shown in figures 4-2 through 4. Figures 4-2 through 4-13 show the distribution of the link attack probability for each case. Figures 4-14 through 4-26 showcase the criticality of the links in the network by estimating the probability of an attack. Figures 4-27 through 4-75 showcase the most critical paths between the top five most affected origin-destination pairs. Results from the same analysis but considering only freight related travel times (i.e., truck total travel time or truck cost) as the objective of the attacker are shown in Figures 4-39 through 4-75.

We observe that as we decrease the attack efficiency (i.e., the link capacity reduction) the probability of a link being attacked becomes normally distributed. In other words, the more effective the attack the more concentrated on fewer links it will be. On the other hand, ineffective attacks do not show any significant preference among the links. We also observe that the main difference between the total cost and truck only cost based solutions is a higher concentration of attacks, for the latter, when the attack effectiveness decreases (i.e. there is a significant number of links that will not be attacked for cases 7 through 12 when compared with the total cost case). This is to be expected as trucks use different routes than passenger vehicles and have a more concentrated origin-destination demand.

All the results from the analysis performed in Chapter 4 have been compiled in an ArcGIS map package and are available through this link: https://www.dropbox.com/s/hxk0fwcni3jeg00/REES_36_FinalMap.mpk?dl=0

Table 4-1 Vehicle Hours Travelled Change (%): Base Case VS Attacked/Protected Network

	Capacity Reduction of Links Attacked =100%				Capacity Reduction of Links Attacked =50%				Capacity Reduction of Links Attacked =25%			
NLP/NLA	Case 1: 5 Links Attacked	Case 2: 10 Links Attacked	Case 3: 15 Links Attacked	Case 4: 20 Links Attacked	Case 5: 5 Links Attacked	Case 6: 10 Links Attacked	Case 7: 15 Links Attacked	Case 8: 20 Links Attacked	Case 9: 5 Links Attacked	Case 10: 10 Links Attacked	Case 11: 15 Links Attacked	Case 12: 20 Links Attacked
0	NF	NF	NF	NF	152	268	268	288	17	17	18	20
1	NF	NF	NF	NF	23	41	164	33	3	7	7	7
2	NF	NF	NF	NF	17	10	41	19	3	3	4	5
3	NF	NF	NF	NF	1	7	22	8	2	3	3	4
4	NF	NF	NF	NF	1	7	10	8	2	3	3	3
5	NF	NF	NF	NF	1	6	8	7	2	2	2	3
6	NF	NF	NF	NF	1	5	7	4	2	2	2	2
7	NF	NF	NF	NF	1	4	5	4	1	2	2	2
8	NF	NF	NF	NF	1	3	4	3	1	2	2	2
9	NF	NF	NF	NF	1	3	2	2	1	2	2	2
10	12	NF	NF	NF	1	2	2	2	1	1	2	2
11	10	7	NF	4	1	2	2	2	1	1	1	1
12	10	4	11	4	1	2	2	2	1	1	1	1
13	5	4	6	4	1	2	2	2	1	1	1	1
14	4	4	4	3	1	2	2	2	1	1	1	1
15	4	3	4	3	1	2	2	1	1	1	1	1
16	3	3	3	3	1	2	2	1	1	1	1	1
17	3	3	2	2	0	2	2	1	1	1	1	1
18	2	3	2	2	0	1	1	1	1	1	1	1
19	2	2	2	2	0	1	1	1	1	1	1	0
20	2	2	2	0	0	1	1	0	1	1	1	0
21	2	2	2	0	0	1	1	0	0	1	1	0
22	2	2	2	0	0	1	1	0	0	1	1	0
23	2	2	2	0	0	1	1	0	0	1	1	0

NPL/NLA: Ratio of number of links protected to number of links attacked, NF: Network Failed

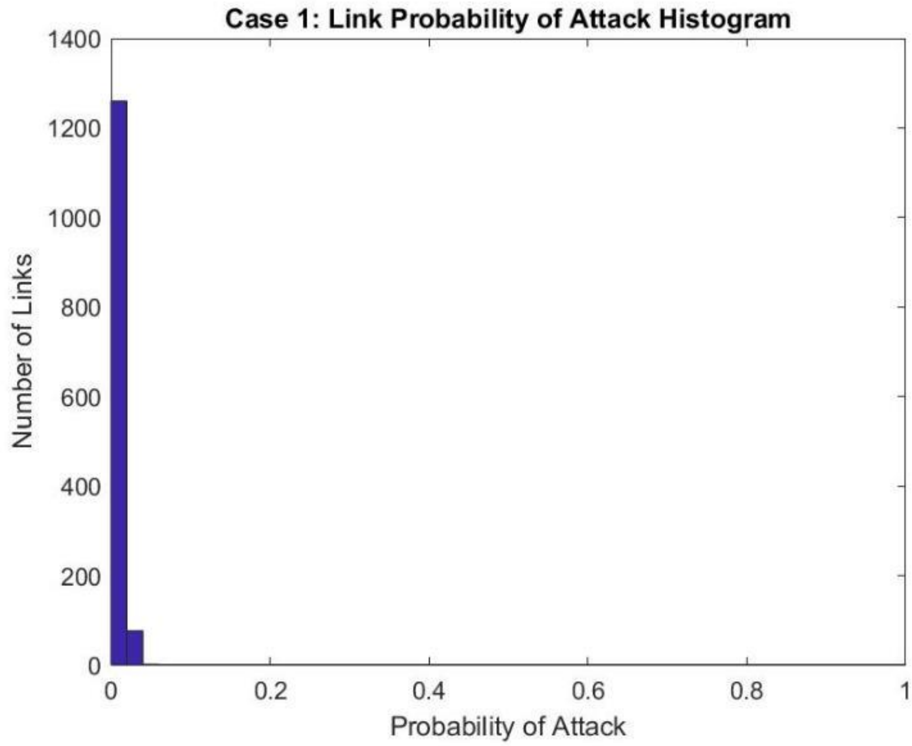


Figure 0-2. Histogram of Link Probability of Attack for Case 1.

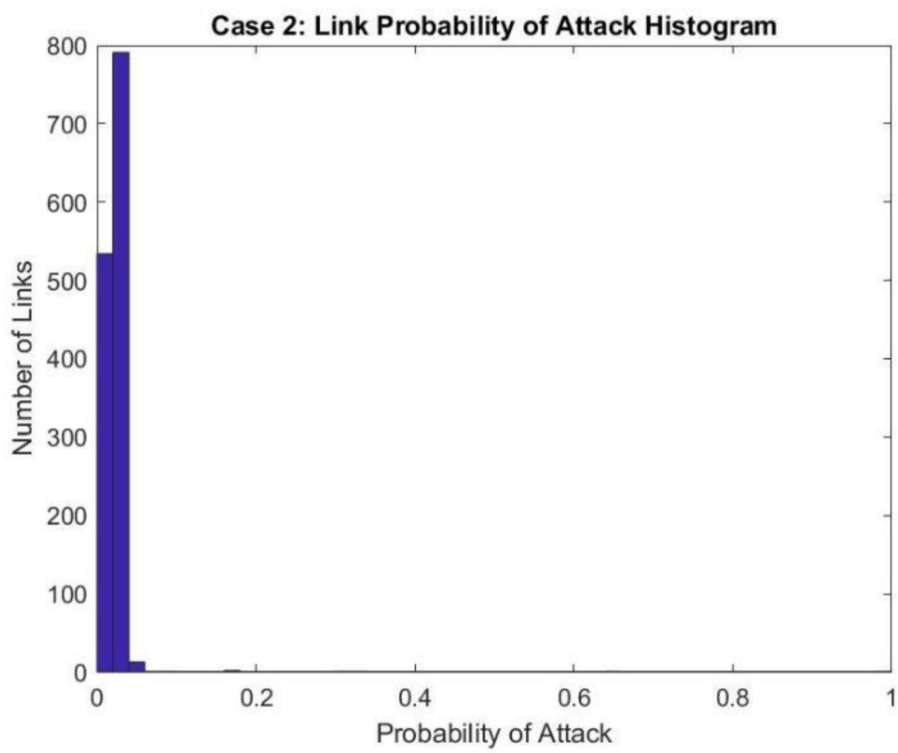


Figure 0-3. Histogram of Link Probability of Attack for Case 2.

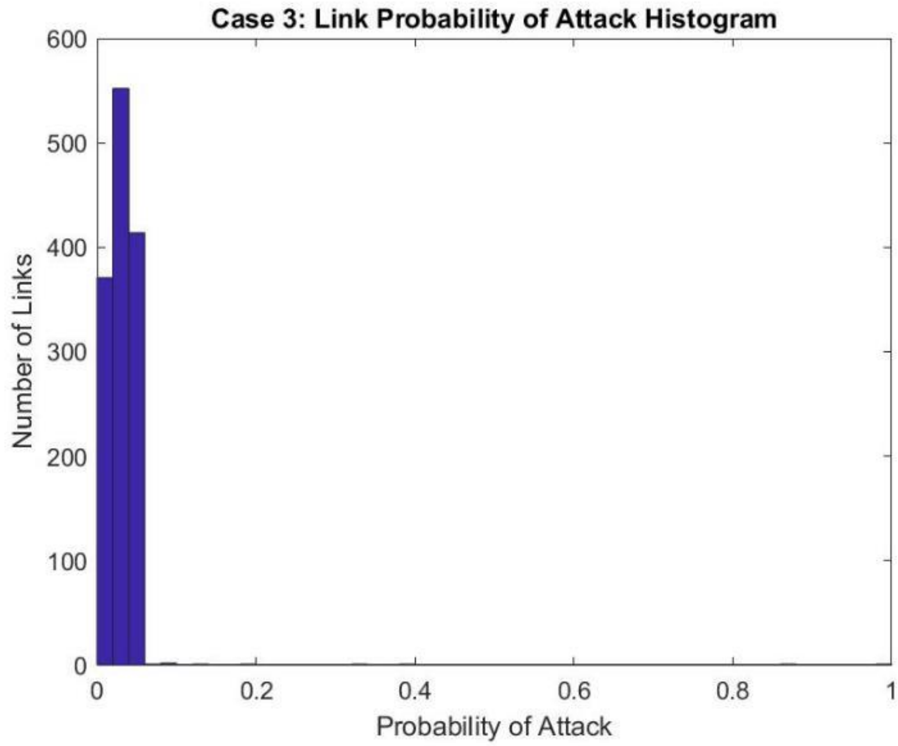


Figure 0-4. Histogram of Link Probability of Attack for Case 3.

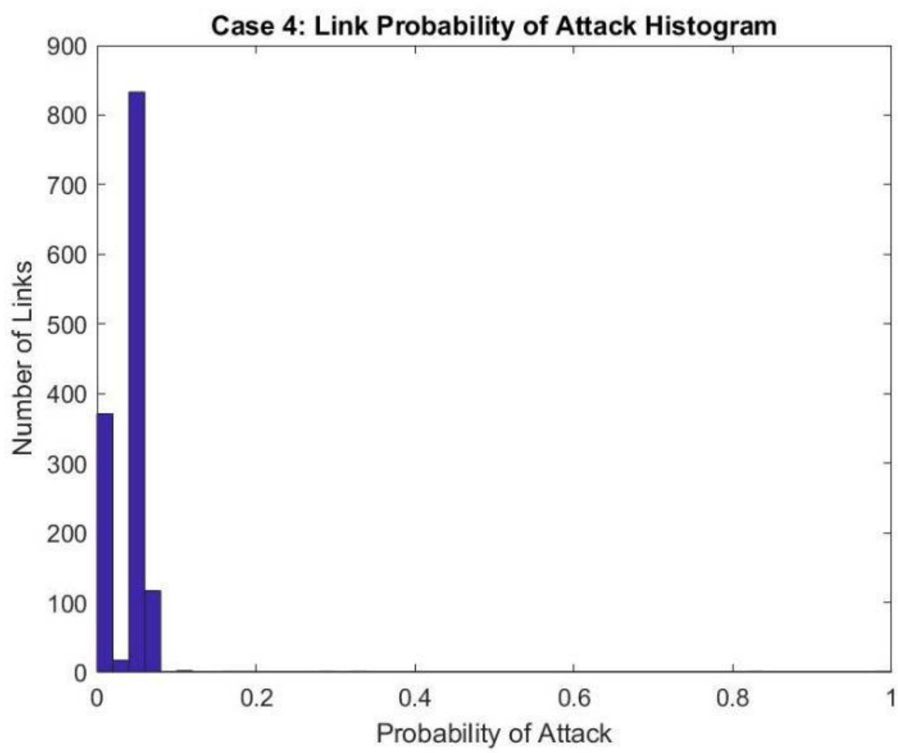


Figure 0-5. Histogram of Link Probability of Attack for Case 4.

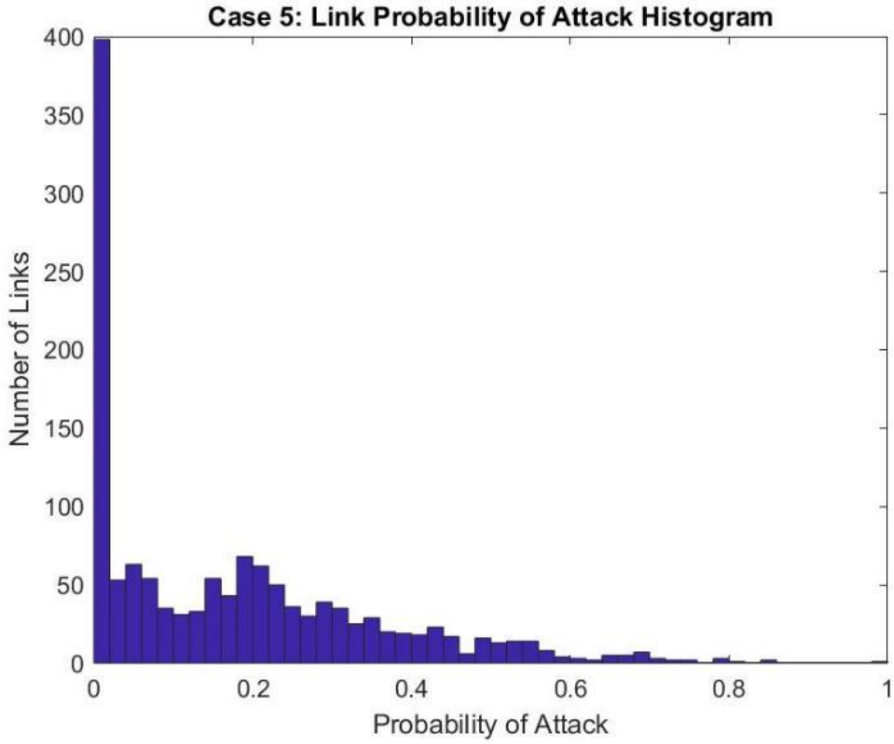


Figure 0-6. Histogram of Link Probability of Attack for Case 5.

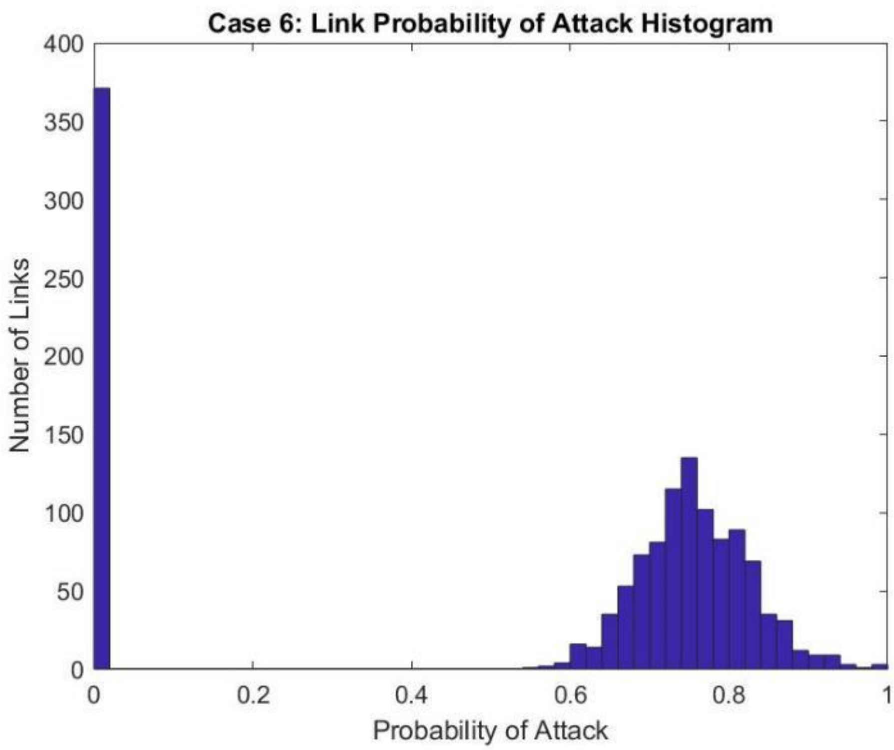


Figure 0-7. Histogram of Link Probability of Attack for Case 6.

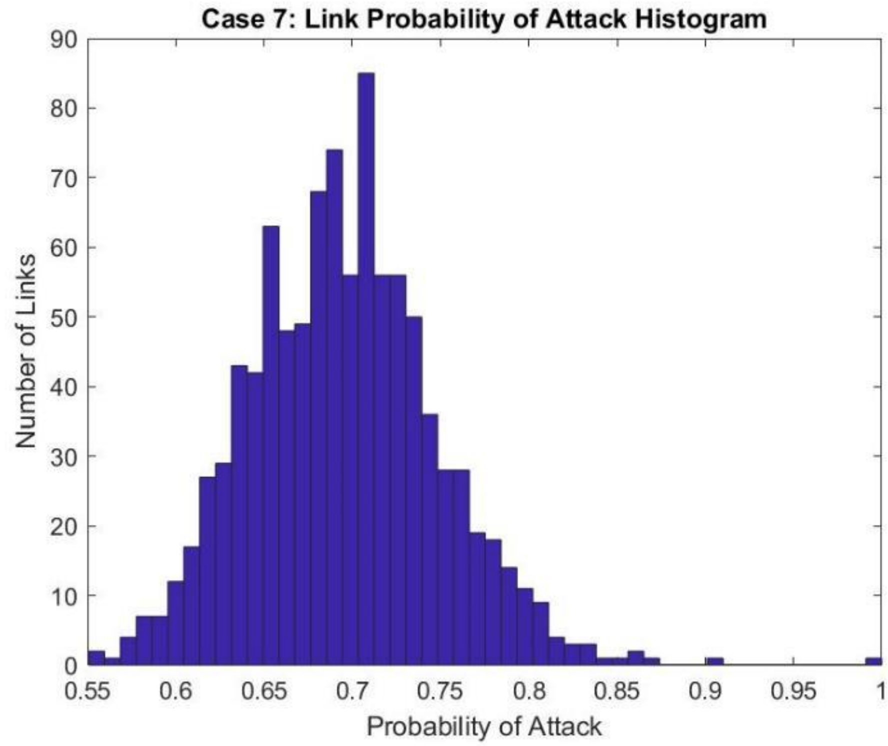


Figure 0-8. Histogram of Link Probability of Attack for Case 7.

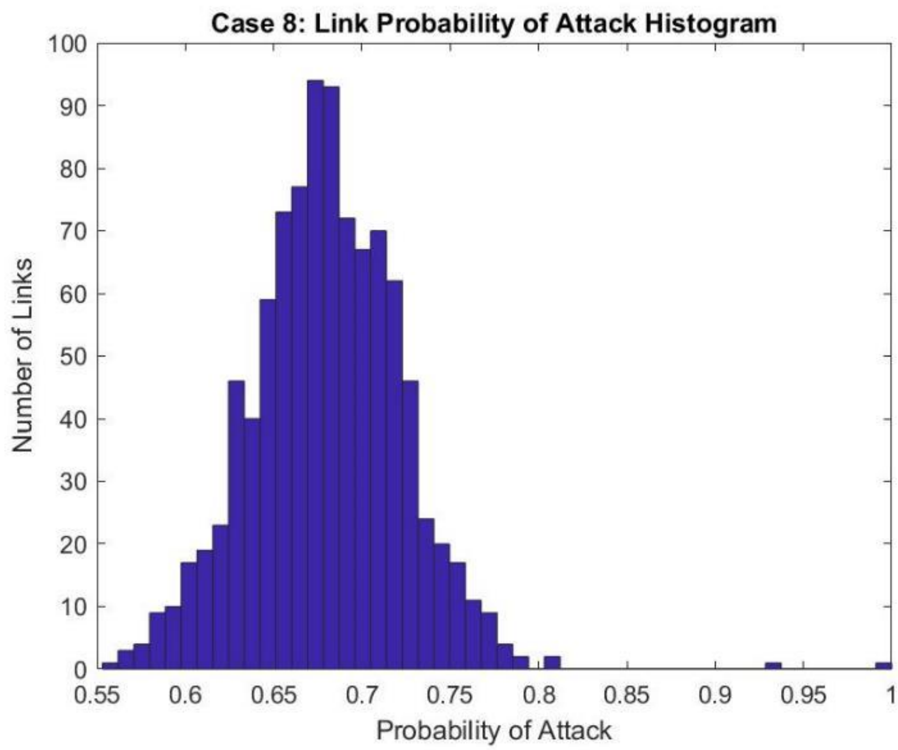


Figure 0-9. Histogram of Link Probability of Attack for Case 8.
4

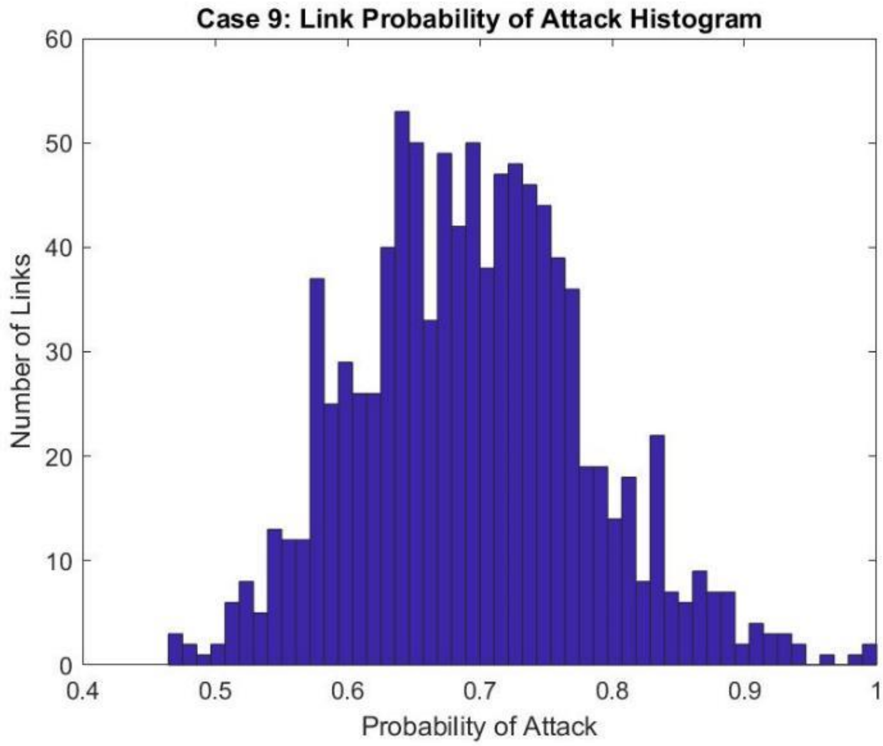


Figure 0-10. Histogram of Link Probability of Attack for Case 9.

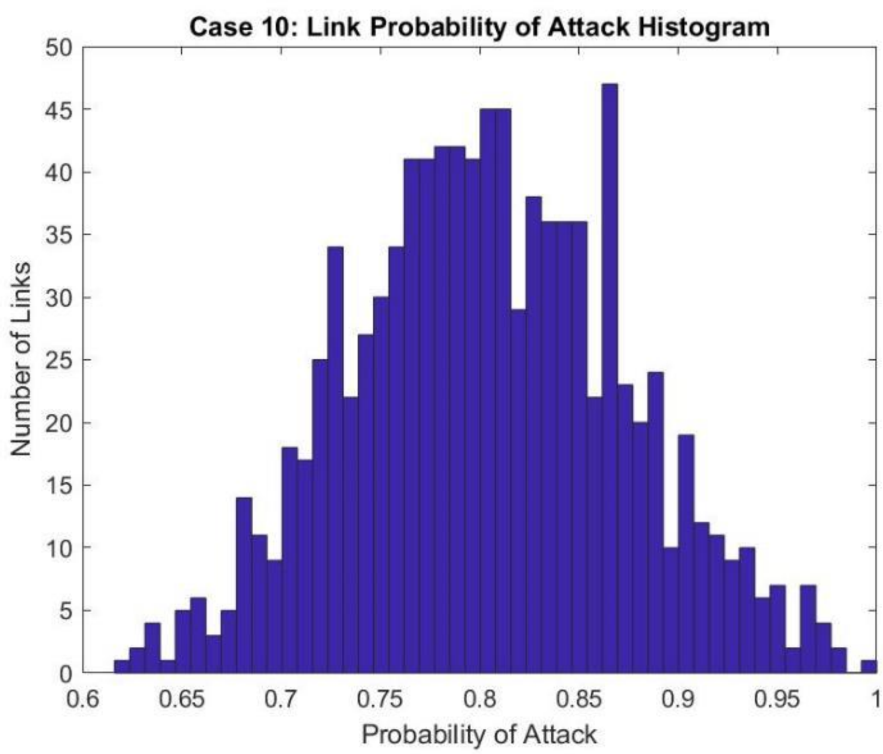


Figure 0-11. Histogram of Link Probability of Attack for Case 10.

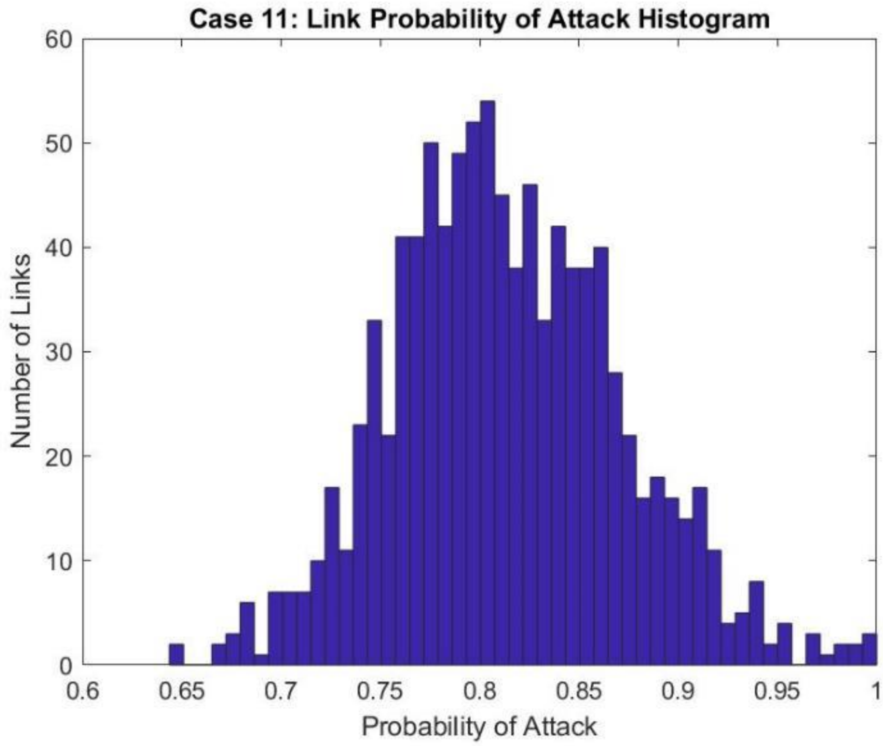


Figure 0-12. Histogram of Link Probability of Attack for Case 11.

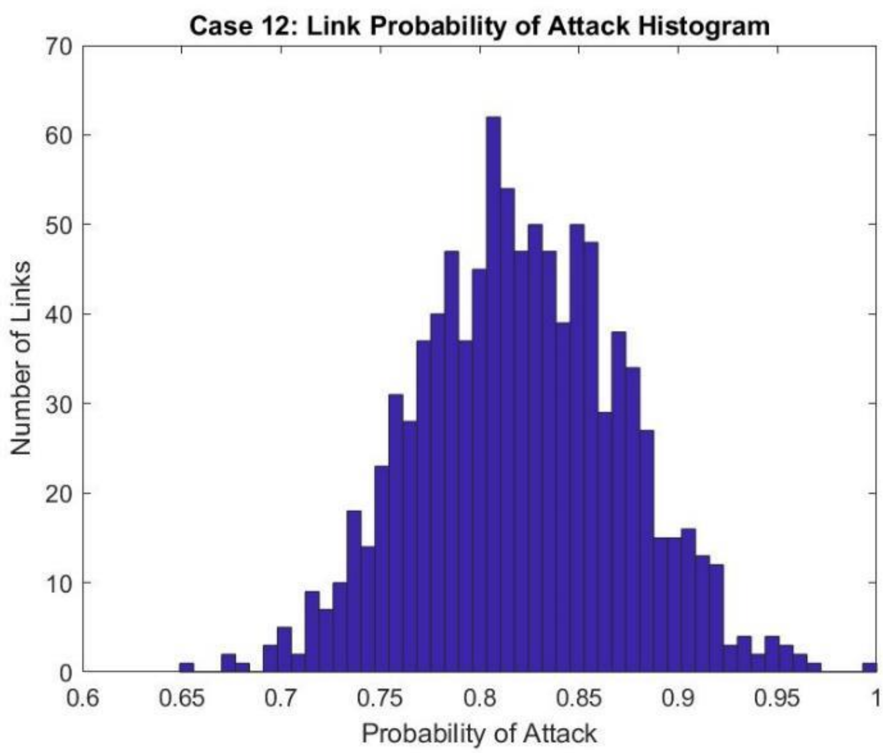


Figure 0-13. Histogram of Link Probability of Attack for Case 12.

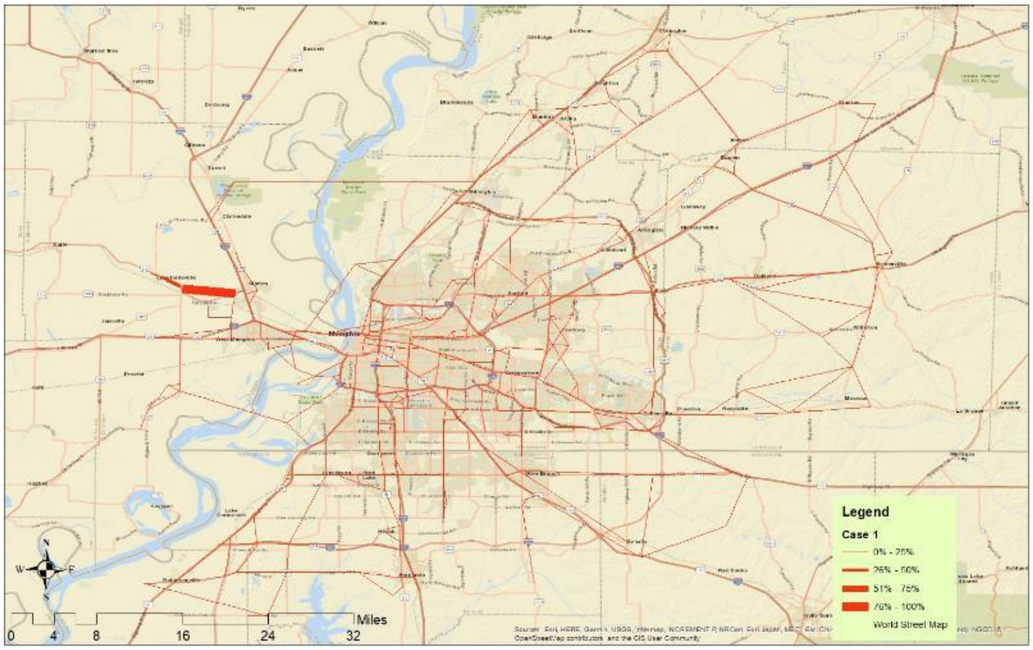


Figure 0-14. Link Probability for Attack for Case 1.

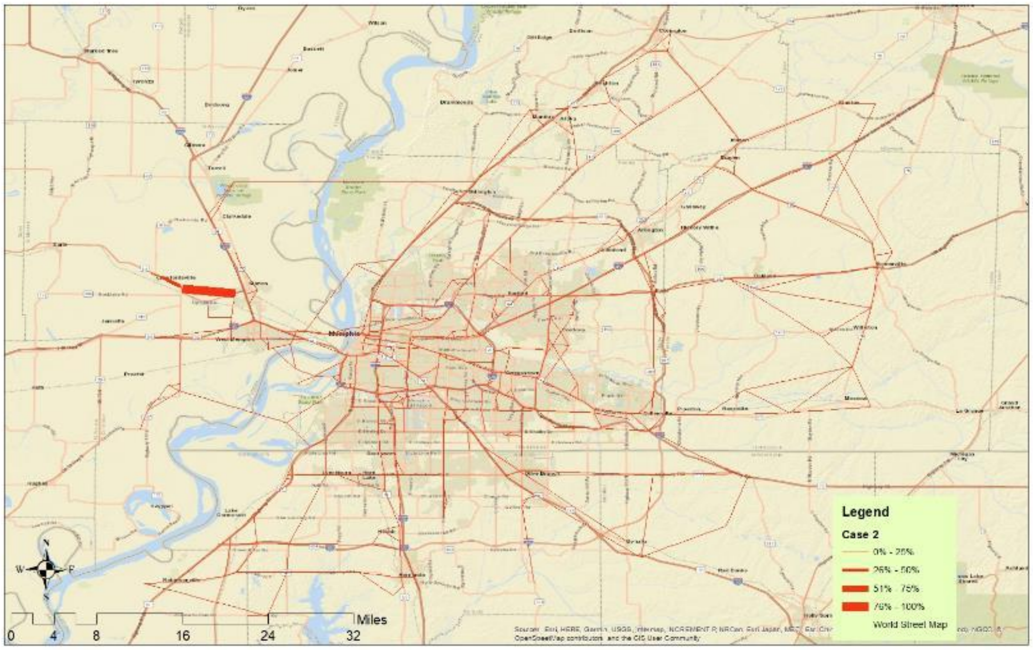


Figure 0-15. Link Probability for Attack for Case 2.

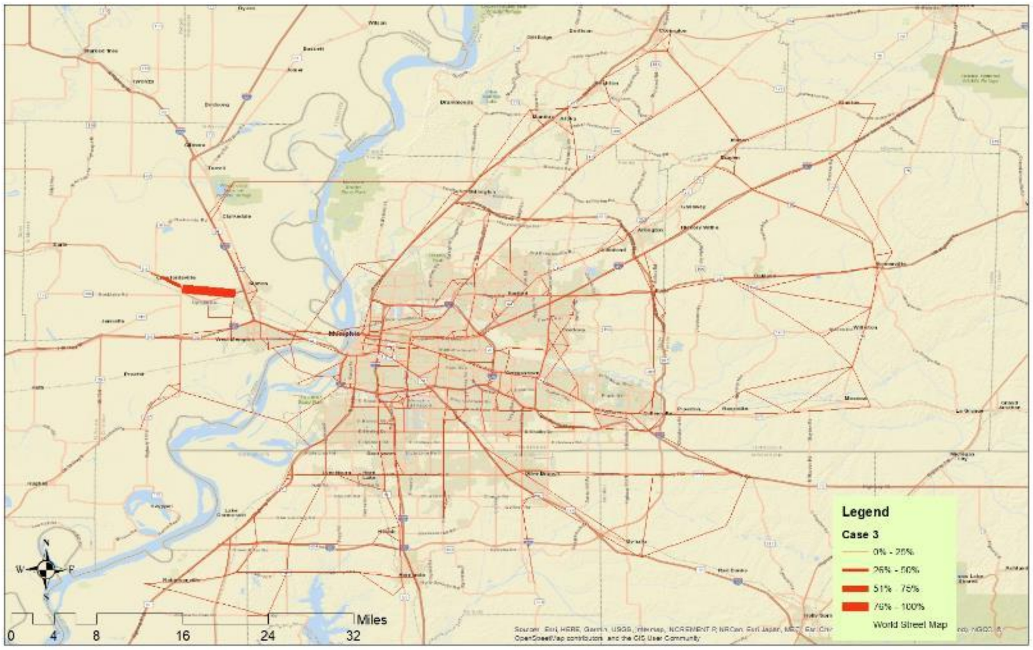


Figure 0-16. Link Probability for Attack for Case 3.

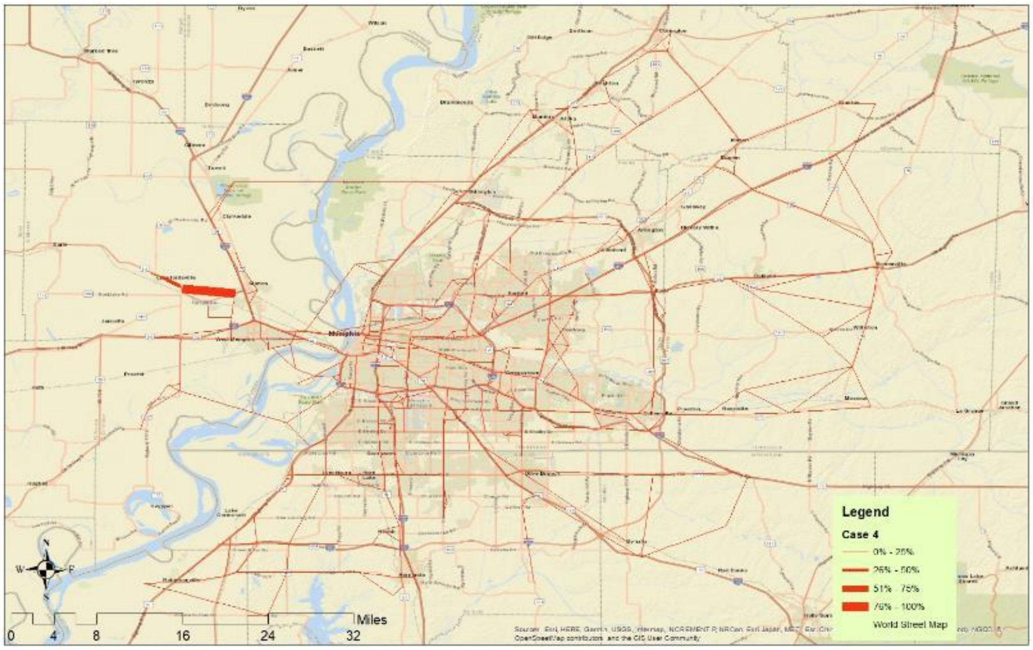


Figure 0-17. Link Probability for Attack for Case 4.

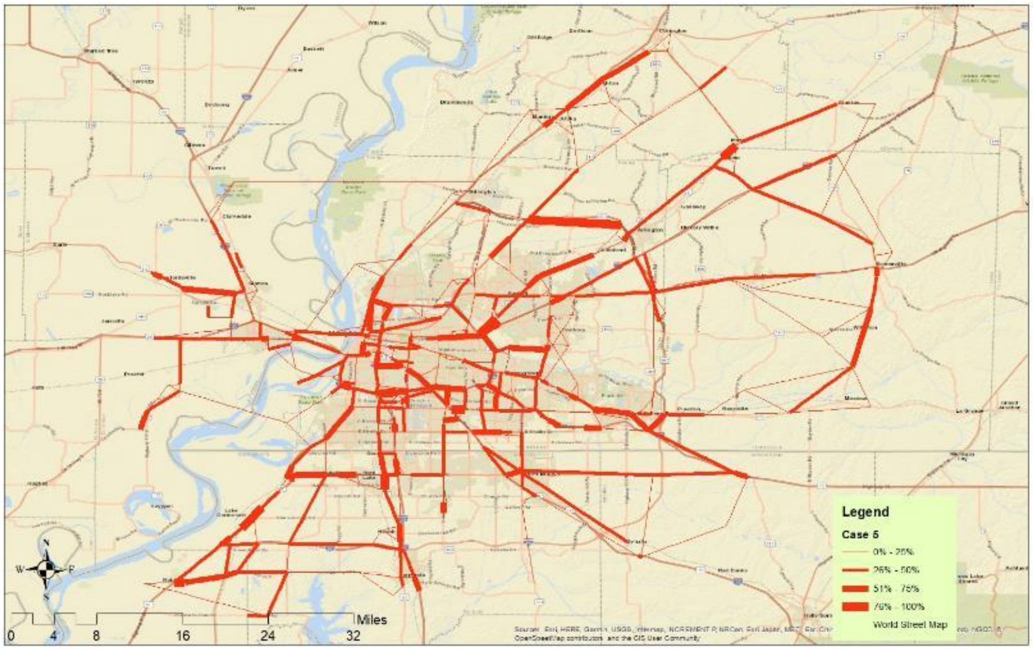


Figure 0-18. Link Probability for Attack for Case 5.

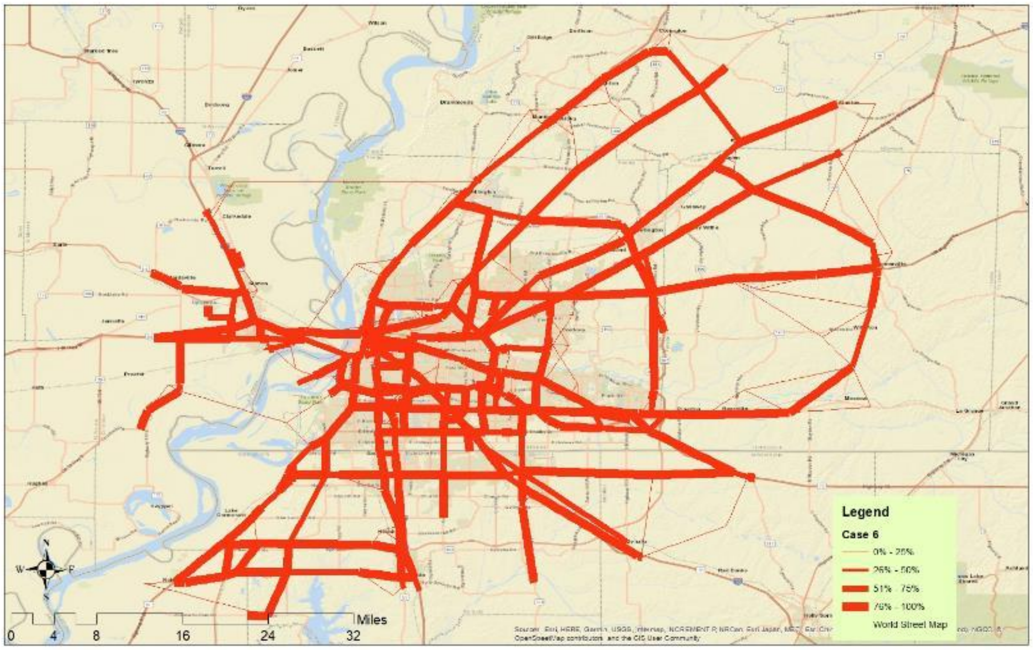


Figure 0-19. Link Probability for Attack for Case 6.

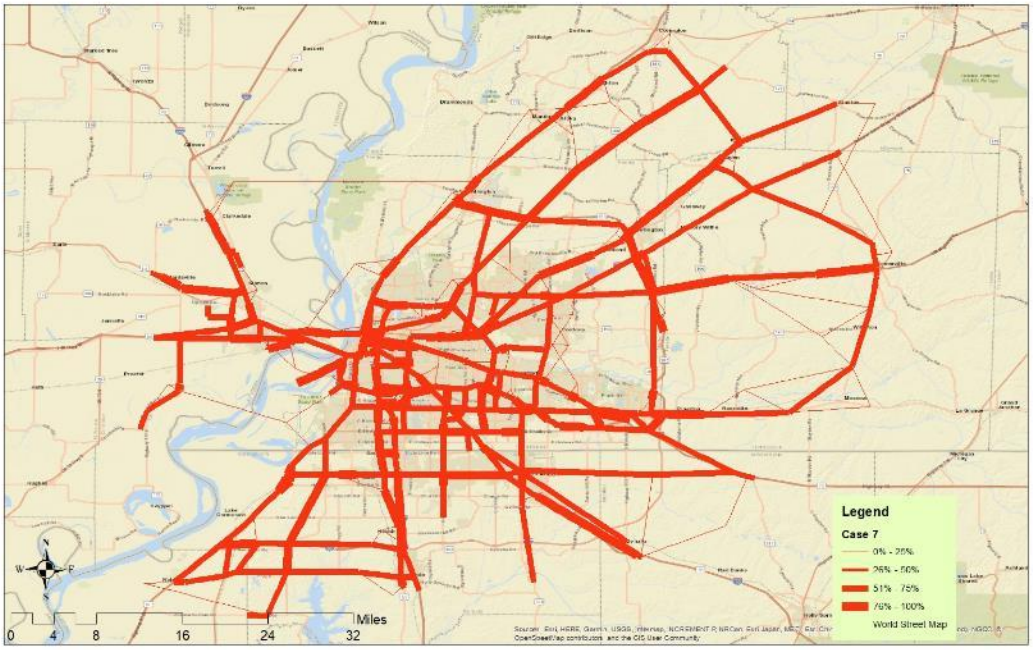


Figure 0-20. Link Probability for Attack for Case 7.

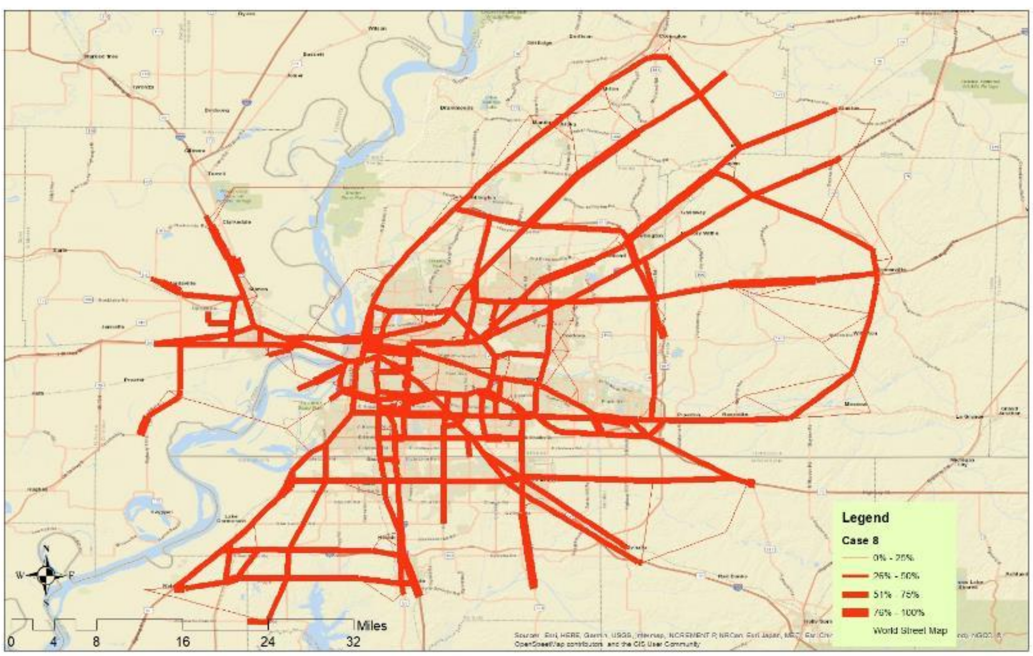


Figure 0-21. Link Probability for Attack for Case 8.

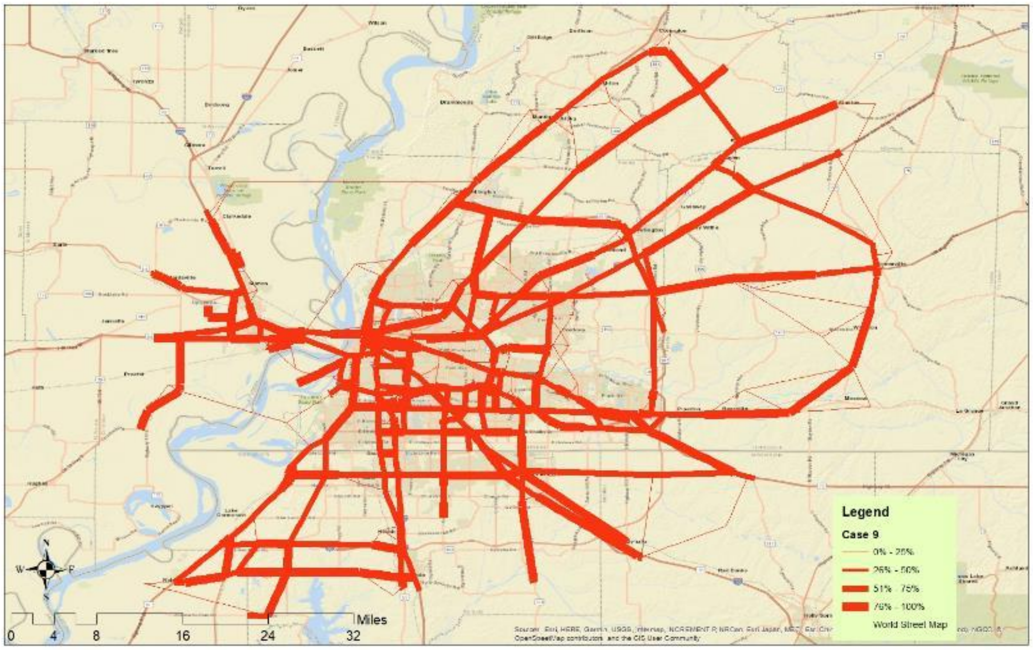


Figure 0-22. Link Probability for Attack for Case 9.

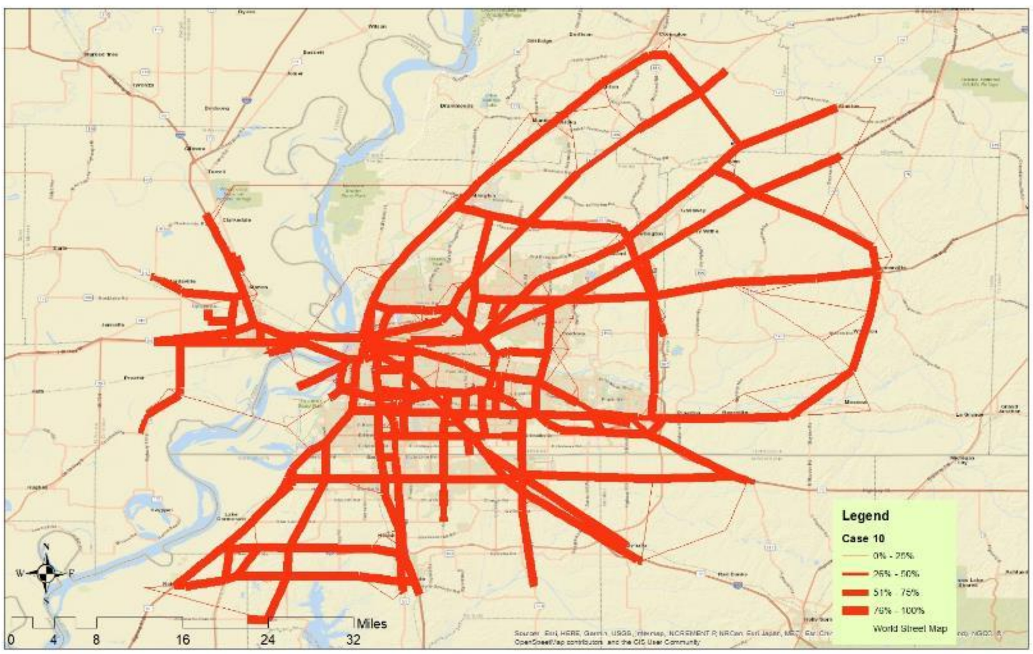


Figure 0-23. Link Probability for Attack for Case 10.

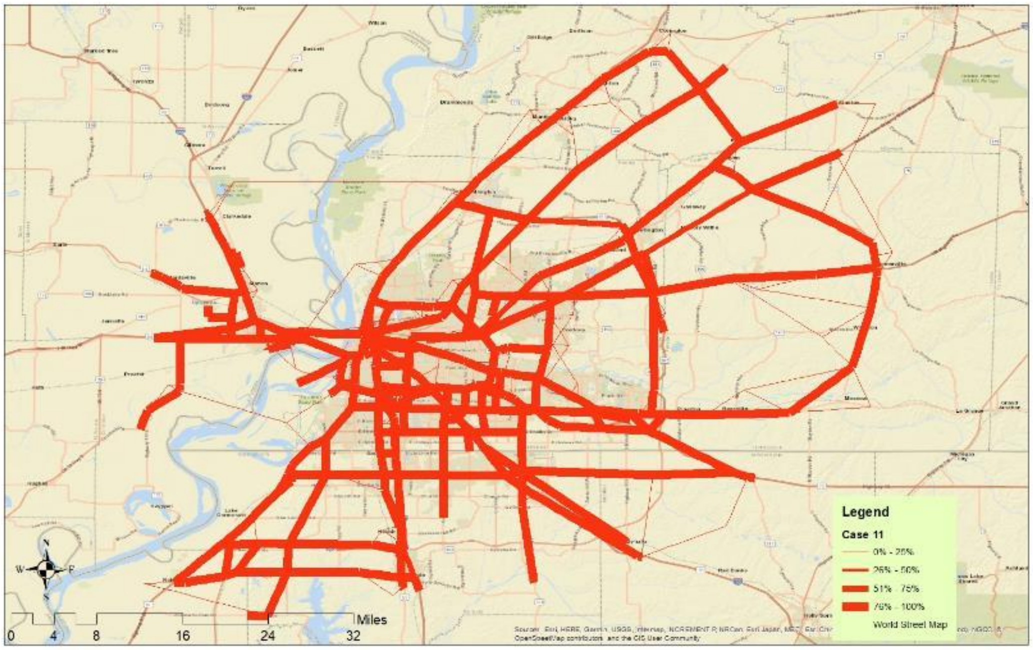


Figure 0-24. Link Probability for Attack for Case 11.

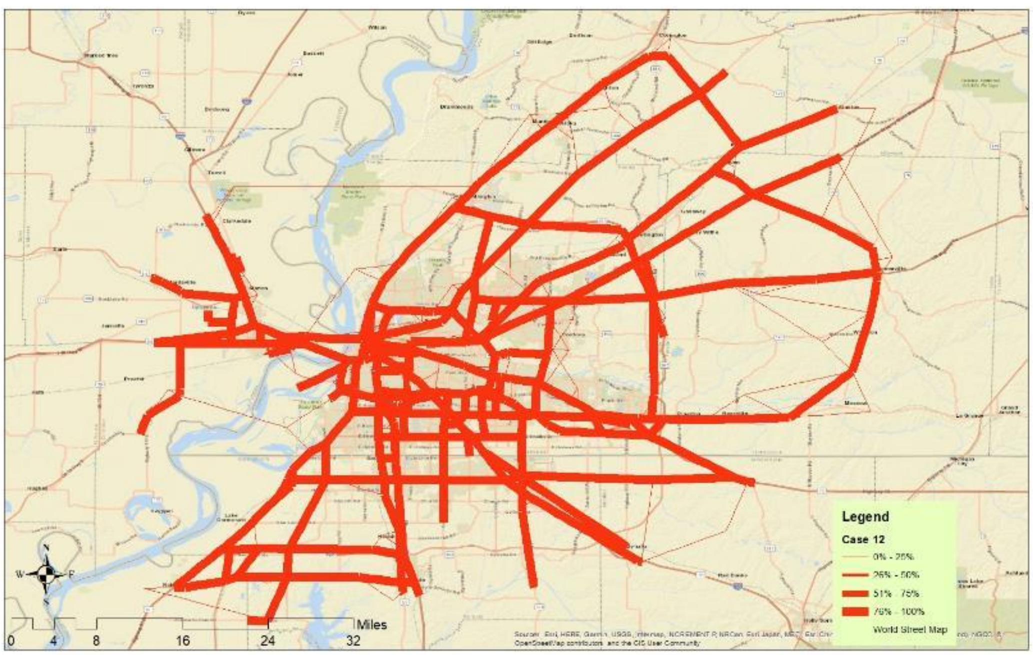


Figure 0-25. Link Probability for Attack for Case 12.

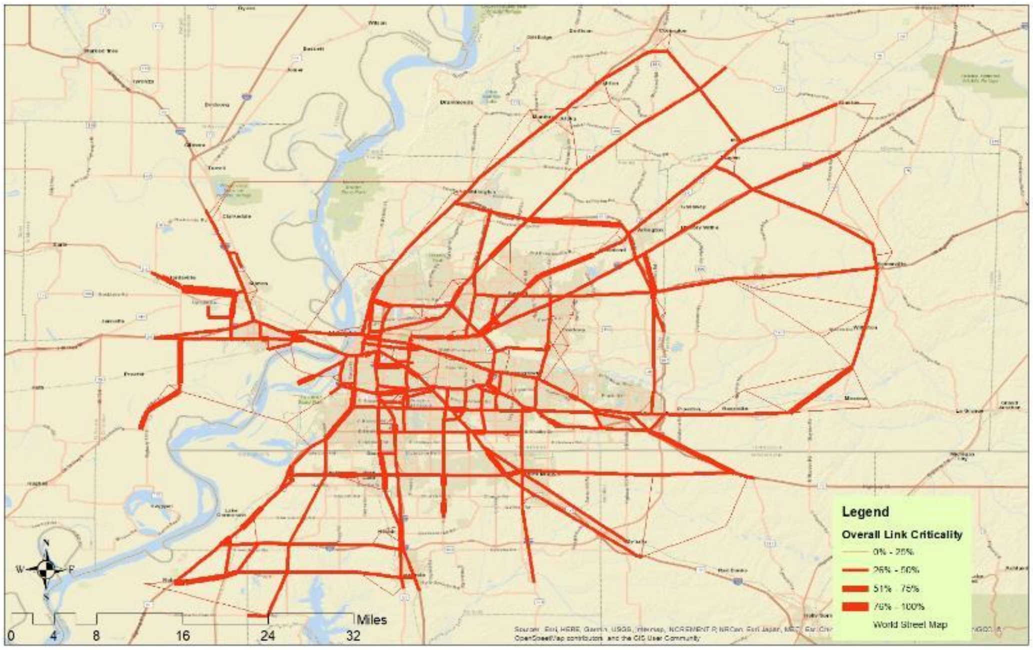


Figure 0-26. Overall Link Probability for Attack

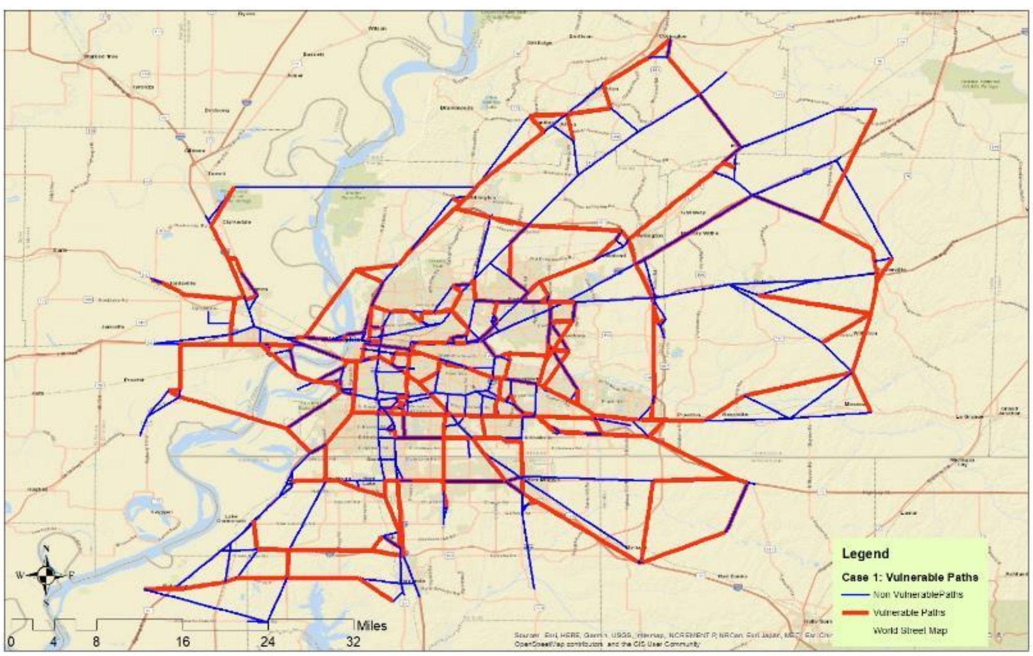


Figure 0-27. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 1.

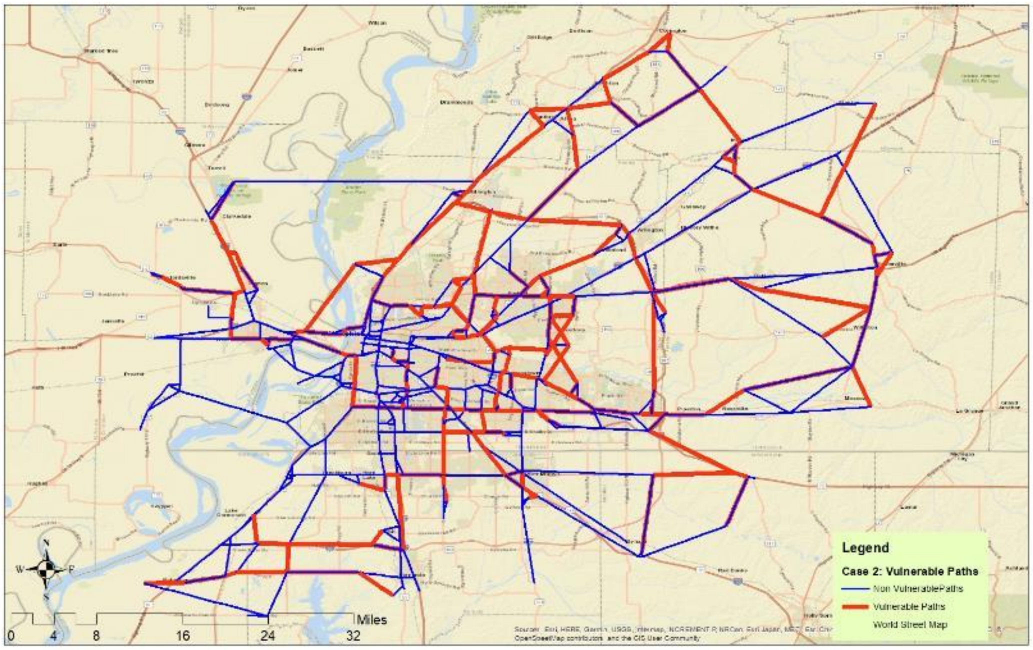


Figure 0-28. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 2.

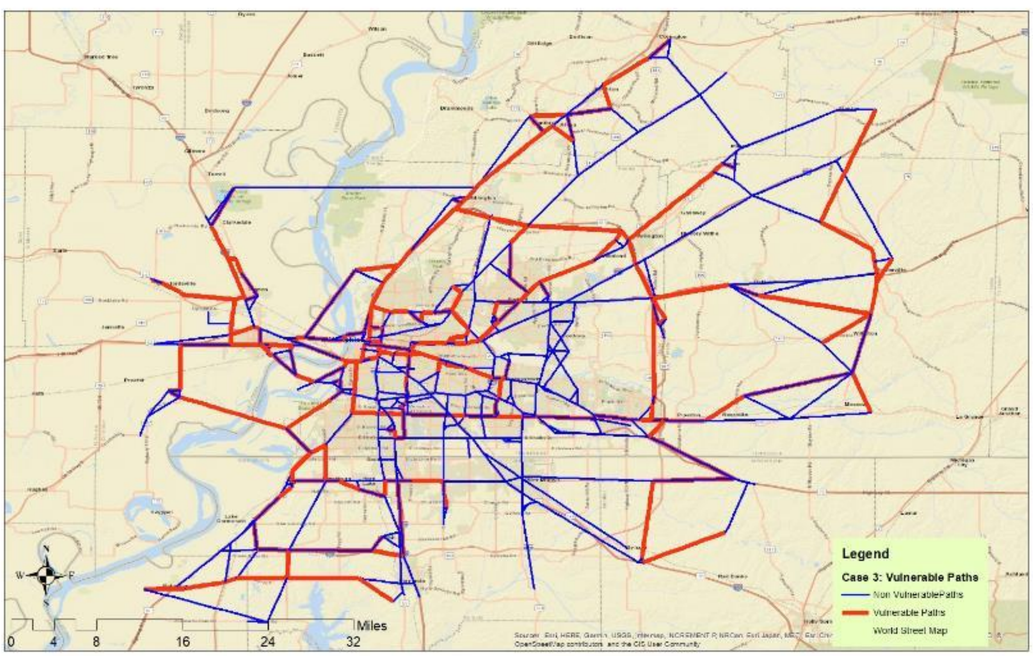


Figure 0-29. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 3.

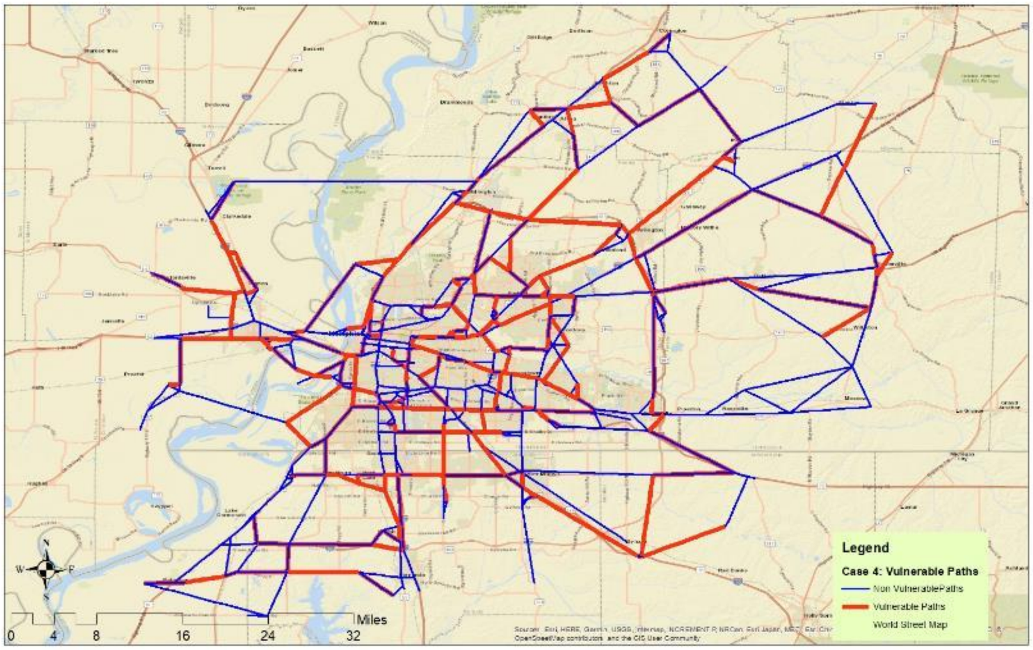


Figure 0-30. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 4.

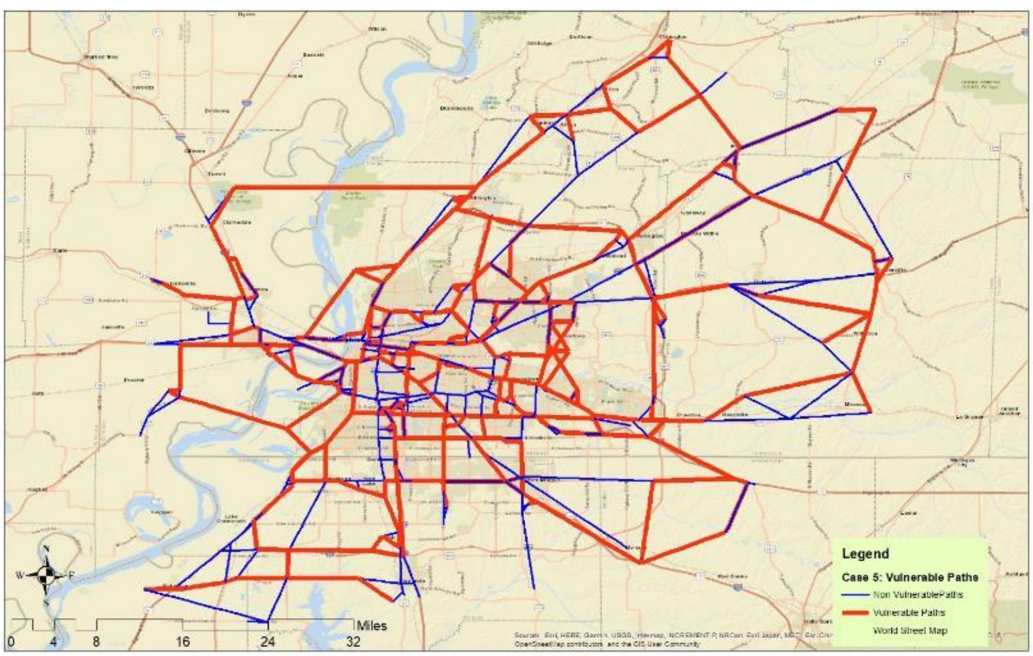


Figure 0-31. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 5.

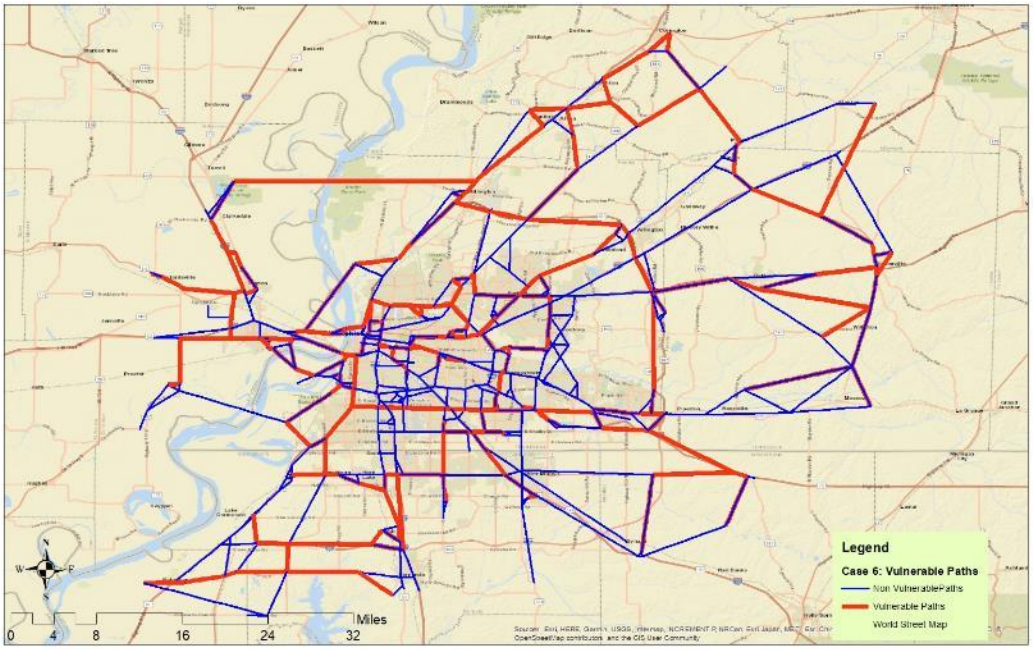


Figure 0-32. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 6.

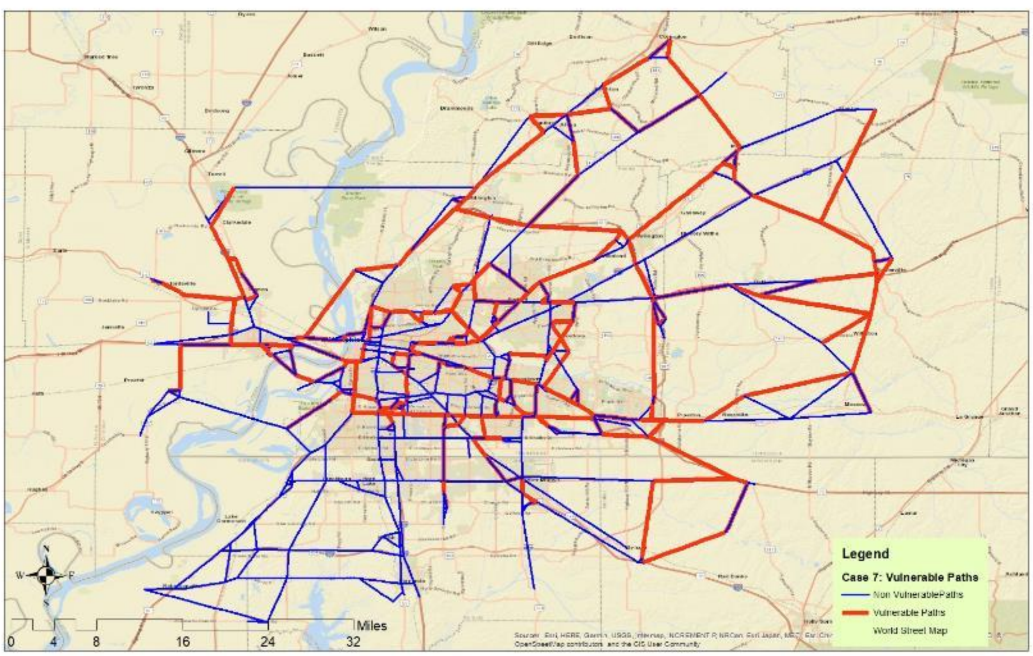


Figure 0-33. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 7.

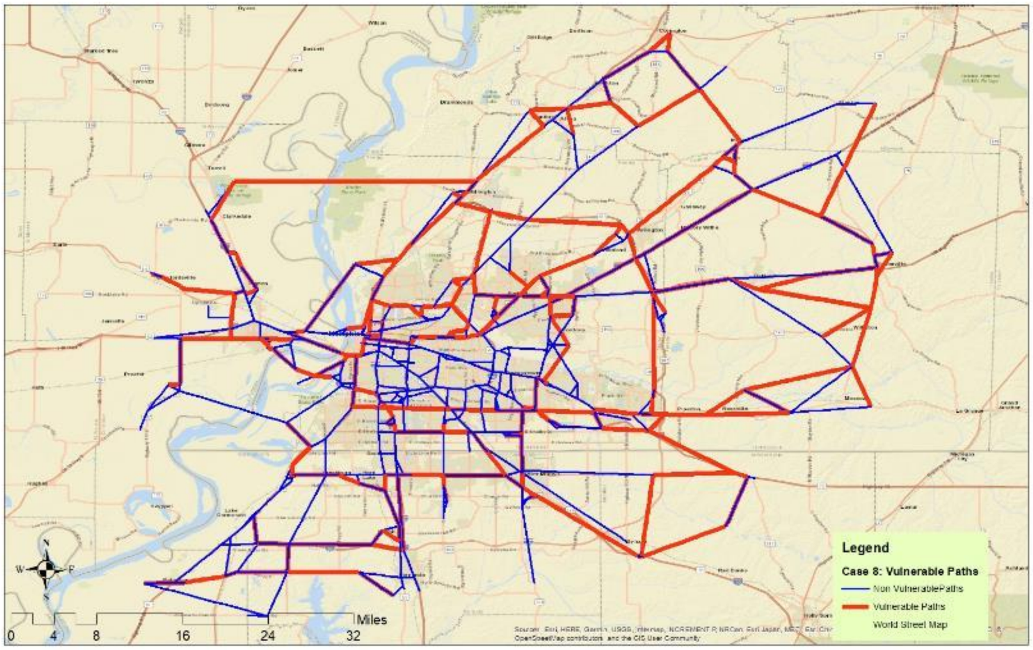


Figure 0-34. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 8.

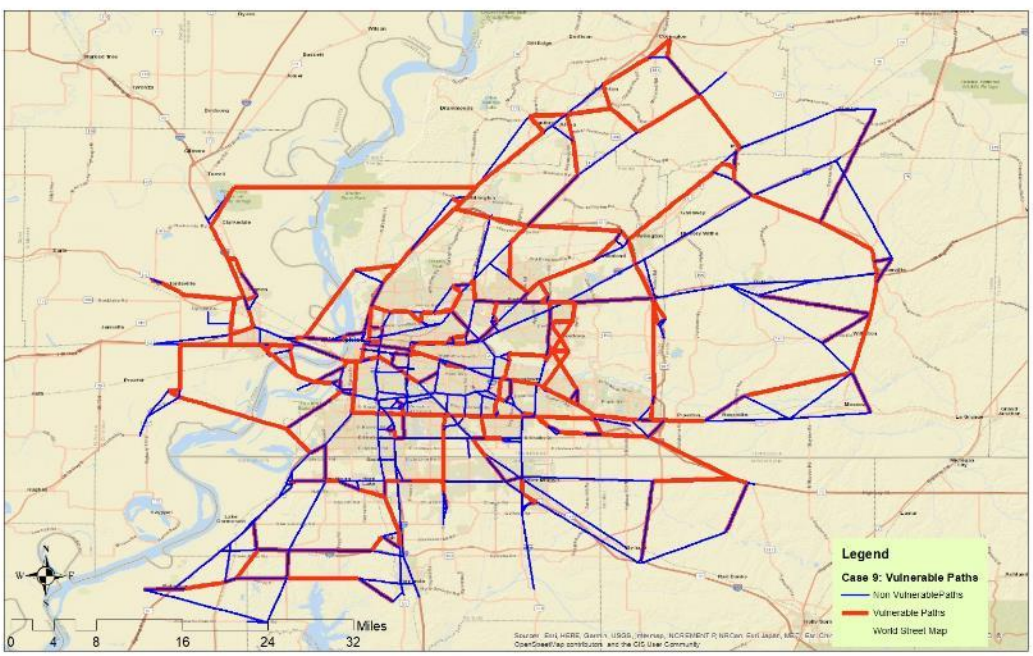


Figure 0-35. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 9.

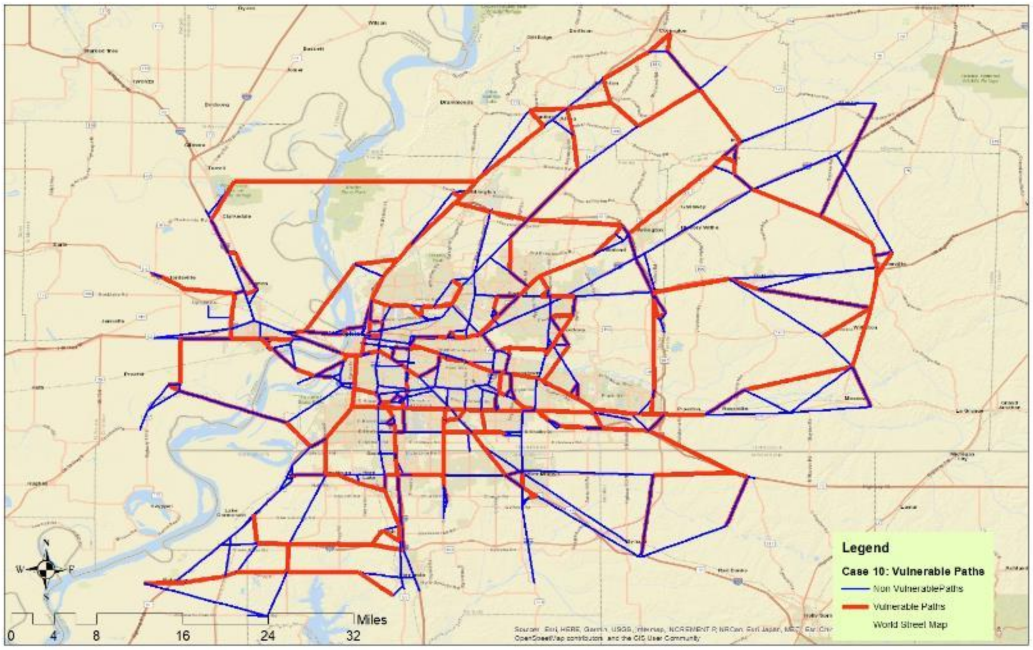


Figure 0-36. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 10.

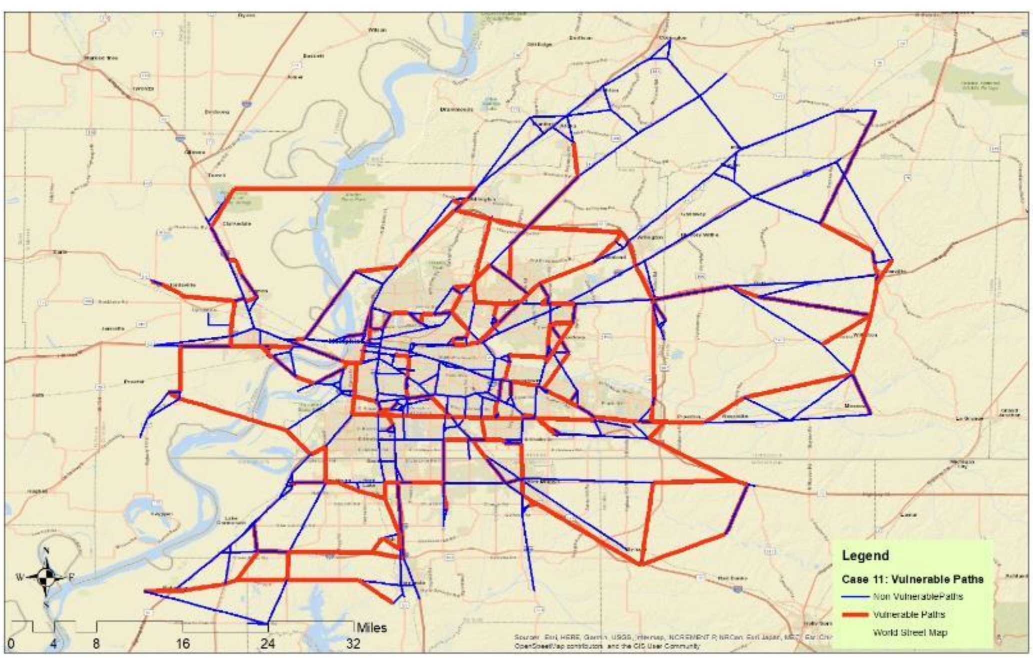


Figure 0-37. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 11.

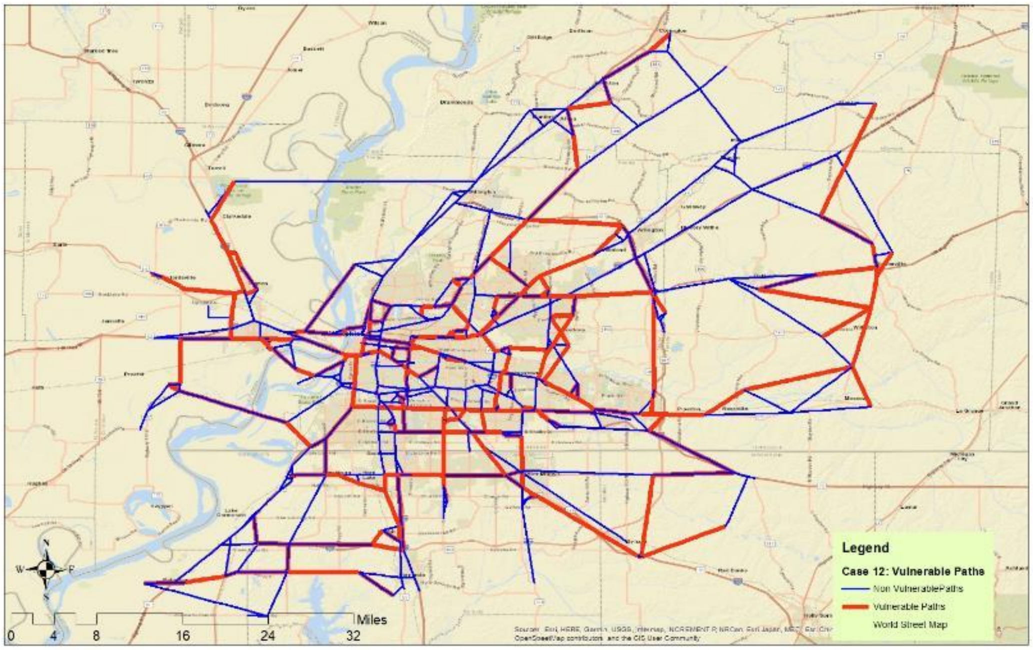


Figure 0-38. Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 12

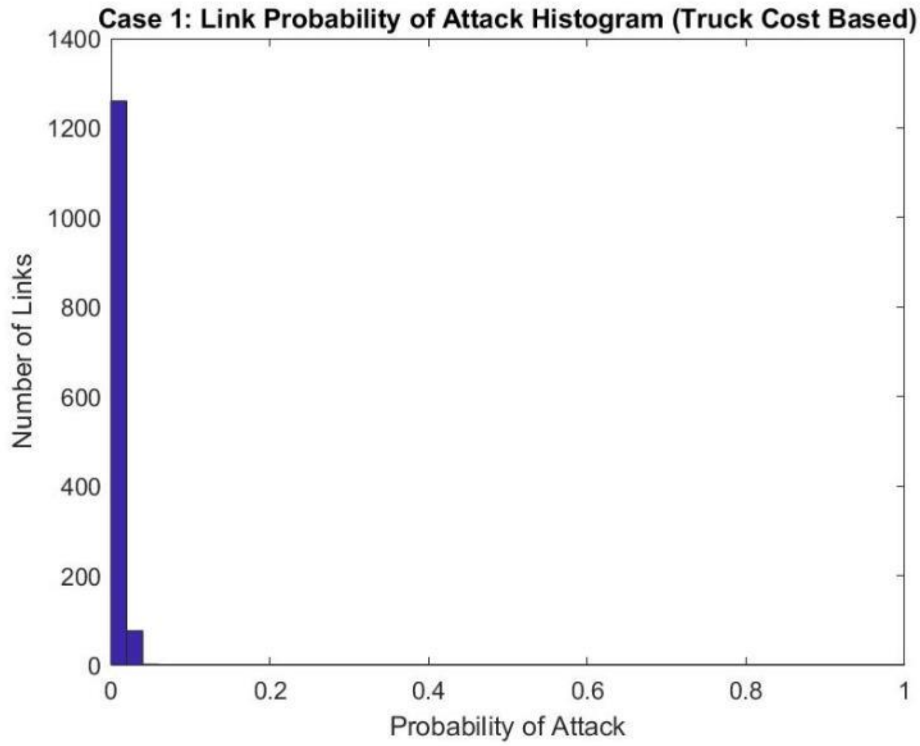


Figure 0-39. Histogram of Link Probability of Attack for Case 1 (Truck Cost Based).

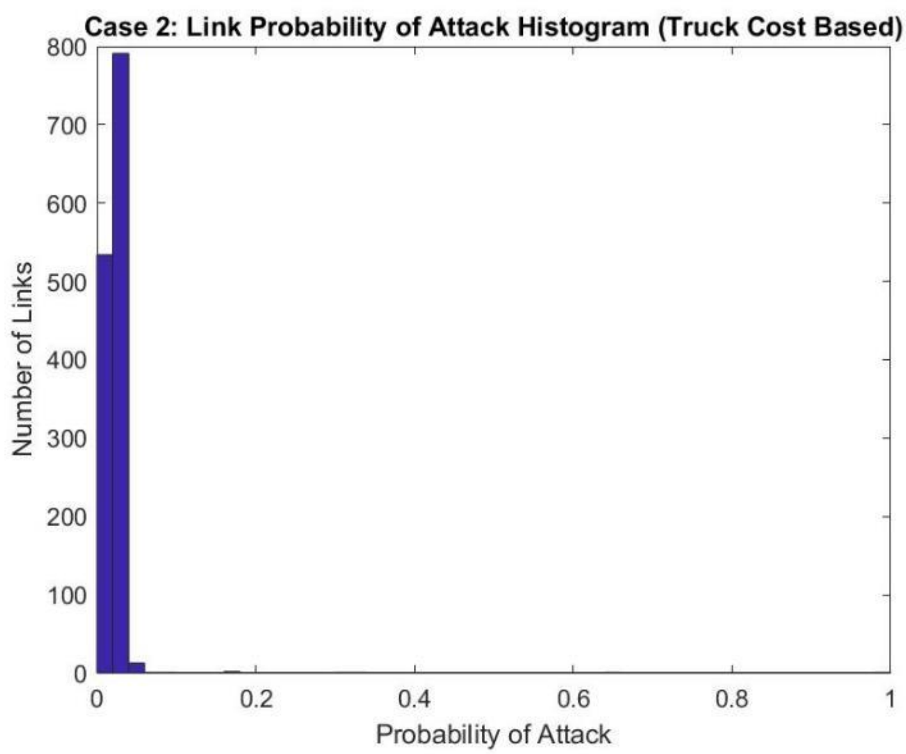


Figure 0-40. Histogram of Link Probability of Attack for Case 2 (Truck Cost Based).

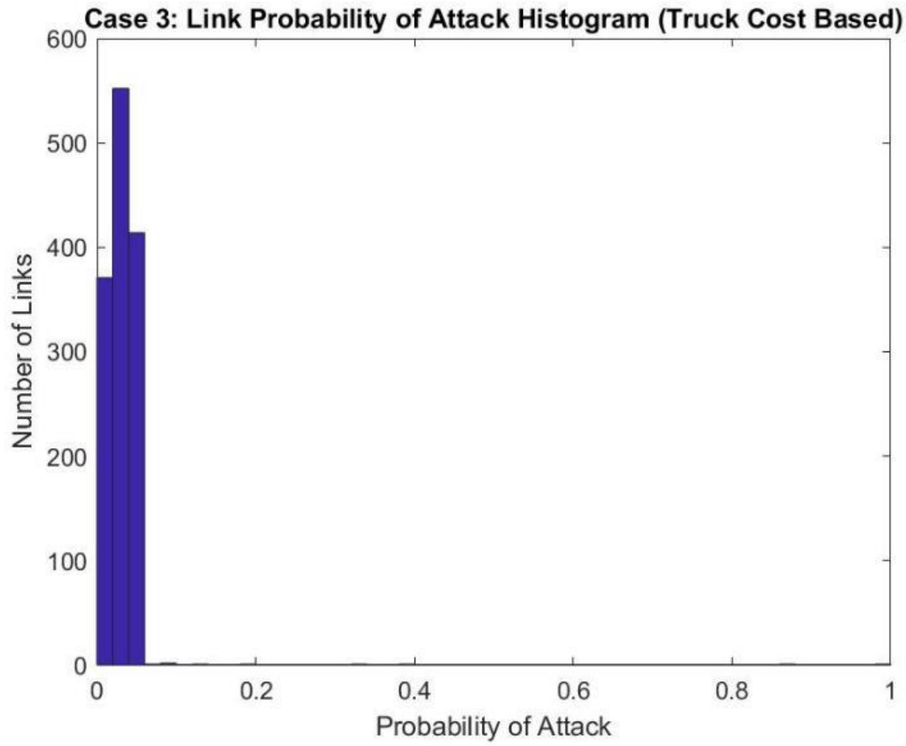


Figure 0-41. Histogram of Link Probability of Attack for Case 3 (Truck Cost Based).

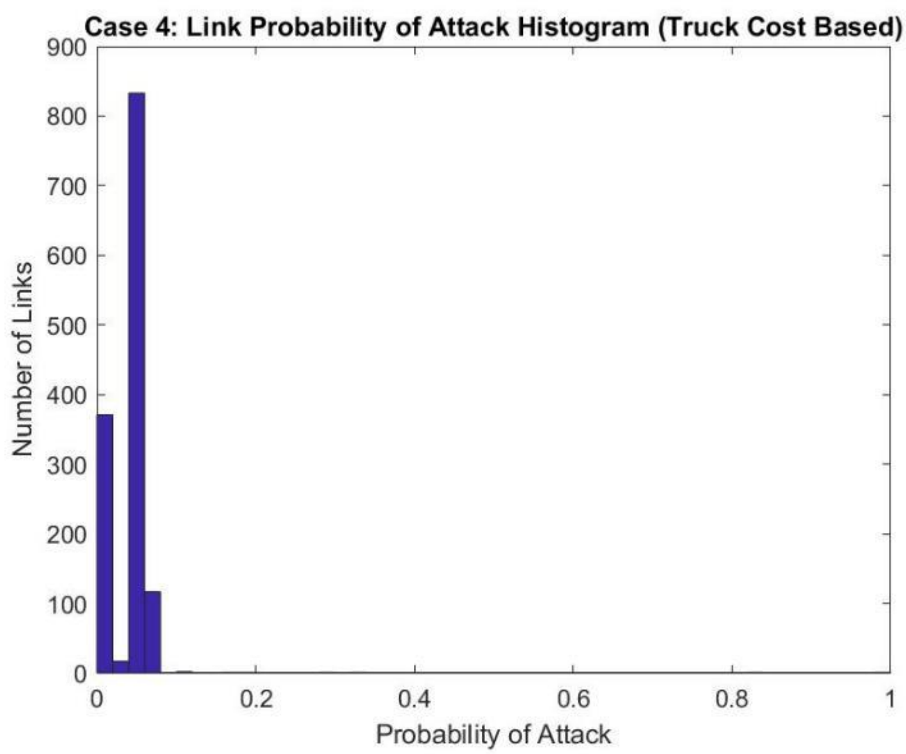


Figure 0-42. Histogram of Link Probability of Attack for Case 4 (Truck Cost Based).

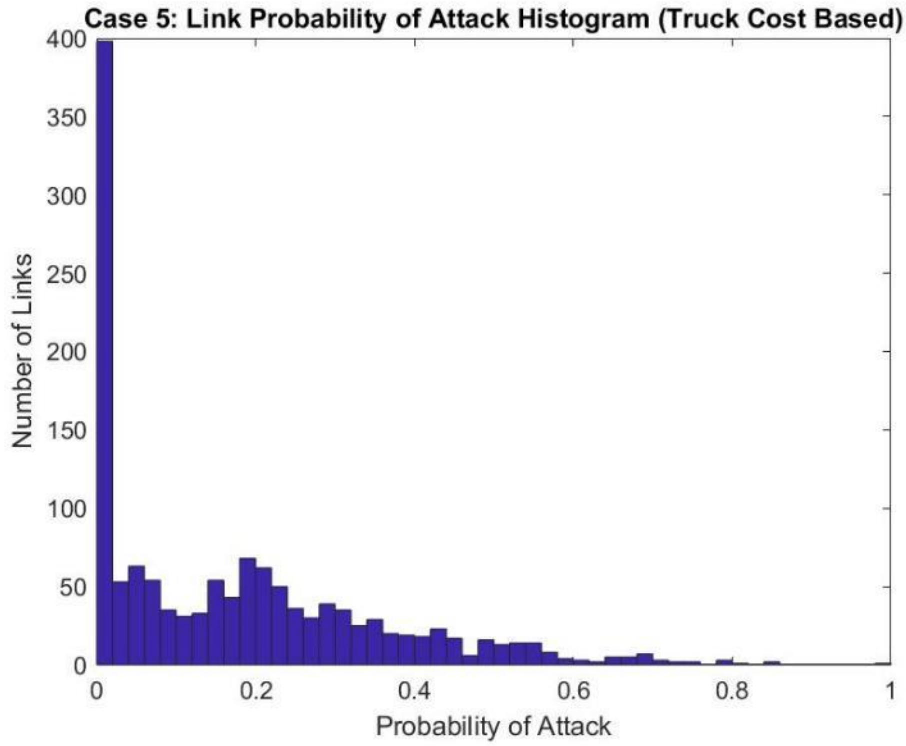


Figure 0-43. Histogram of Link Probability of Attack for Case 5 (Truck Cost Based).

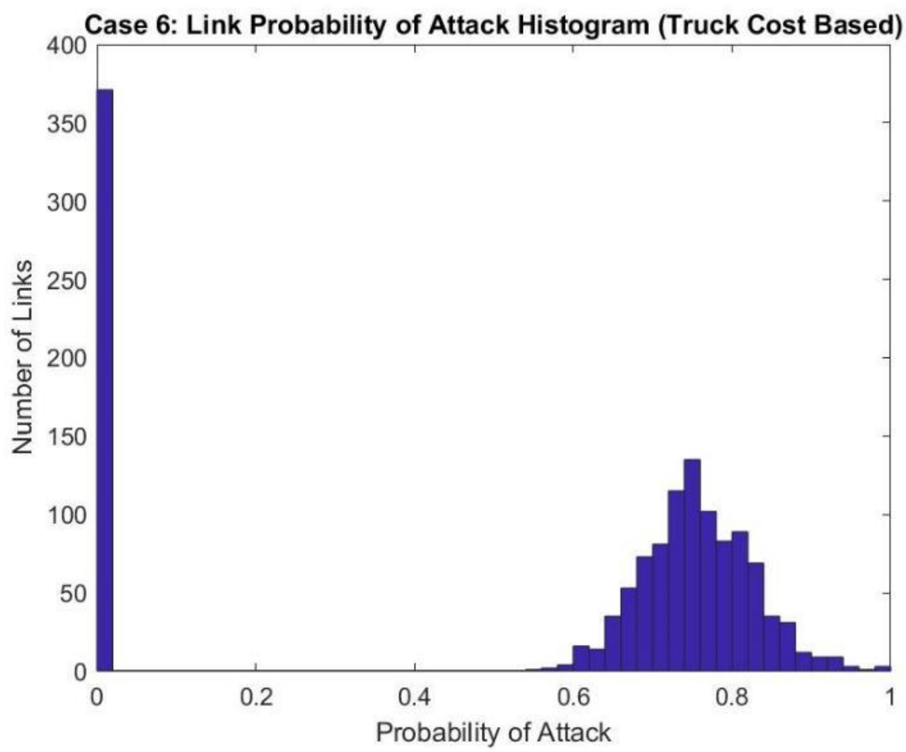


Figure 0-44. Histogram of Link Probability of Attack for Case 6 (Truck Cost Based).

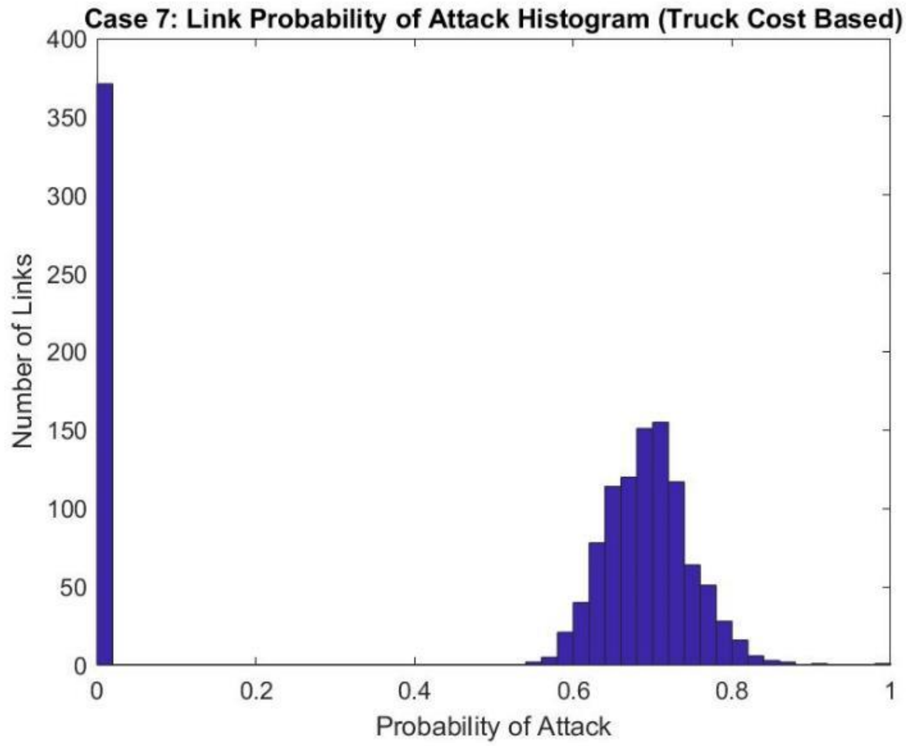


Figure 0-45. Histogram of Link Probability of Attack for Case 7 (Truck Cost Based).

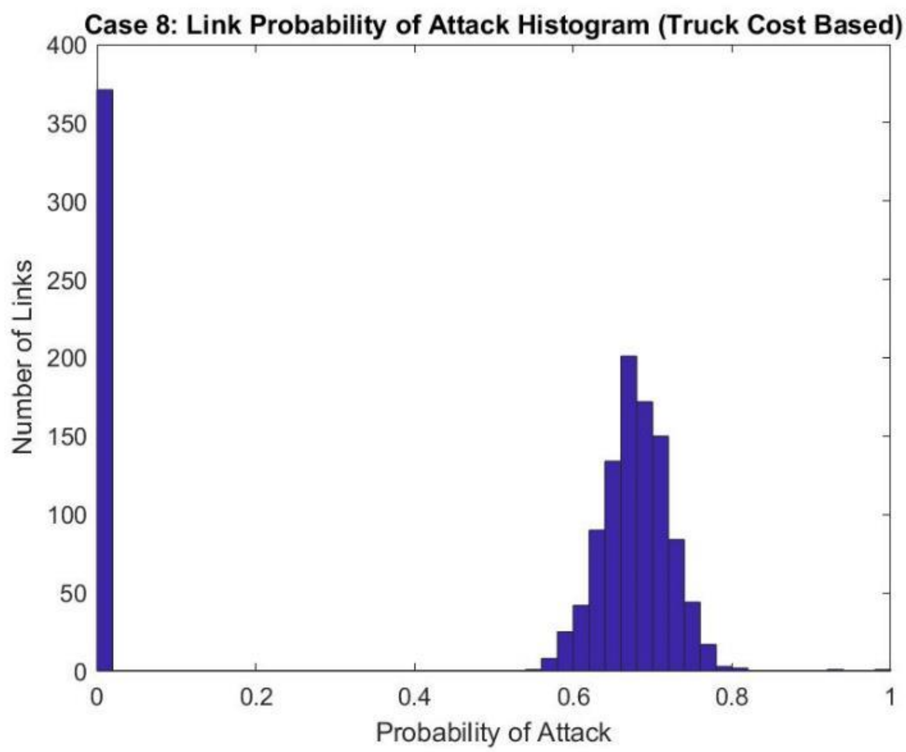


Figure 0-46. Histogram of Link Probability of Attack for Case 8 (Truck Cost Based).

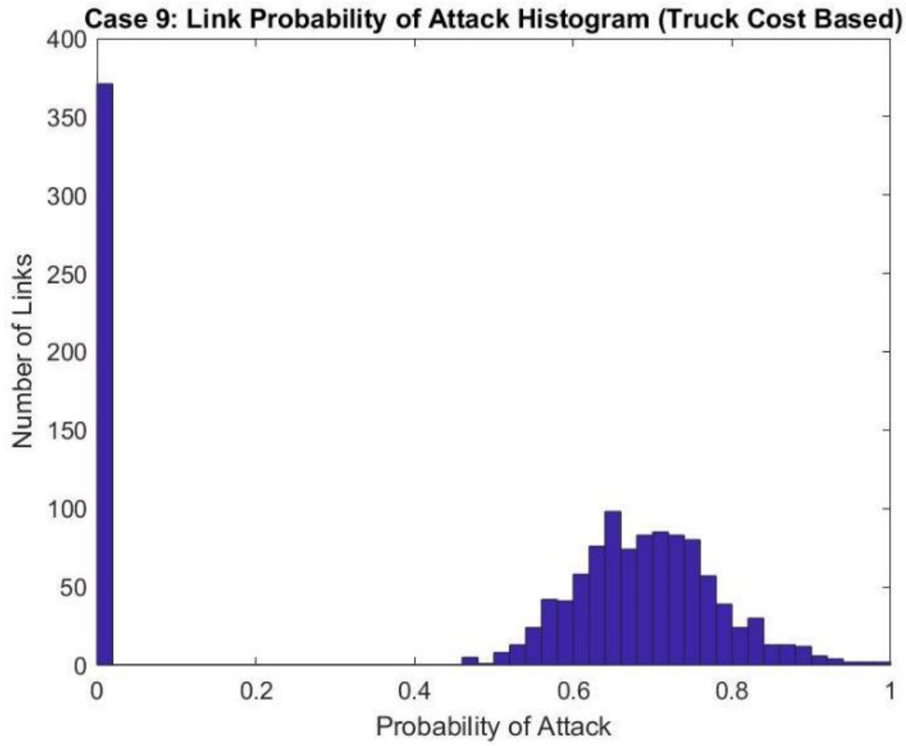


Figure 0-47. Histogram of Link Probability of Attack for Case 9 (Truck Cost Based).

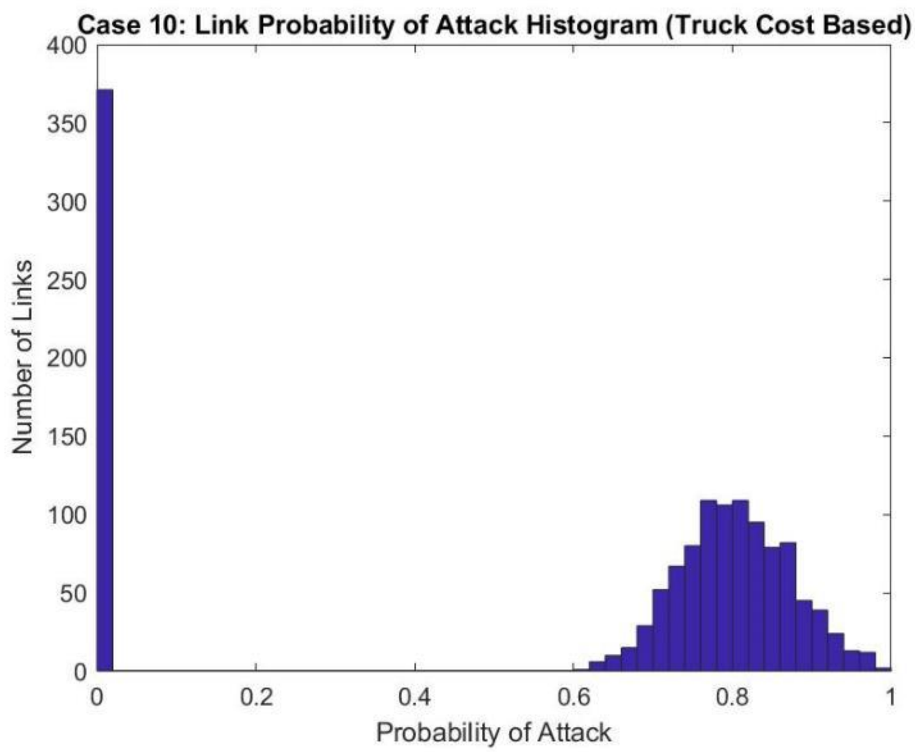


Figure 0-48. Histogram of Link Probability of Attack for Case 10 (Truck Cost Based).

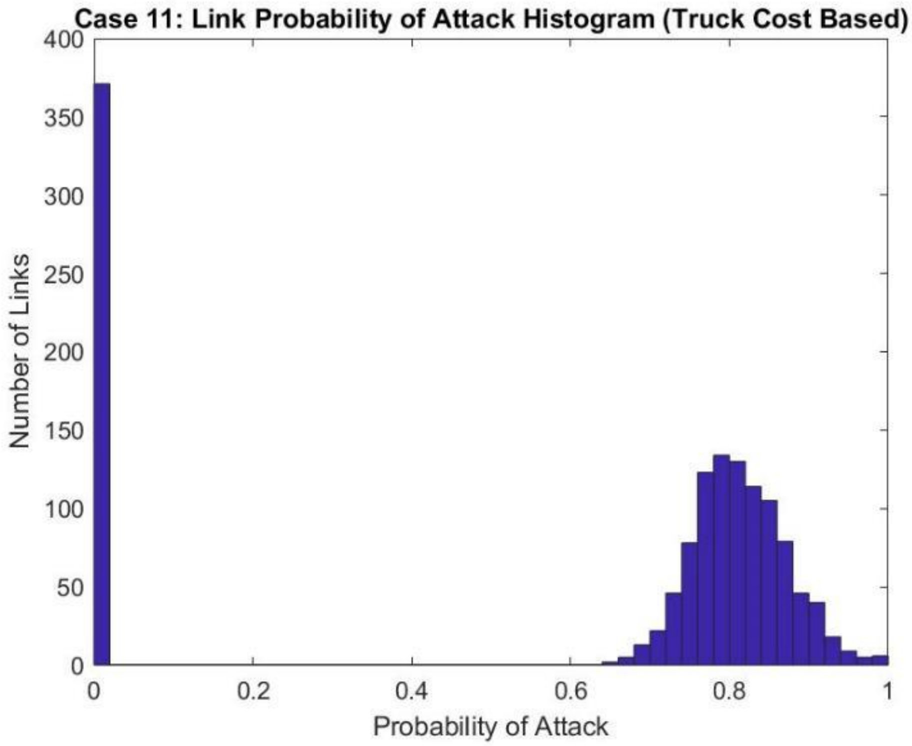


Figure 0-49. Histogram of Link Probability of Attack for Case 11 (Truck Cost Based).

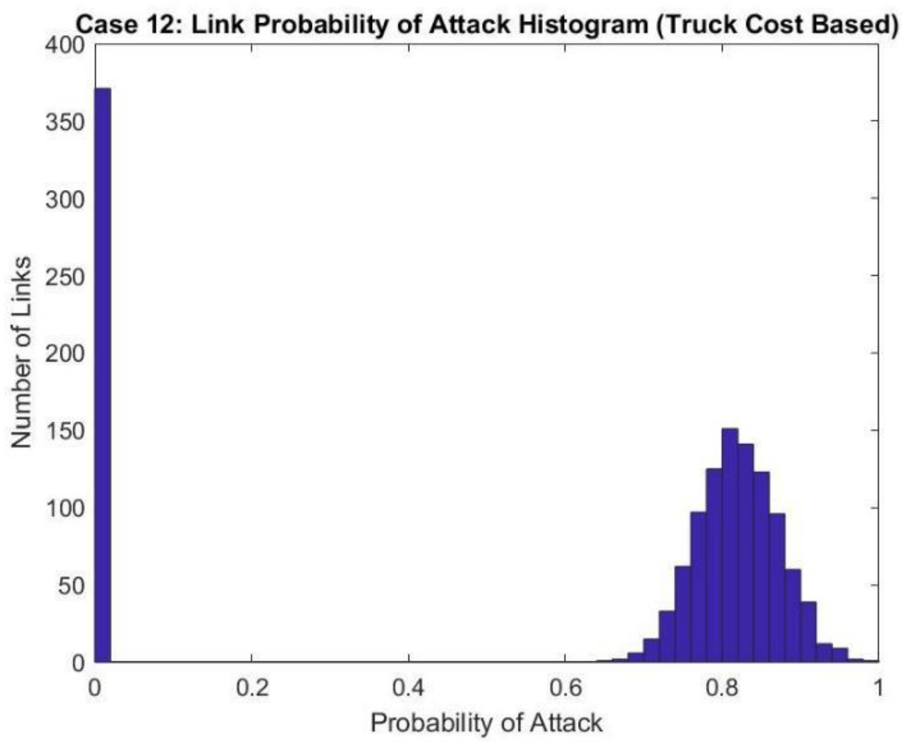


Figure 0-50. Histogram of Link Probability of Attack for Case 12 (Truck Cost Based).

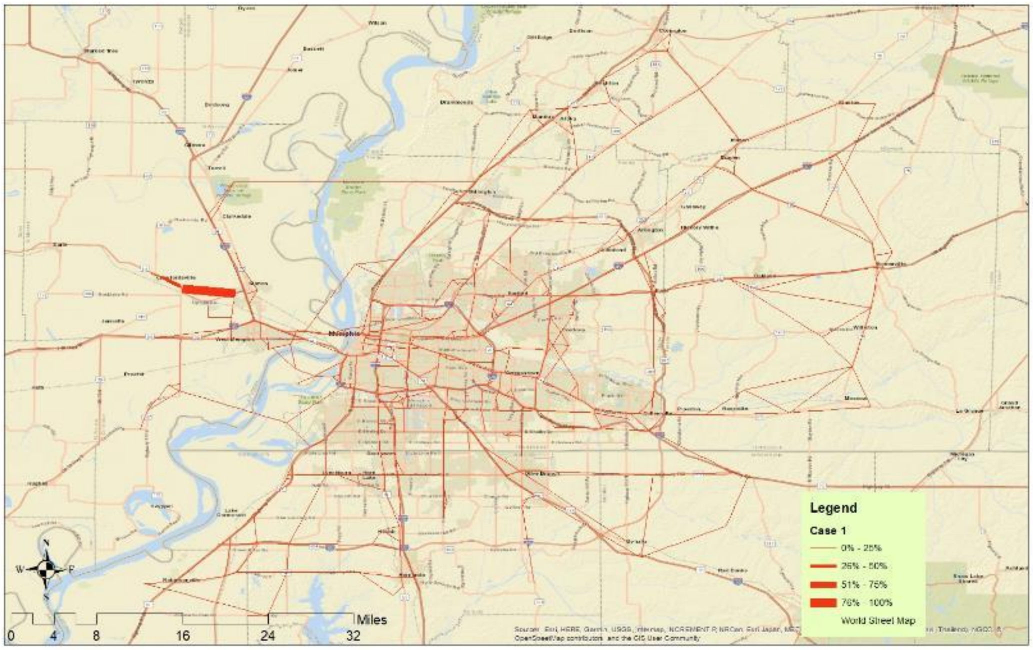


Figure 0-51. Link Probability for Attack for Case 1 (Truck Cost Based).

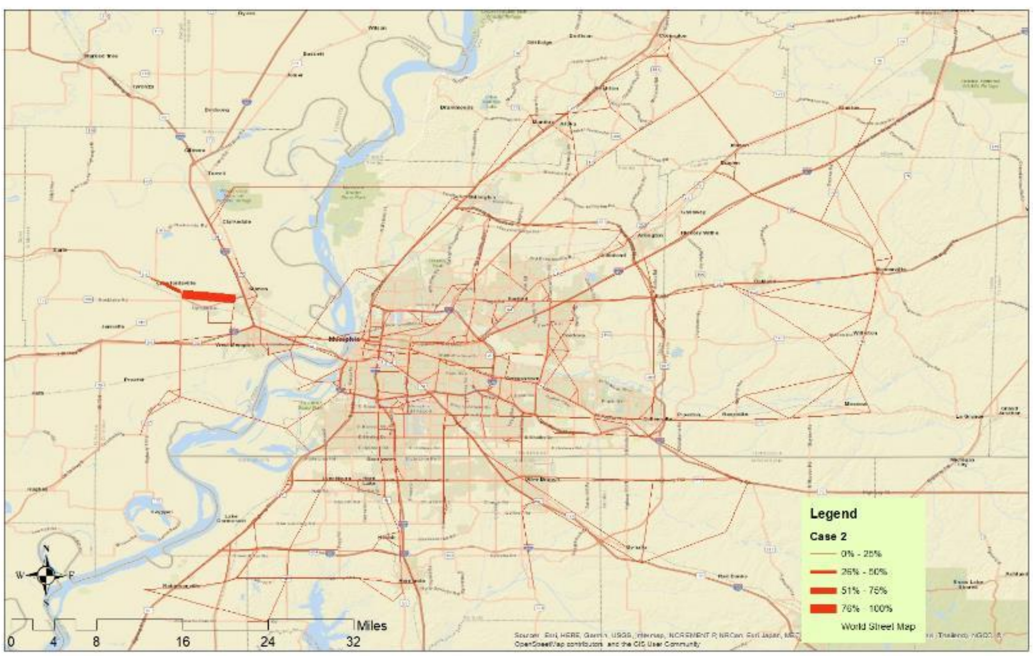


Figure 0-52. Link Probability for Attack for Case 2 (Truck Cost Based)

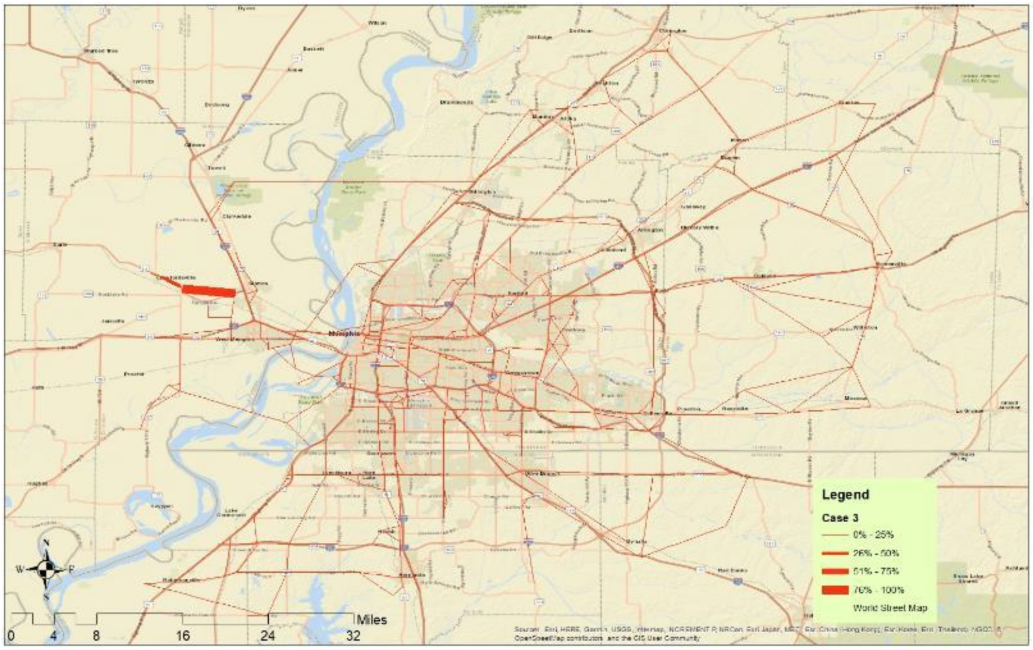


Figure 0-53. Link Probability for Attack for Case 3 (Truck Cost Based)

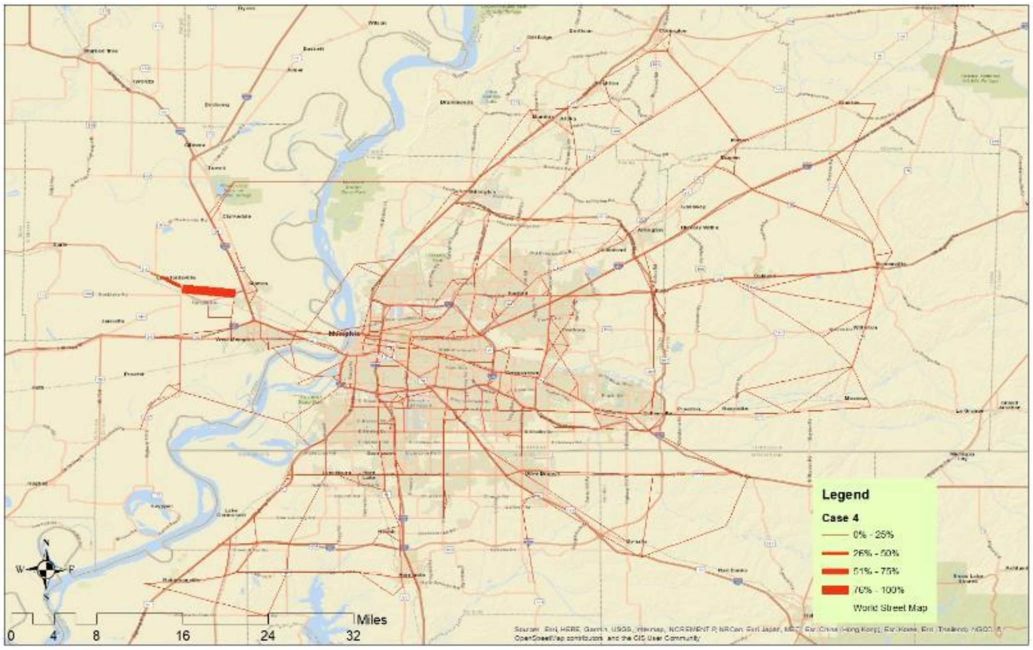


Figure 0-54. Link Probability for Attack for Case 4 (Truck Cost Based)

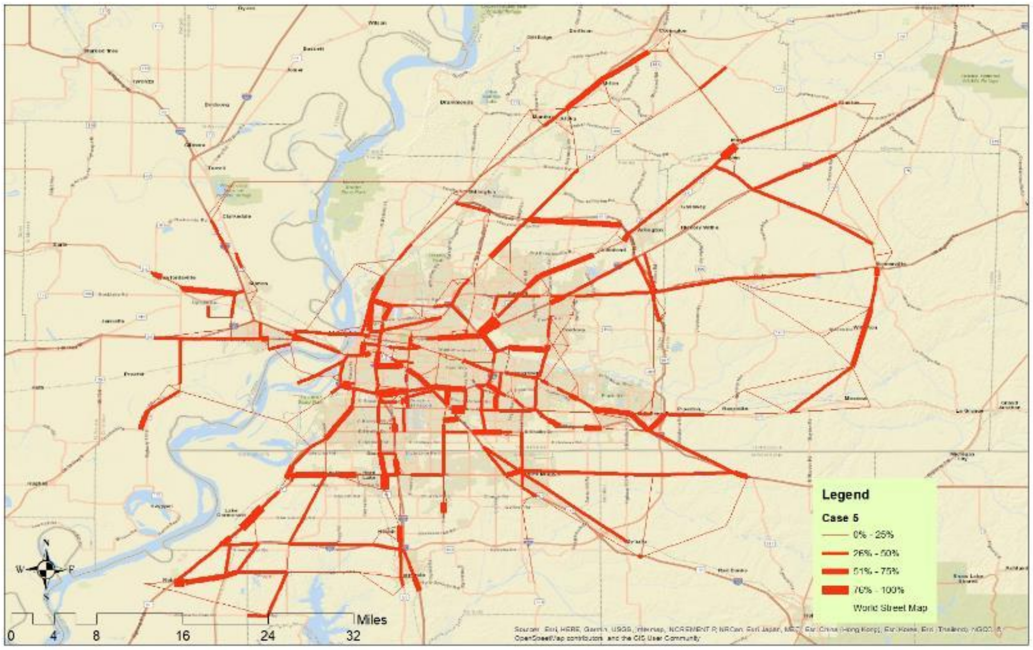


Figure 0-55. Link Probability for Attack for Case 5 (Truck Cost Based)

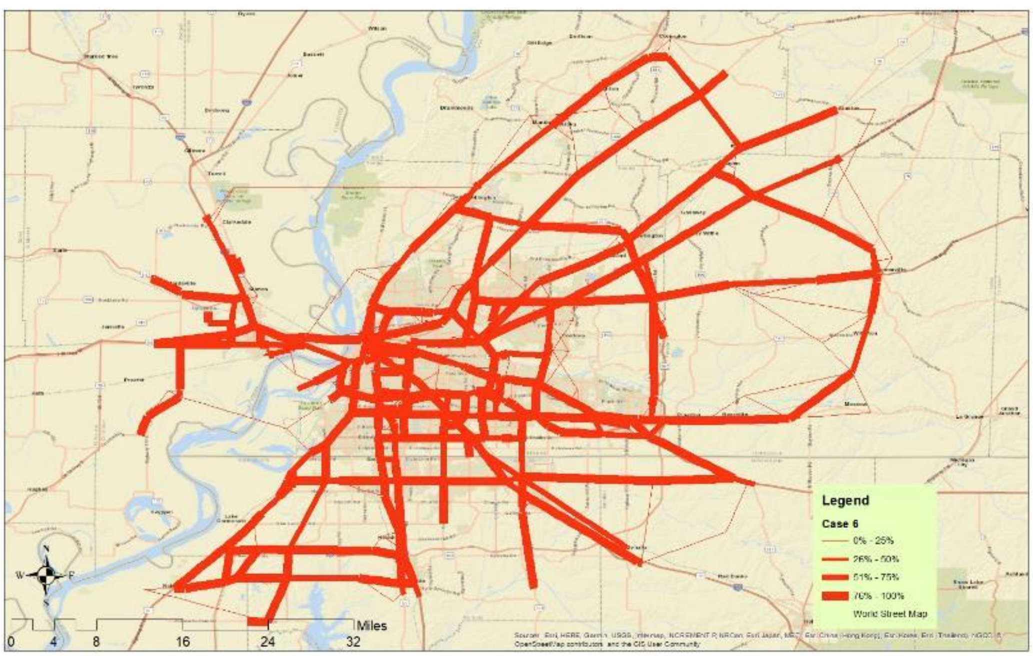


Figure 0-56. Link Probability for Attack for Case 6 (Truck Cost Based)

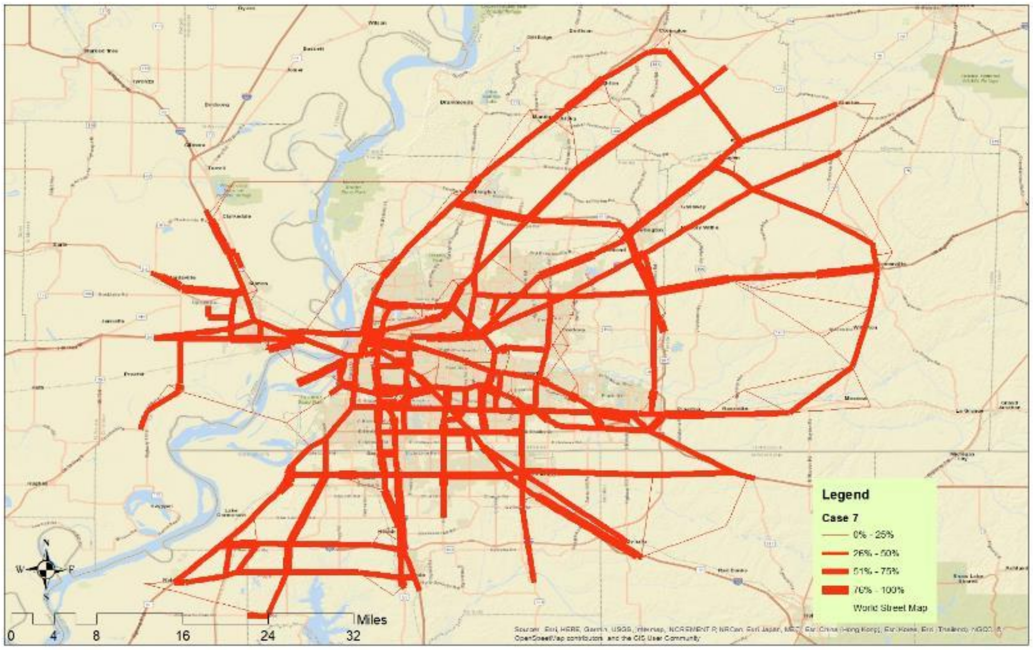


Figure 0-57. Link Probability for Attack for Case 7 (Truck Cost Based)

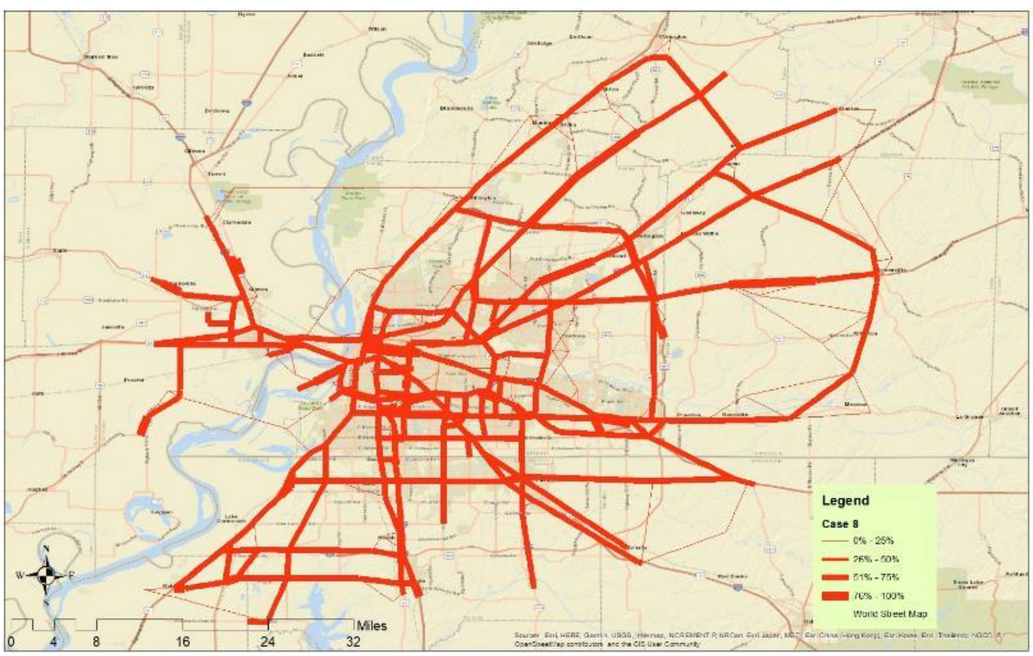


Figure 0-58. Link Probability for Attack for Case 8 (Truck Cost Based)

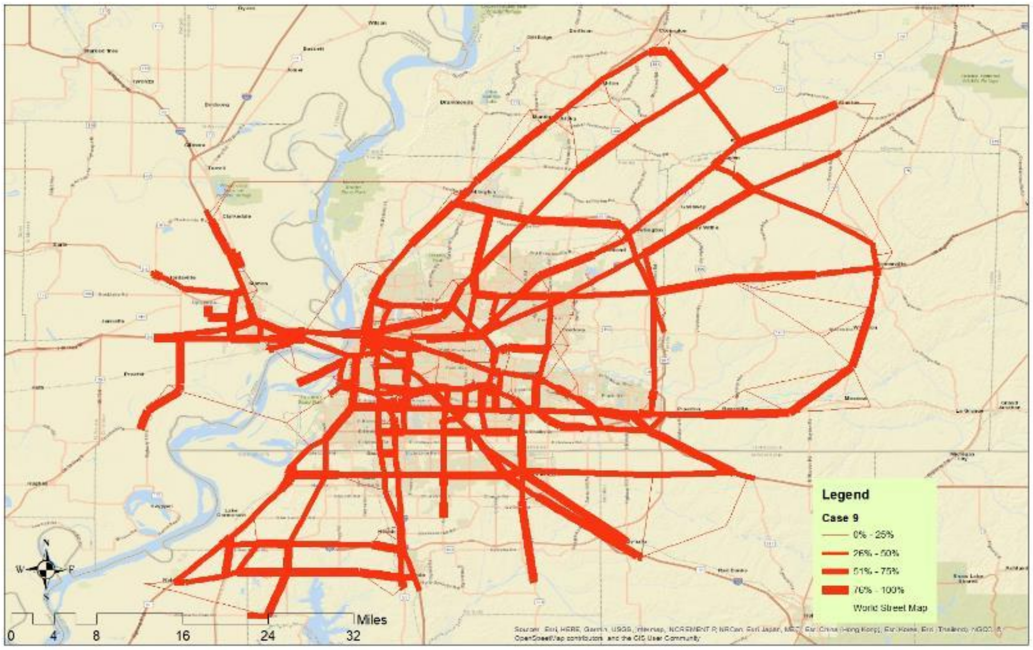


Figure 0-59. Link Probability for Attack for Case 9 (Truck Cost Based)

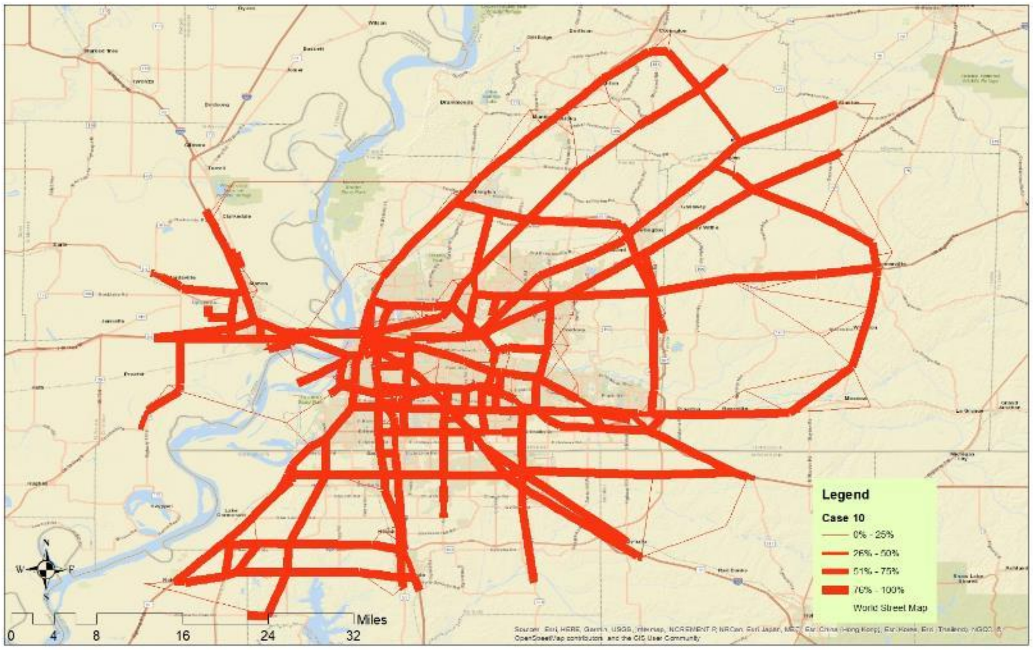


Figure 0-60. Link Probability for Attack for Case 10 (Truck Cost Based)

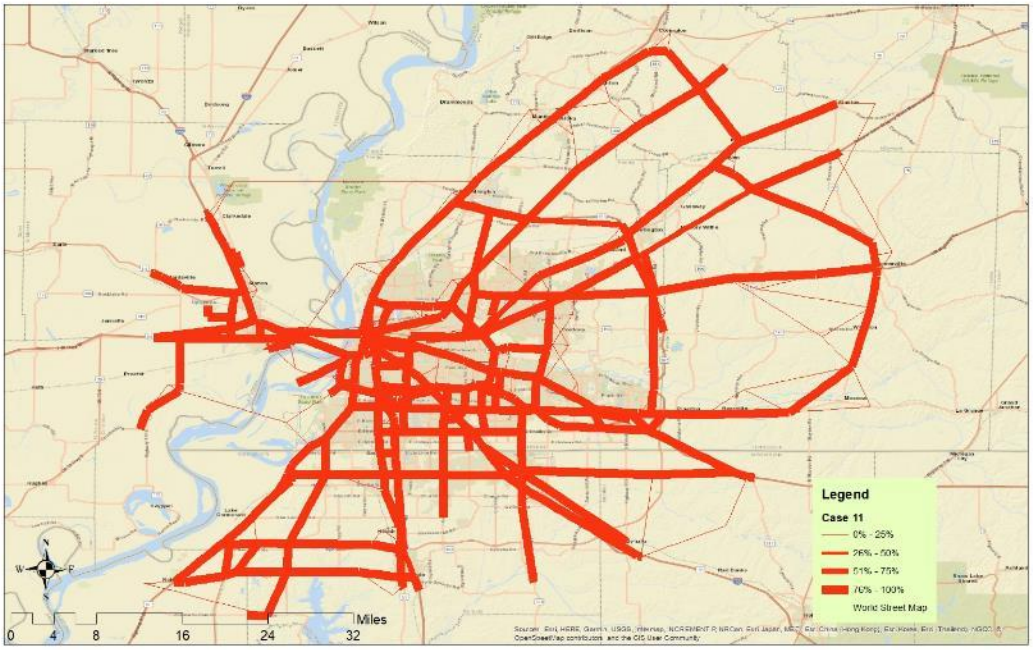


Figure 0-61. Link Probability for Attack for Case 11 (Truck Cost Based)

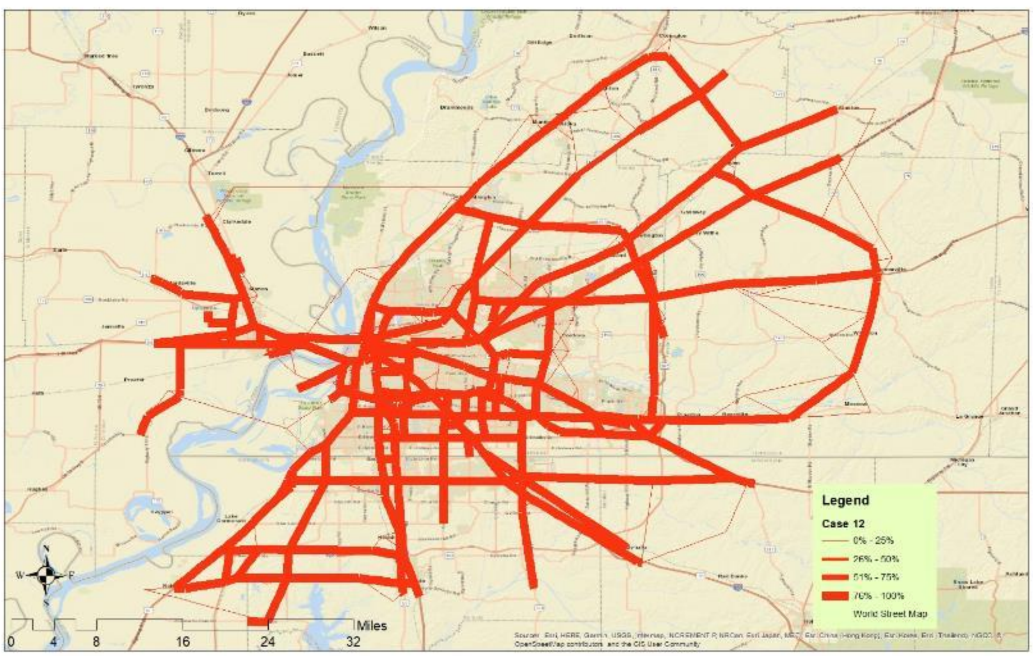


Figure 0-62. Link Probability for Attack for Case 12 (Truck Cost Based)

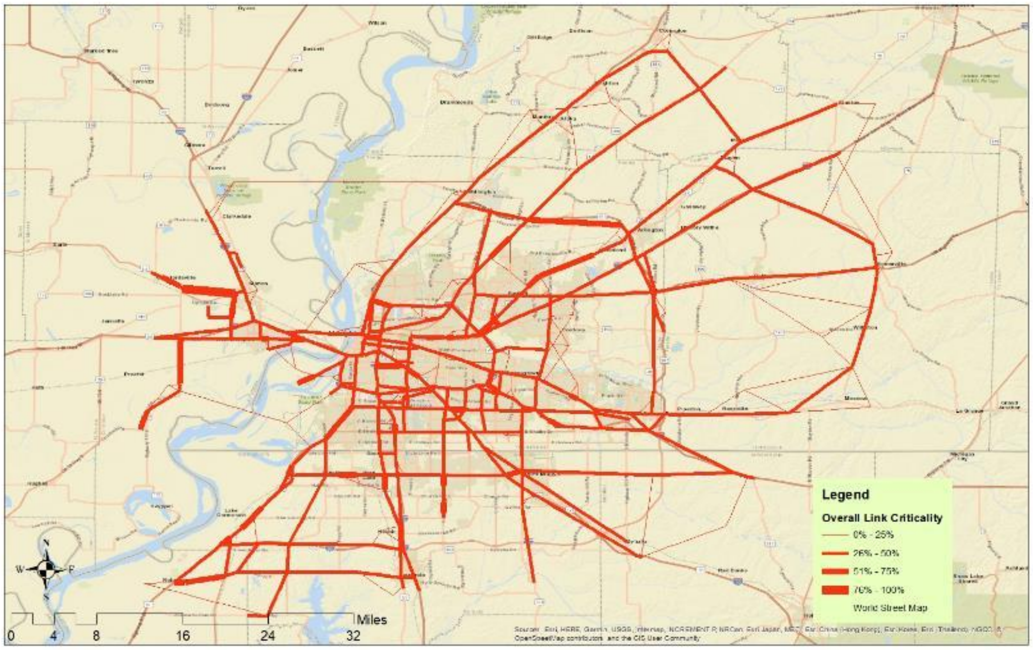


Figure 0-63. Overall Link Probability for Attack (Truck Cost Based).

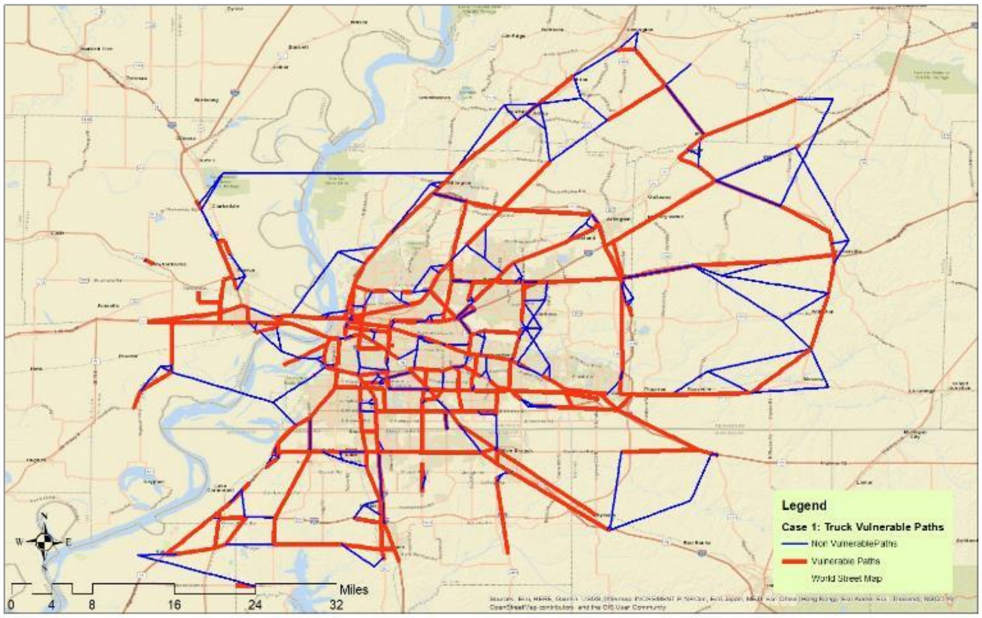


Figure 0-64. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 1

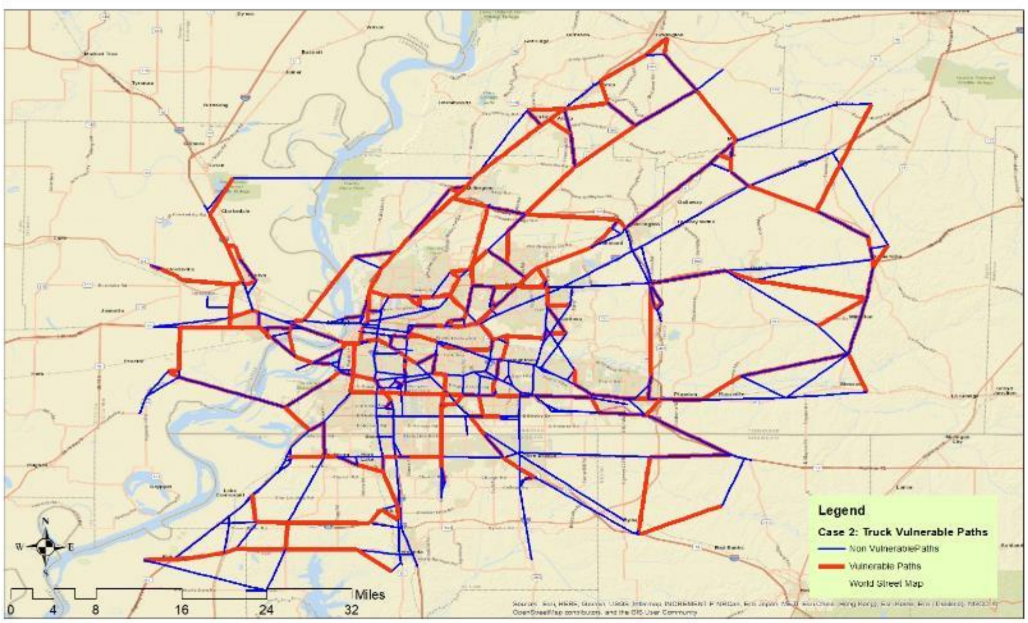


Figure 0-65. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 2

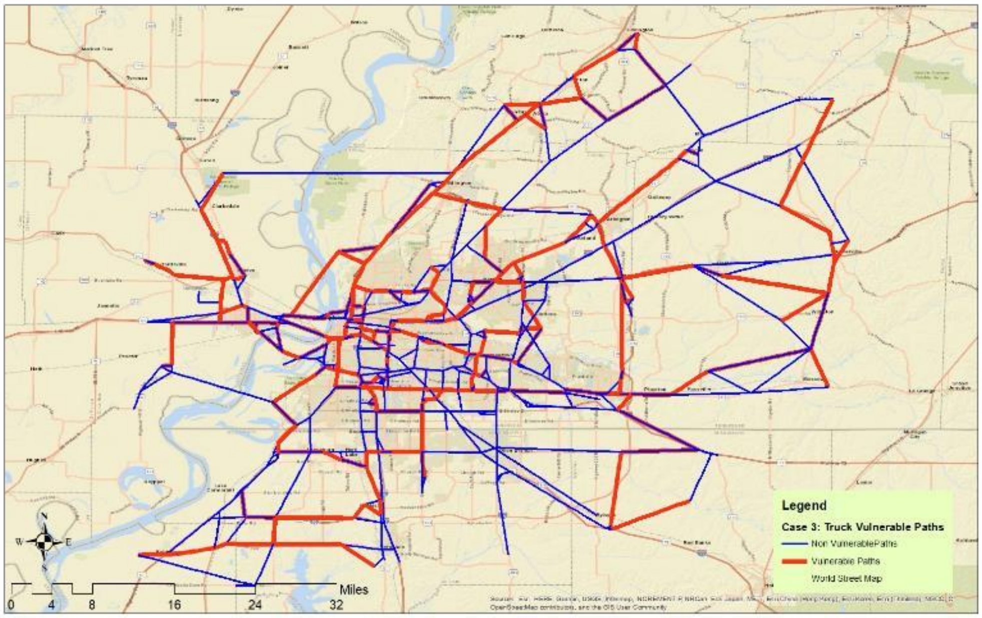


Figure 0-66. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 3

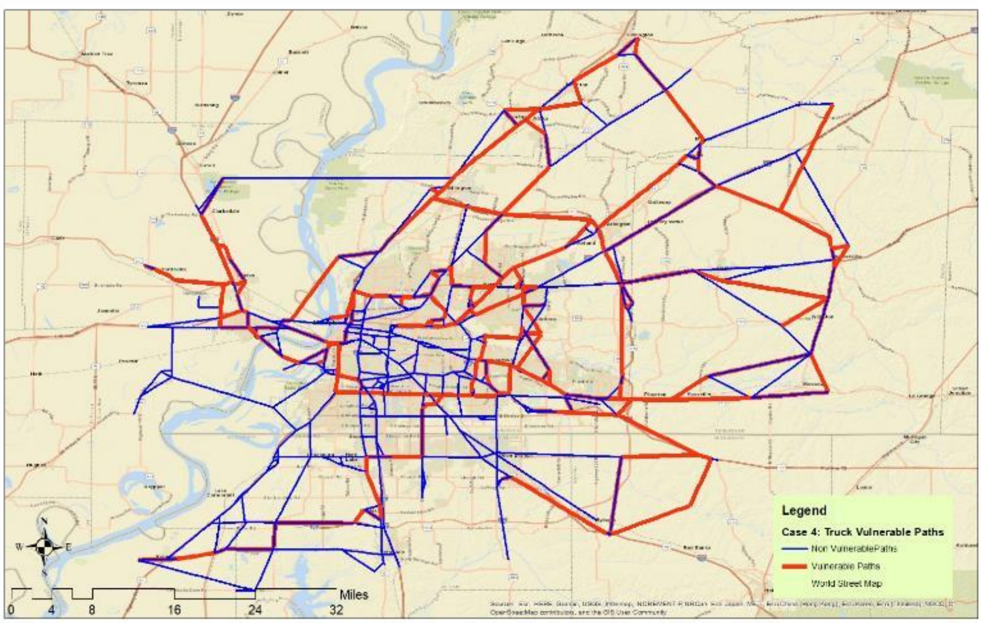


Figure 0-67. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 4

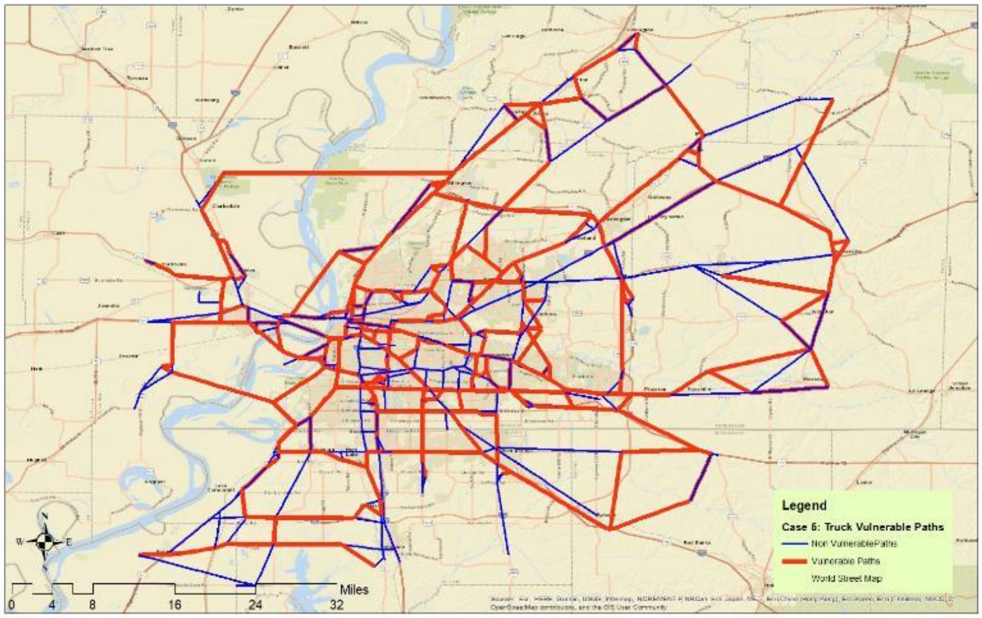


Figure 0-68. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 5

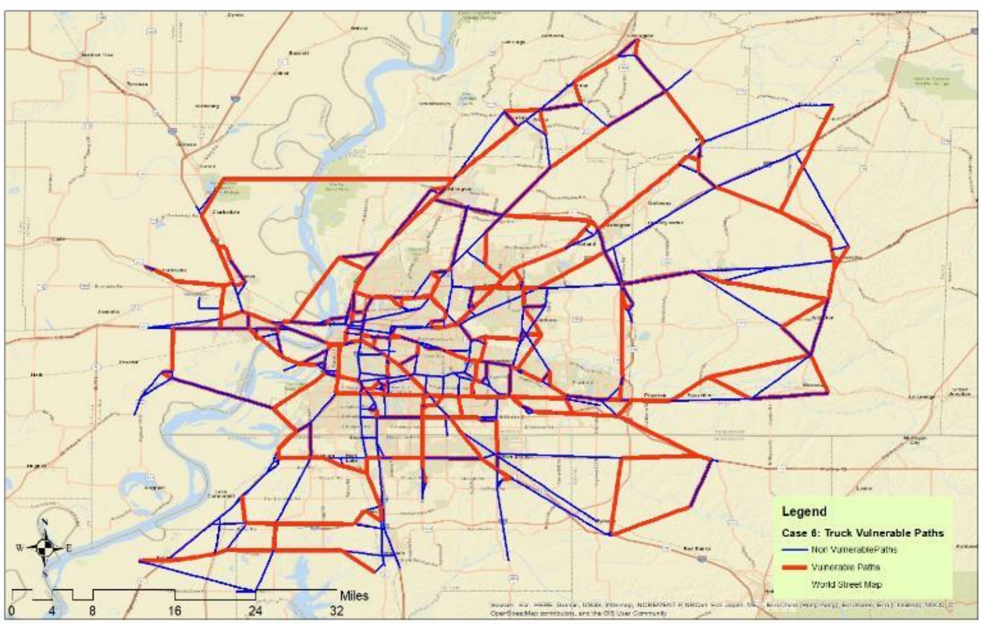


Figure 0-69. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 6

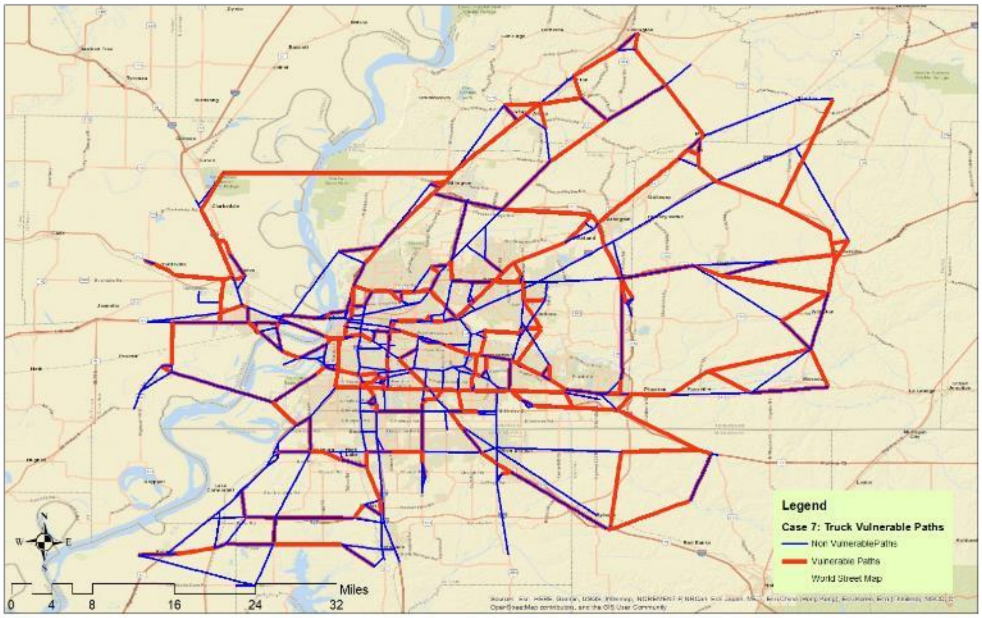


Figure 0-70. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 7

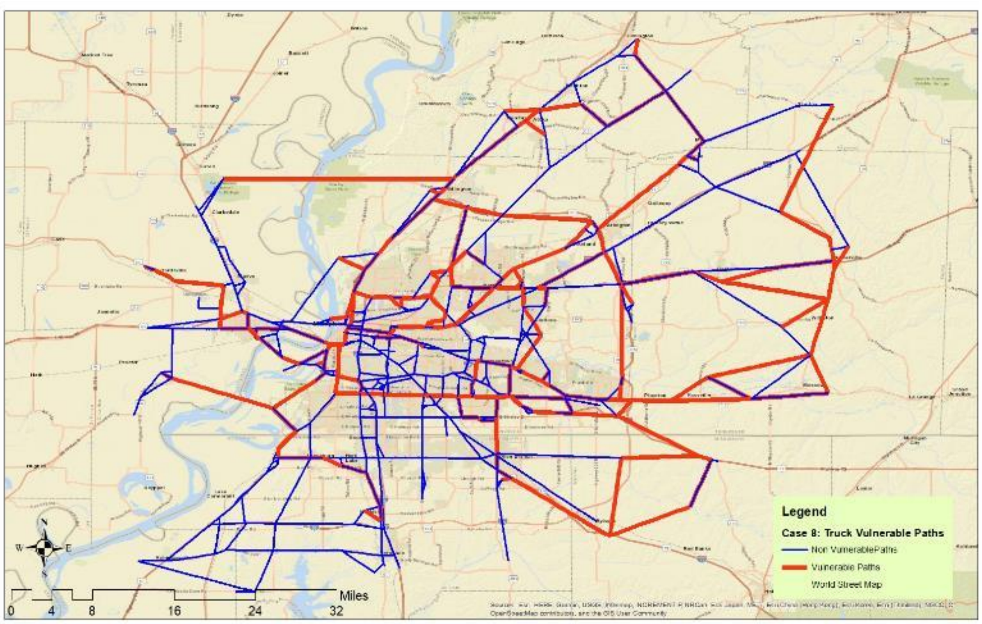


Figure 0-71. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 8

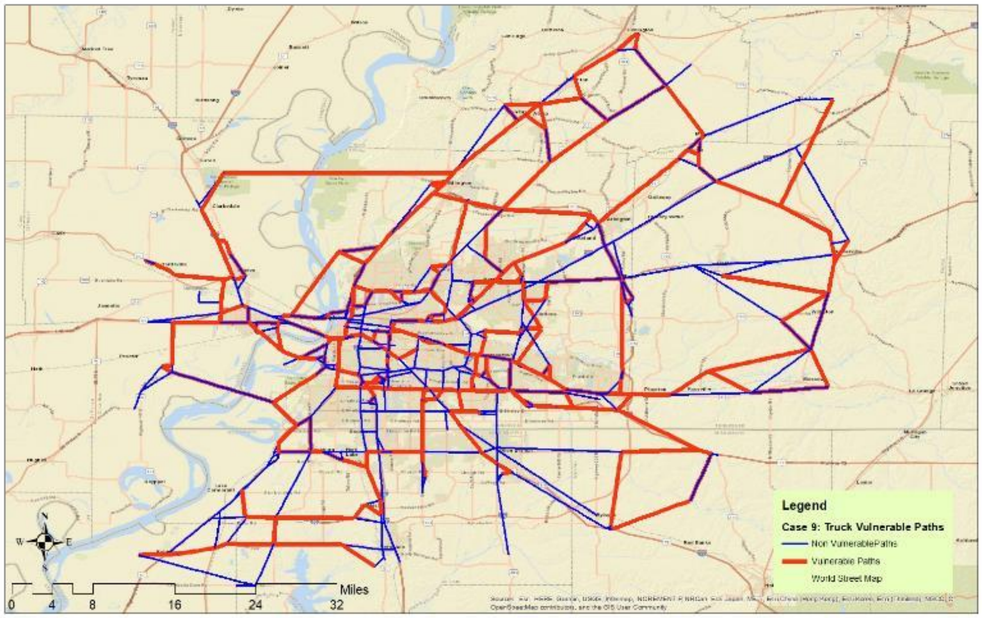


Figure 0-72. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 9

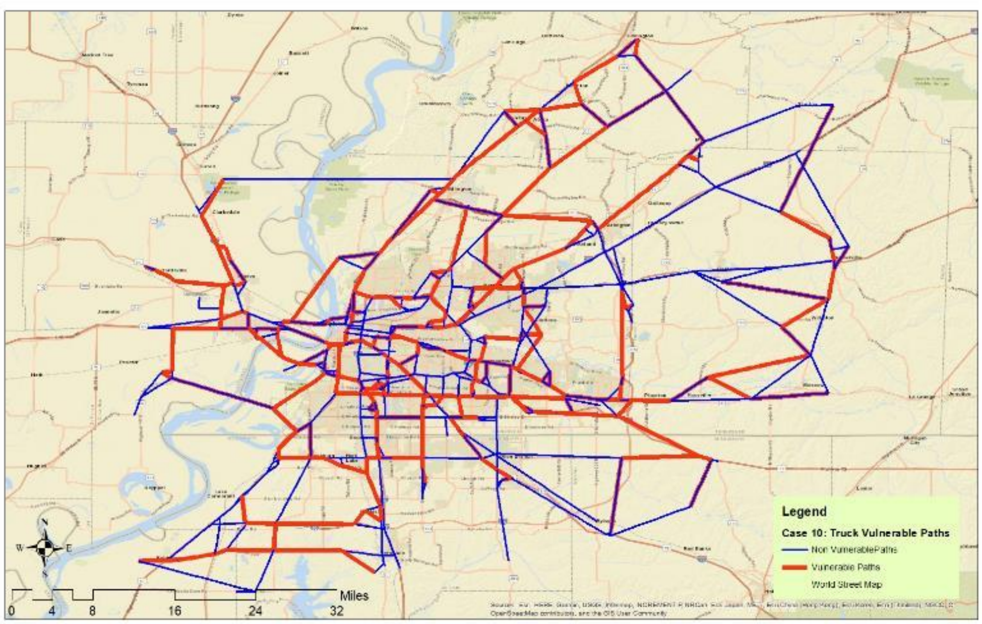


Figure 0-73. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 10

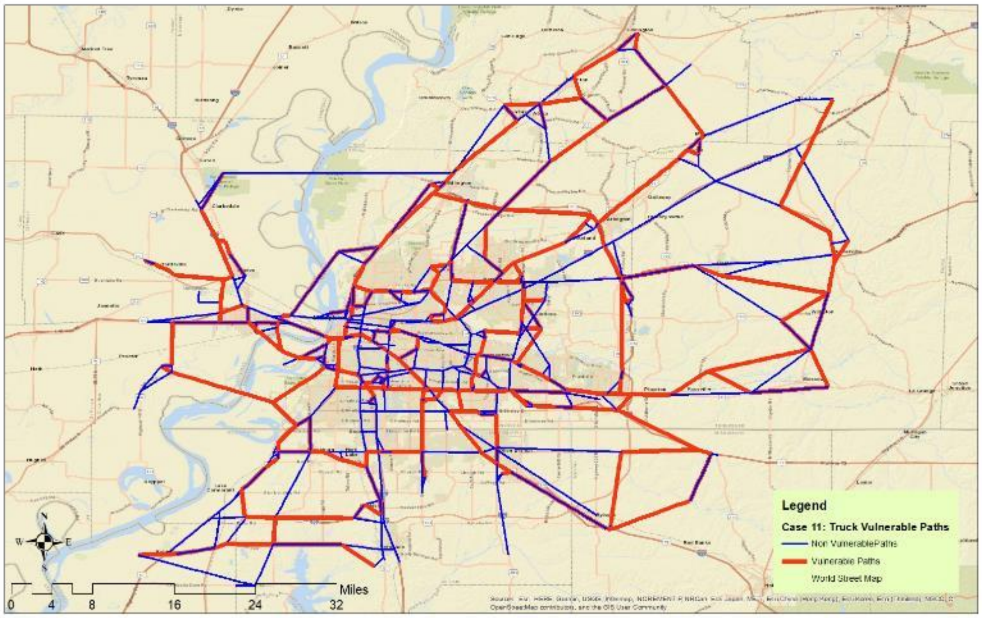


Figure 0-74. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 11

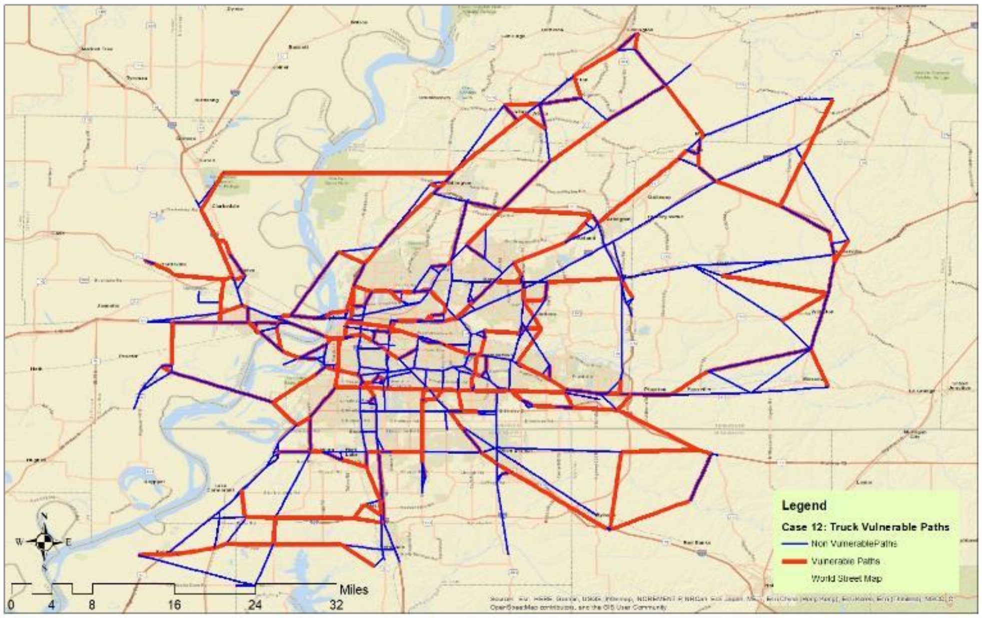


Figure 0-75. Truck Critical Paths Between Top Five Affected Origin Destination Pairs and First Ten Sets of Critical Links for Case 12

CHAPTER 5: CONCLUSIONS AND FUTURE RESEARCH

In this project a modeling framework, solution algorithms, and GIS-based tools that can assist decision makers in identifying and ranking vulnerable and critical links and paths of a transportation network for both passengers and freight was developed and implements in Memphis, TN. The developed tools and framework can be used to account for different type of attackers possessing high to low intelligence and tools to identify links to compromise. A number of numerical experiments that were performed showed that the transportation network is extremely vulnerable to attacks and in cases of total capacity loss the network will fail most of the times. Additional insights drawn from this research showed that the attacks concentrated around origins and destination with a high amount of demand in a way that would effectively isolate that origin or destination (i.e., a bridge) and this concentration of attacks spanned all the cases evaluated (when the capacity reduction was high). Also, in the cases where the defender would try to protect the links around the origins and destinations, the attacker would simply shift attacks downstream on the same roadways and still establish the desired isolation of the origin or destination. One interesting result, that can help in the decision making and in the implementation of link protection plans, was that the (intelligent) attacker's focus on a small number of links increases with the severity of the attack and that attacks by unintelligent attackers will, most likely, have no significant impact on the networks performance.

5.1 Dissemination and Outreach

The research team is in the process of scheduling presentations of the project outcomes to the State and Regional Level Freight Advisory Committees in Tennessee, MPOs in Tennessee, and the Tennessee Model Users Group. The research team will also submit results from the projects to academic journals and conferences for consideration for publication and presentation.

5.2 Future research

There are several avenues of future research that can improve upon the work presented herein. These research avenues involve the expansion of the hierarchical three-level game proposed in this research by introducing a combination of sets of links with capital investment that protect and/or increase capacity. These links can further be allowed to be attacked with a decreased capacity reduction as compared to the case where no protection or capacity increase has occurred by the defender. Other improvements that could be implemented include the use of different traffic assignment algorithms and the development of an ArcGIS tool that would implement the models and procedures presented in Chapter 4.

REFERENCES

Abounacer, R., Rekik, M., Renaud, J., 2014. An exact solution approach for multi-objective location–transportation problem for disaster response. Computers & Operations Research 41, 83–93.

Alderson, David L, Brown, G.G., Carlyle, W.M., Wood, R.K., 2011. Solving defender-attacker-defender models for infrastructure defense. DTIC Document.

Alderson, David L., Brown, G.G., Carlyle, W.M., Wood, R.K., 2011. Solving Defender-Attacker-Defender Models for Infrastructure Defense, in: 12th INFORMS Computing Society Conference. Presented at the Operations Resaerch, Computing, and Homeland Defense, INFORMS, pp. 28–49. https://doi.org/10.1287/ics.2011.0047

Barceló, J. (Ed.), 2010. Fundamentals of traffic simulation, International series in operations research & management science. Springer, New York.

Bar-Gera, H., 2010. Traffic assignment by paired alternative segments. Transportation Research Part B: Methodological 44, 1022–1046. https://doi.org/10.1016/j.trb.2009.11.004

Bell, M.G.., Kanturska, U., Schmocker, J.-D., Fonzone, A., 2008. Attacker-defender models and road network vulnerability. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 366, 1893–1906. https://doi.org/10.1098/rsta.2008.0019

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

Berdica, K., Mattsson, L.-G., 2007. Vulnerability: a model-based case study of the road network in Stockholm, in: Critical Infrastructure. Springer, pp. 81–106.

Bricha, N., Nourelfath, M., 2013. Critical supply network protection against intentional attacks: A game-theoretical model. Reliability Engineering & System Safety 119, 1–10. https://doi.org/10.1016/j.ress.2013.05.001

Cao, J.X., Li, X.X., Wang, Z.Y., Wu, J., 2013. The Robust Model of Continuous Transportation Network Design Problem with Demand and Cost Uncertainties. Procedia - Social and Behavioral Sciences 96, 970–980. https://doi.org/10.1016/j.sbspro.2013.08.111

Cats, O., Jenelius, E., n.d. Planning for the unexpected: The value of reserve capacity for public transport network robustness. Transportation Research Part A: Policy and Practice. https://doi.org/10.1016/j.tra.2015.02.013

Chen, A., Yang, C., Kongsomsaksakul, S., Lee, M., 2007. Network-based accessibility measures for vulnerability analysis of degradable transportation networks. Networks and Spatial Economics 7, 241–256.

Chen, B.Y., Lam, W.H., Sumalee, A., Li, Q., Li, Z.-C., 2012. Vulnerability analysis for large-scale and congested road networks with demand uncertainty. Transportation Research Part A: Policy and Practice 46, 501–516.

Clegg, R., 2007. Empirical studies on road traffic response to capacity reduction. Transportation and traffic theory 155–178.

Dalziell, E., Nicholson, A., 2001. Risk and impact of natural hazards on a road network. Journal of transportation engineering 127, 159–166.

de Araújo, D.R.B., Bastos-Filho, C.J. a., Martins-Filho, J.F., 2015. An evolutionary approach with surrogate models and network science concepts to design optical networks. Engineering Applications of Artificial Intelligence 43, 67–80. https://doi.org/10.1016/j.engappai.2015.04.004

Dehghanisanij, M., Flintsch, G.W., McNeil, S., 2013. Vulnerability analysis of degrading roadway networks, in: TRB 2013 Annual Meeting, Transportation Research Board.

Dimitriou, L., Stathopoulos, A., 2009. Optimal co-evolutionary strategies for the competitive maritime network design problem. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 5484 LNCS, 818–827. https://doi.org/10.1007/978-3-642-01129-0_92

Elvik, R., 2000. How much do road accidents cost the national economy? Accident Analysis & Prevention 32, 849–851.

Farahani, R.Z., Miandoabchi, E., Szeto, W.Y., Rashidi, H., 2013. A review of urban transportation network design problems. European Journal of Operational Research 229, 281–302. https://doi.org/10.1016/j.ejor.2013.01.001

Flisberg, P., Lidén, B., Rönnqvist, M., 2009. A hybrid method based on linear programming and tabu search for routing of logging trucks. Computers & Operations Research 36, 1122–1144. https://doi.org/10.1016/j.cor.2007.12.012

Florian, M., Morosan, C.D., 2014. On uniqueness and proportionality in multi-class equilibrium assignment. Transportation Research Part B: Methodological 70, 173–185. https://doi.org/10.1016/j.trb.2014.06.011

Gallo, M., Acierno, L.D., Montella, B., n.d. Compendium of Papers A meta-heuristic algorithm for solving the road network design problem in regional contexts.

Gallo, M., D'Acierno, L., Montella, B., 2012. A Meta-heuristic Algorithm for Solving the Road Network Design Problem in Regional Contexts. Procedia - Social and Behavioral Sciences 54, 84–95. https://doi.org/10.1016/j.sbspro.2012.09.728

Golias, M.M., Higgs, B., 2016. Discovering the Vulnerable Physical Routes in a Network.

Golob, T.F., Recker, W.W., 2003. Relationships among urban freeway accidents, traffic flow, weather, and lighting conditions. Journal of Transportation Engineering 129, 342–353.

Higgs, B., Golias, M.M., Mishra, S., 2017. Multi-Level Multi-Objective Vulnerability Assessment of Transportation Networks. Presented at the 96th Annual Meeting of the TRB, Washington, DC.

Higgs, B., Naimi, A., Golias, M.M., Mishra, S., 2016. An innovative approach to solve the network design problem concerning intelligent vulnerabilities. Presented at the Annual Meeting of the TRB, Washington, DC.

Jenelius, Erik, 2010. Large-scale road network vulnerability analysis.

Jenelius, E., 2010. Redundancy importance: Links as rerouting alternatives during road network disruptions. 1st Conference on Evacuation Modeling and Management 3, 129–137. https://doi.org/10.1016/j.proeng.2010.07.013

Jenelius, E., Mattsson, L.-G., 2012. Road network vulnerability analysis of area-covering disruptions: A grid-based approach with case study. Transportation Research Part A: Policy and Practice, Network vulnerability in large-scale transport networks 46, 746–760. https://doi.org/10.1016/j.tra.2012.02.003

Jenelius, E., Petersen, T., Mattsson, L.-G., 2006. Road network vulnerability: Identifying important links and exposed regions. Transportation Research A 40, 537–560.

Kaplan, S., Garrick, B.J., 1981. On The Quantitative Definition of Risk. Risk Analysis 1, 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Karami, A., Guerrero-zapata, M., 2015. Neurocomputing A hybrid multiobjective RBF-PSO method for mitigating DoS attacks in Named Data Networking. Neurocomputing 151, 1262–1282. https://doi.org/10.1016/j.neucom.2014.11.003

Kim, Y., Kang, W.-H., Song, J., 2012a. Assessment of seismic risk and importance measures of interdependent networks using a non simulation-based method. Journal of Earthquake Engineering 16, 777–794. https://doi.org/10.1080/13632469.2012.661121

Kim, Y., Kang, W.-H., Song, J., 2012b. Assessment of seismic risk and importance measures of interdependent networks using a non simulation-based method. Journal of Earthquake Engineering 16, 777–794. https://doi.org/10.1080/13632469.2012.661121

Knoop, V.L., Snelder, M., van Zuylen, H.J., Hoogendoorn, S.P., 2012. Link-level vulnerability indicators for real-world networks. Transportation Research Part A: Policy and Practice 46, 843–854.

Kumar, A., Peeta, S., 2015. Entropy weighted average method for the determination of a single representative path flow solution for the static user equilibrium traffic assignment problem. Transportation Research Part B: Methodological 71, 213–229. https://doi.org/10.1016/j.trb.2014.11.002

Kumar, A., Peeta, S., 2014. SLOPE-BASED PATH SHIFT PROPENSITY ALGORITHM FOR THE STATIC TRAFFIC ASSIGNMENT PROBLEM. INTERNATIONAL JOURNAL FOR TRAFFIC AND TRANSPORT ENGINEERING 4, 297–319. https://doi.org/10.7708/ijtte.2014.4(3).05

Latora, V., Marchiori, M., 2005. Vulnerability and protection of infrastructure networks. Physical Review E 71, 015103.

Lu, Q., George, B., Shekhar, S., 2005. Capacity Constrained Routing Algorithms for Evacuation Planning: A Summary of Results, in: Medeiros, C.B., Egenhofer, M.J., Bertino, E. (Eds.), Advances in Spatial and Temporal Databases, Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 291–307.

Lu, Q.-C., Peng, Z.-R., 2011. Vulnerability Analysis of Transportation Network Under Scenarios of Sea Level Rise. Transportation Research Record: Journal of the Transportation Research Board 2263, 174–181.

Luathep, P., Sumalee, A., Ho, H.W., Kurauchi, F., 2011. Large-scale road network vulnerability analysis: a sensitivity analysis based approach. Transportation 38, 799–817. https://doi.org/10.1007/s11116-011-9350-0

LUATHEP, P., SUWANNO, P., TANEERANANON, P., 2013a. Identification of Critical Locations in Road Networks due to Disasters. Presented at the Proceedings of the Eastern Asia Society for Transportation Studies.

LUATHEP, P., SUWANNO, P., TANEERANANON, P., 2013b. Identification of Critical Locations in Road Networks due to Disasters. Presented at the Proceedings of the Eastern Asia Society for Transportation Studies.

Mathew, T. V., Sharma, S., 2006. Continuous Network Design with Emission Pricing as a Bi-Level Optimization Problem. Applications of Advanced Technology in Transportation 804–809. https://doi.org/10.1061/40799(213)129

Miandoabchi, E., Daneshzand, F., Szeto, W.Y., Zanjirani Farahani, R., 2013. Multi-objective discrete urban road network design. Computers & Operations Research 40, 2429–2449. https://doi.org/10.1016/j.cor.2013.03.016

Miller-Hooks, E., Zhang, X., Faturechi, R., 2012. Measuring and maximizing resilience of freight transportation networks. Computers & Operations Research 39, 1633–1643.

Mouskos, K.C., 1991. A Tabu-based Heuristic Search Strategy to Solve a Discrete Transportation Equilibrium Network Design Problem.

Murray-Tuite, P.M., Mahmassani, H.S., 2004. Methodology for determining vulnerable links in a transportation network. Transportation Research Record 88–96.

Nagurney, A., Qiang, Q., 2007. A transportation network efficiency measure that captures flows, behavior, and costs with applications to network component importance identification and vulnerability, in: Proceedings of the POMS 18th Annual Conference, Dallas, Texas, USA, May.

Oppenheim, I.J., 1977. Vulnerability of Transportation and Water Systems to Seismic Hazard Methodology for Hazard Cost Evaluation, in: The Current State of Knowledge of Lifeline Earthquake Engineering. ASCE, pp. 394–409.

Parvaresh, F., Husseini, S.M.M., Golpayegany, S.A.H., Karimi, B., 2014. Hub network design problem in the presence of disruptions. Journal of Intelligent Manufacturing 25, 755–774. https://doi.org/10.1007/s10845-012-0717-7

Patriksson, M., Rockafellar, R.T., 2002. A Mathematical Model and Descent Algorithm for Bilevel Traffic Management. Transportation Science 36, 271–291. https://doi.org/10.1287/trsc.36.3.271.7826

Poljansek, K., Bono, F., Gutierrez, E., 2012. Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks. Earthq. Eng. Struct. Dyn. 41, 61–79. https://doi.org/10.1002/eqe.1118

Poorzahedy, H., Rouhani, O.M., 2007a. Hybrid meta-heuristic algorithms for solving network design problem. European Journal of Operational Research 182, 578–596. https://doi.org/10.1016/j.ejor.2006.07.038

Poorzahedy, H., Rouhani, O.M., 2007b. Hybrid meta-heuristic algorithms for solving network design problem. European Journal of Operational Research 182, 578–596. https://doi.org/10.1016/j.ejor.2006.07.038

Pratt, R., Lomax, T., 1996. Performance measures for multimodal transportation systems. Transportation Research Record: Journal of the Transportation Research Board 85–93.

Rossi, T.F., McNeil, S., Hendrickson, C., 1989. Entropy Model for Consistent Impact-Fee Assessment. Journal of Urban Planning and Development 115, 51–63. https://doi.org/10.1061/(ASCE)0733-9488(1989)115:2(51)

Scott, D.M., Novak, D.C., Aultman-Hall, L., Guo, F., 2006. Network Robustness Index: A new method for identifying critical links and evaluating the performance of transportation networks. Journal of Transport Geography 14, 215–227. https://doi.org/10.1016/j.jtrangeo.2005.10.003

Sharma, S., Mathew, T. V, 2011. Multiobjective network design for emission and travel-time trade-off for a sustainable large urban transportation network. Environment and Planning B: Planning and Design 38, 520–538. https://doi.org/10.1068/b37018

Sherali, H.D., Carter, T.B., Hobeika, A.G., 1991. A location-allocation model and algorithm for evacuation planning under hurricane/flood conditions. Transportation Research Part B: Methodological 25, 439–452.

Smith, A.B., Katz, R.W., 2013. US billion-dollar weather and climate disasters: data sources, trends, accuracy and biases. Natural hazards 67, 387–410.

Sullivan, J.L., Novak, D.C., Aultman-Hall, L., Scott, D.M., 2010. Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: A link-based capacity-reduction approach. Transportation Research Part A: Policy and Practice 44, 323–336. https://doi.org/10.1016/j.tra.2010.02.003

Tampere, C.M., Stada, J., Immers, B., Peetermans, E., Organe, K., 2007. Methodology for identifying vulnerable sections in a national road network. Transportation Research Record: Journal of the Transportation Research Board 2012, 1–10.

Taylor, M.A., Sekhar, S.V., D'Este, G.M., 2006. Application of accessibility based methods for vulnerability analysis of strategic road networks. Networks and Spatial Economics 6, 267–291.

United States., 1964. Traffic assignment manual for application with a large, high speed computer. U.S. Dept. of Commerce, Bureau of Public Roads, Office of Planning, Urban Planning Division; for sale by the Superintendent of Documents, U.S. Govt. Print. Off., Washington.

Wang, Z., Chan, A.P.C., Yuan, J., Xia, B., Skitmore, M., Li, Q., 2015. Recent Advances in Modeling the Vulnerability of Transportation Networks. Journal of Infrastructure Systems 21, 06014002. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000232

Wu, J., Duenas-Osorio, L., 2013. Calibration and validation of a seismic damage propagation model for interdependent infrastructure systems. Earthquake Spectra 29, 1021–1041. https://doi.org/10.1193/1.4000160

Xie, F., Levinson, D., 2011. Evaluating the effects of the I-35W bridge collapse on road-users in the twin cities metropolitan region. Transportation Planning and Technology 34, 691–703. https://doi.org/10.1080/03081060.2011.602850

YANG, L., QIAN, D., 2012. Vulnerability Analysis of Road Networks. Journal of Transportation Systems Engineering and Information Technology 12, 105–110. https://doi.org/10.1016/S1570-6672(11)60188-8

Yun-peng, W., Yu-qin, F., Wen-xiang, L.I., Fulcher, W.C., Zhang, L., n.d. Road network vulnerability analysis based on improved ant colony algorithm 1–11.

Zhang, L., Wen, Y., Huang, Z., Jin, M., 2010. Framework of Calculating the Measures of Resilience (MOR) for Intermodal Transportation Systems.

Zhang, M., Lomax, T., 2008. Estimating Congestion Index at the Link Level with TransCAD GIS, in: Plan, Build, and Manage Transportation Infrastructure in China. ASCE, pp. 7–17.

Zhao, F., Zeng, X., 2006. Simulated Annealing–Genetic Algorithm for Transit Network Optimization. Journal of Computing in Civil Engineering 20, 57–68. https://doi.org/10.1061/(ASCE)0887-3801(2006)20:1(57)

APPENDIX A: GIS TOOLBOX USER MANUAL

The research team developed an ArcGIS toolbox that implements the three heuristic-based approaches described in section 2. This section contains the user manual of the ArcGIS toolbox with examples using the Freight Analysis Framework network for Shelby County, TN. The toolbox and the example data can be downloaded from: https://www.dropbox.com/s/zmvn27tvpcpimug/REES%20Software.zip?dl=0

NET CONVERSION TOOL

Description

This tool will convert TransCAD transportation network exported as ESRI Shape to the required input format of the GSB, RSH and KSP Tool input parameter Network.

Example Input Files

- **Network Shapefile.shp** – Transportation Network exported from TransCAD as ESRI Shape

STEP 1

Open newly added REES Tools toolbox and launch Net Conversion Tool (see Figure A-1)

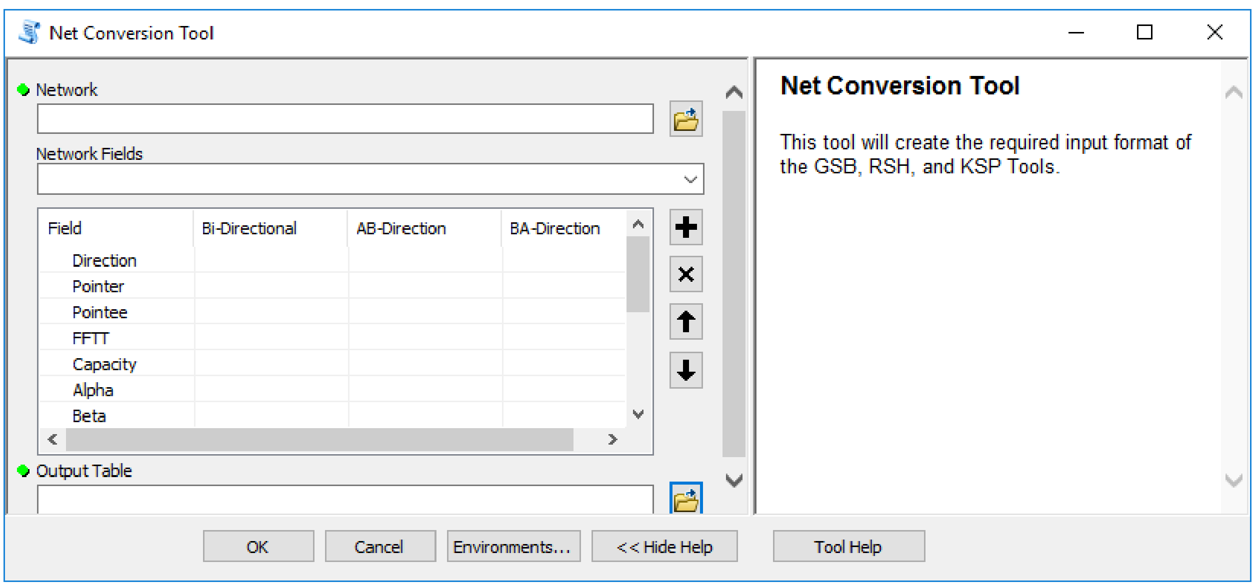


Figure A-1 Net Conversion Tool

STEP 2

Input path to transportation network (.shp) into the tool first input parameter Network (see Figure A-2).

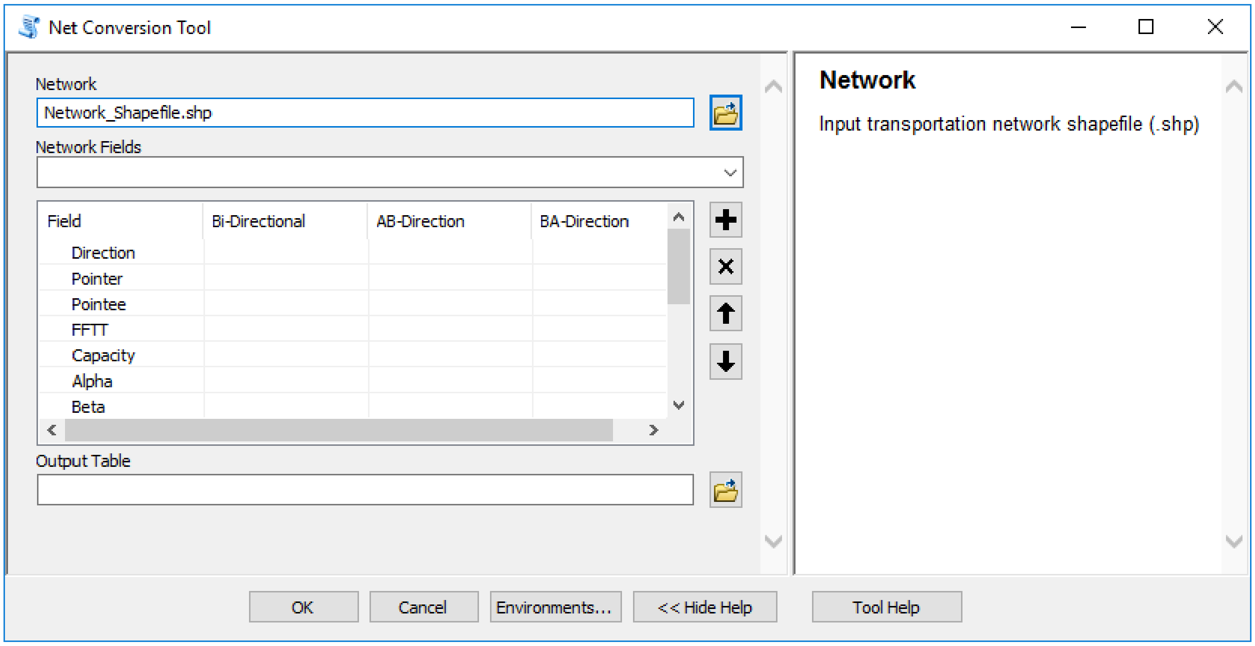


Figure A-2 Input Transportation Network Shapefile (.shp)

STEP 3

Select the input network attribute fields to the corresponding table fields and their direction in input parameter Network Fields (see Figure A-3).

(Direction [Denoted as: Bi-Directional = 0, AB-Direction = 1, BA-Direction = -1], Pointer (link begin node ID) and Pointee (link end node ID) are required fields for the tool to be executed, for the other fields if no corresponding fields will be selected the fields will be assigned with null values, except Alpha and Beta fields, where default values of 0.15 and 4 will be selected.)

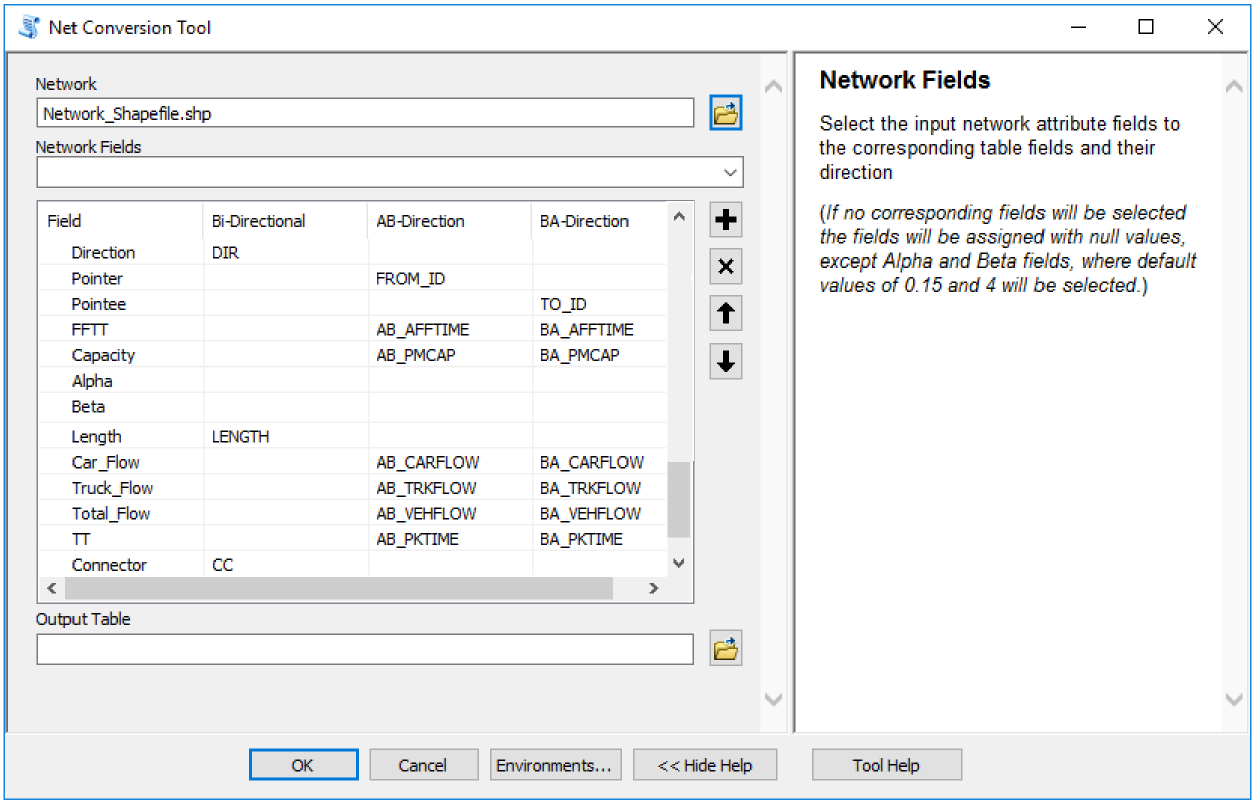


Figure A-3 Select the corresponding Input Network Attribute Fields

STEP 4

In toolbox Output Table parameter input output folder path where processed files will be exported (see Figure A-4).

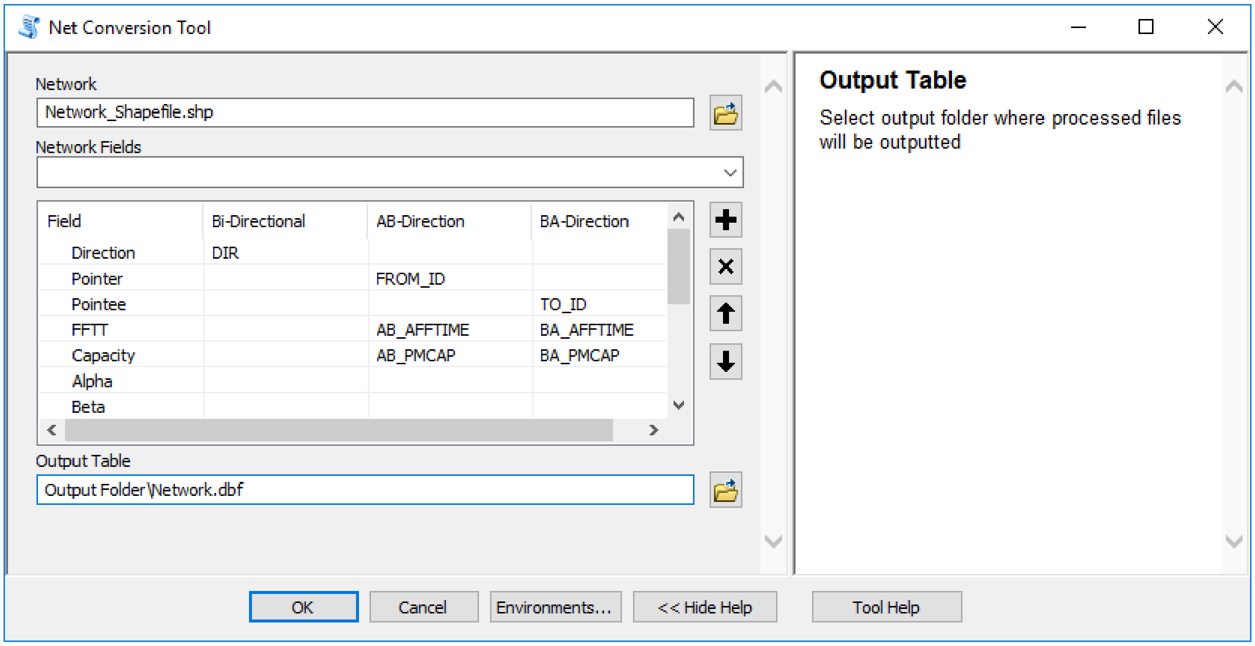


Figure A-4 Input Path to Output Table

STEP 5

Once all required parameters are inputted, press OK to execute the application. The ArcGIS application invokes a task completion window, which reports status of each task (see Figure A-5). Also, processed table (see Figure A-6) in (.dbf) format will be imported to ArcMap display.

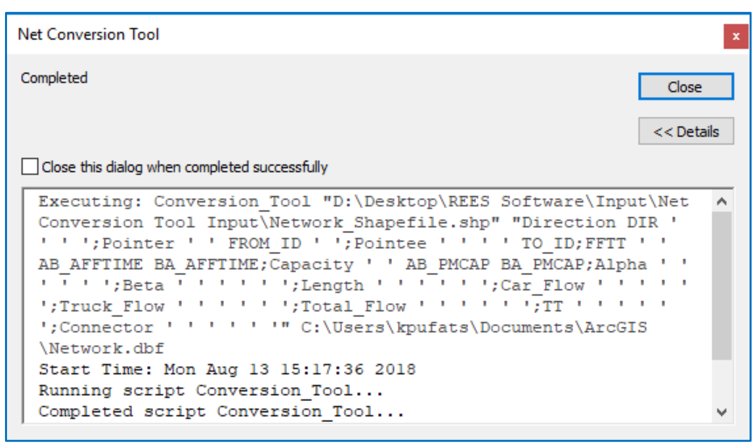


Figure A-5 Application Performance Task Window

Network

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
0	1	332761	332886	2.59158	3953.300971	0.15	4	2.567685	9388.449217	1841.200848	11229.650065	0	0
1	2	1002518	332971	4.789769	40000	0.15	4	2.197628	1759.76305	0	1759.76305	0	1
2	3	1002518	333184	4.789769	40000	0.15	4	4.215873	4866.279561	1383.315105	6249.594665	0	1
3	4	332817	333286	6.12815	3063.550015	0.15	4	4.678201	5.838744	0	5.838744	0	0
4	5	2004157	332761	4.624162	40000	0.15	4	2.970565	2000.36132	138.722257	2139.083578	0	1
5	6	332817	332761	1.00086	3063.550015	0.15	4	0.764052	717.936625	41.909628	759.846254	0	0
6	7	334809	334787	0.818759	2088.769535	0.15	4	0.240831	3830	0	3830	0.818839	0
7	8	2004985	334609	0.819589	974.855054	0.15	4	0.23898	910	0	910	0.819593	0
8	9	363190	363366	4.340041	1573.076839	0.15	4	3.799525	2358.540768	86.459232	2445	4.340099	0
9	10	360017	362484	4.100412	3953.300971	0.15	4	4.062604	8683.055147	354.545053	9037.600199	0	0

1 (0 out of 18826 Selected)

Figure A-6 Output Table

THE GREEDY SEARCH BASED VULNERABILITY TOOL (GSB TOOL)

Description

The Greedy Search Based Vulnerability Tool (GSB Tool) has two options to identify the most critical links on a transportation network. The first option involves user providing a table in a form of (.csv) or (.dbf) of Edge IDs and their corresponding percentage of capacity reduction, following input the tool will reduce the capacity of user provided links and run a traffic assignment. The second option involves user selecting field attributes and inputting weights, following input the tool will rank weighted attributes and reduce the capacity (selected by user) for the number of links (selected by user) and finally run a traffic assignment.

Example Input Files

Following tables were used in executing GSB Tool example in format of (.csv) (see Figure A-7) and (.dbf) (see Figure A-8).

- **Network.csv** – Transportation network with the following order of field attributes: Link ID for one direction, From Node, To Node, Free Flow Travel Time, Capacity, Alpha, Beta, Length, Car Flow, Truck Flow, Total Flow, Travel Time, and Connector (0 - No, 1 - yes).
- **Origin-Destination Matrix.csv** – Origin-Destination Matrix with the following order of field attributes: From Node, To Node, Car Demand, Truck Demand, and Total Demand.
- **User Defined Link IDs.csv** – User defined Link ID table with the following order of field attributes: Link ID for one direction and percentage of capacity reduction.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0	
2	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0	
3	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0	
4	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0	
5	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0	
6	6	142446	142454	0.06596	3337	0.15	4	0.076074	2491.711	393.9045	2885.616	0.077615	0	
7	7	126024	142446	0.017417	3337	0.15	4	0.020088	2491.711	393.9045	2885.616	0.020495	0	
8	8	142454	142462	0.085637	3337	0.15	4	0.098768	2491.711	393.9045	2885.616	0.100769	0	
9	9	142462	126032	0.085654	3284	0.15	4	0.098788	2491.711	393.9045	2885.616	0.10179	0	
10	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	1.026567	0	

Network

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	5896	19560	152.7698	31.66175	184.4315									
5	5896	23577	26.571	5.930025	32.50103									
6	5896	25532	239.4124	34.91333	274.3257									
7	5896	25596	73.28497	3.473618	76.75859									
8	5896	28439	55.42994	6.288477	61.71842									
9	5896	33668	36.96075	3.216468	40.17722									
10	5896	39108	77.42817	5.138063	82.56623									
11	5896	39140	70.98827	4.681057	75.66932									
12	5896	45640	86.48406	15.7084	102.1925									
13	5896	45712	59.30251	4.452708	63.75521									

Origin-Destination Matrix

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	6	100												
2	23	100												
3	64	100												
4														
5														
6														
7														
8														
9														
10														

User Defined Link IDs

Figure A-7 Example input tables in form of (.csv)

Network

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
0	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.249593	0
1	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.717664	0
2	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.095184	0
3	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.12022	0
4	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.069962	0
5	6	142446	142454	0.06596	3337	0.15	4	0.076074	2888.440965	401.908496	3290.349461	0.510468	0
6	7	126024	142446	0.017417	3337	0.15	4	0.020088	2888.440965	401.908496	3290.349461	0.019867	0
7	8	142454	142462	0.085637	3337	0.15	4	0.098768	2888.440965	401.908496	3290.349461	0.350355	0
8	9	142462	126032	0.085654	3284	0.15	4	0.098788	2888.440965	401.908496	3290.349461	0.158653	0
9	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	3.416619	0

1 (0 out of 2406 Selected)

Origin-Destination Matrix

OID	Pointer	Pointee	Car_Flow	Truck_Flow	Total_Flow
0	5896	5896	0	0	0
1	5896	6072	216.375015	124.732246	341.107261
2	5896	13777	844.064148	71.881973	915.946121
3	5896	19560	152.769791	31.661749	184.43154
4	5896	23577	26.571001	5.930025	32.501026
5	5896	25532	239.412354	34.91333	274.325684
6	5896	25596	73.284973	3.473618	76.758591
7	5896	28439	55.429943	6.288477	61.71842
8	5896	33668	36.960754	3.216468	40.177222
9	5896	39108	77.428169	5.138063	82.566232
10	5896	39140	70.988266	4.681057	75.669323

1 (0 out of 1936 Selected)

User Defined Link IDs

OID	Edge	CapRed
0	10	25
1	20	50
2	33	40
3	44	10
4	100	100

1 (0 out of 5 Selected)

Figure A-8 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and launch GSB Tool (see Figure A-9)

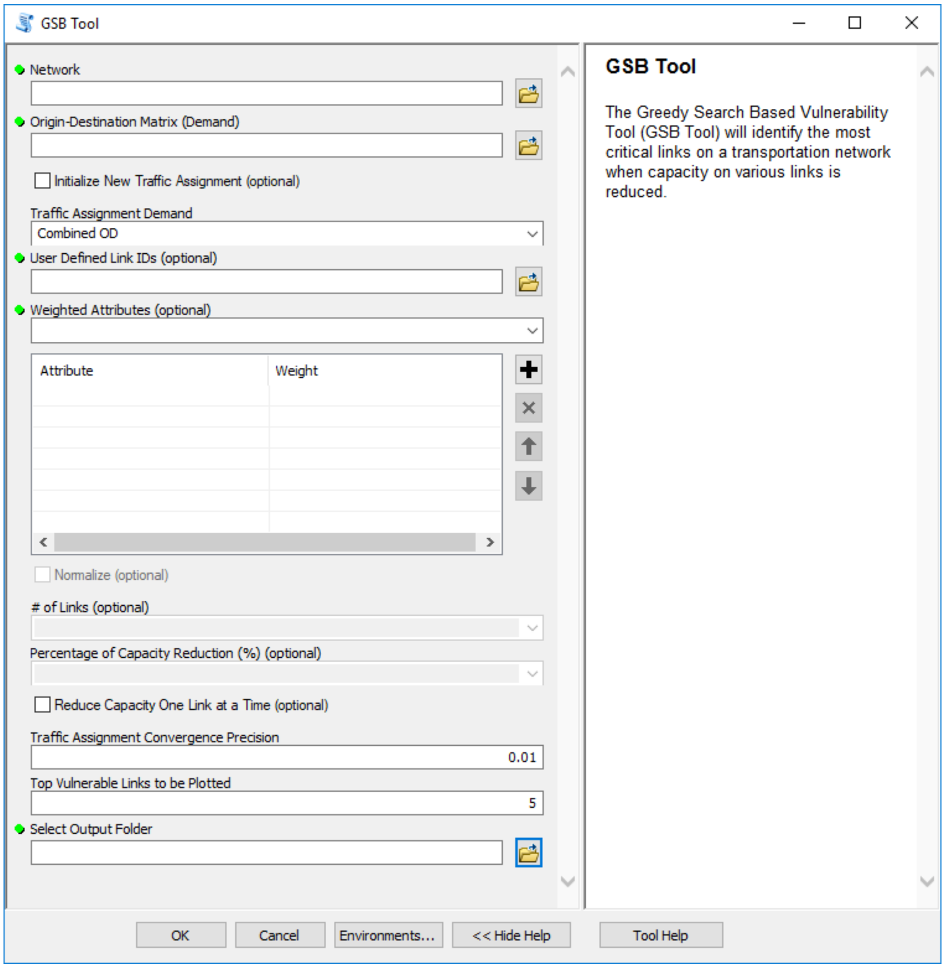


Figure A-9 GSB Tool

STEP 2

Input path to transportation network file in a form of (.csv) or (.dbf) into the tool first input parameter Network (see Figure A-10).

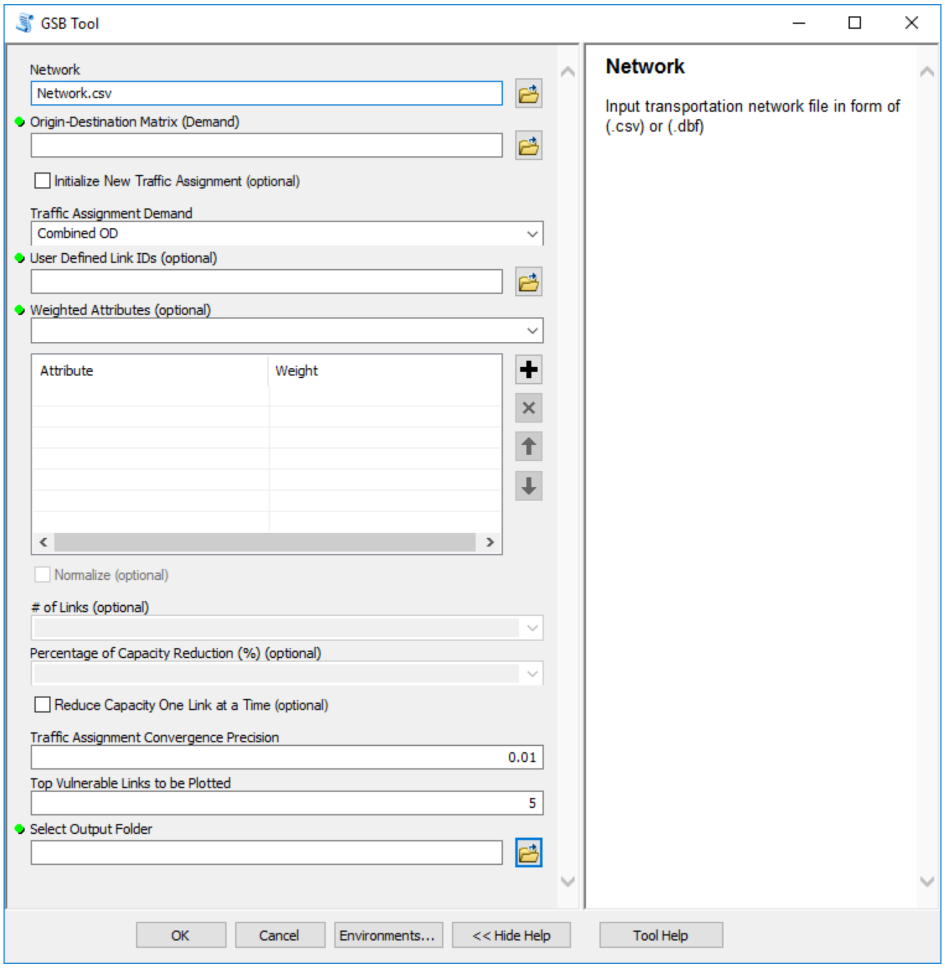


Figure A-10 Input Network

STEP 3

Input path to Origin-Destination Matrix (Demand) file in a form of (.csv) or (.dbf) into the tool second input parameter Origin-Destination Matrix (Demand) (see Figure A-11).

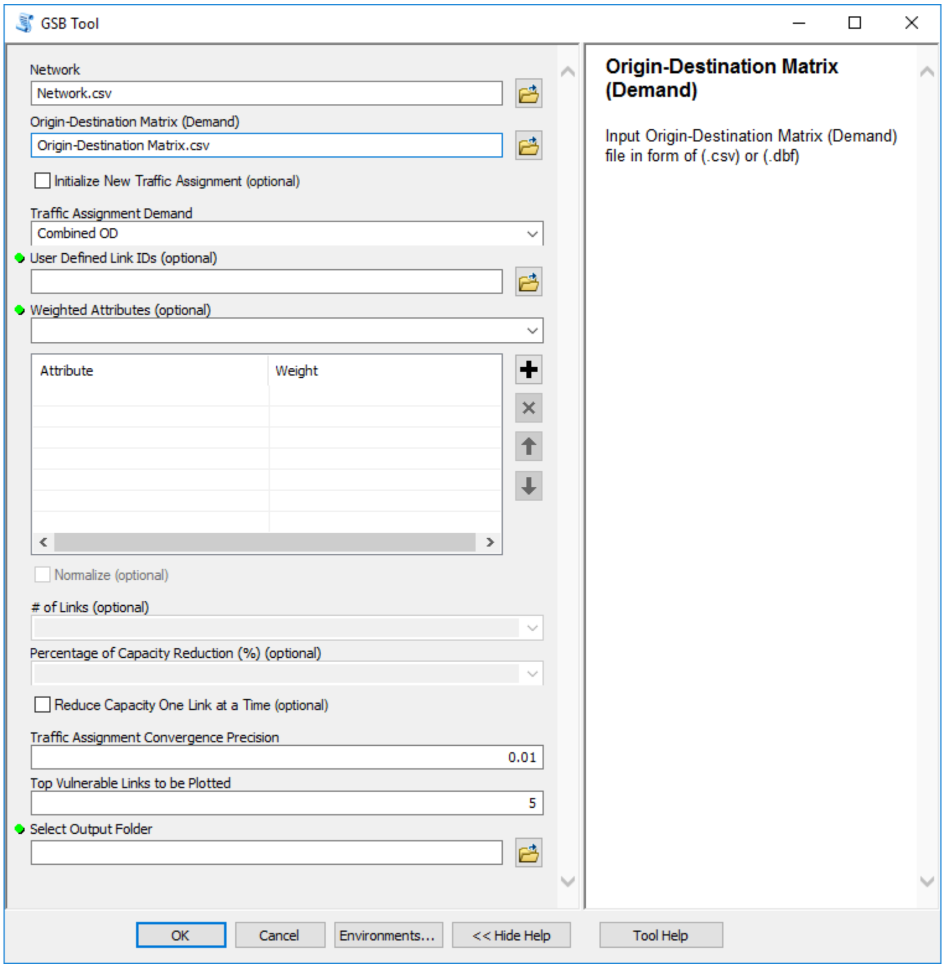


Figure A-11 Input Origin-Destination Matrix

STEP 4 (Optional)

Select option to Initialize New Traffic Assignment if user wishes use a new traffic assignment initialized by the Greedy Search Based Vulnerability Tool (see Figure A-12).

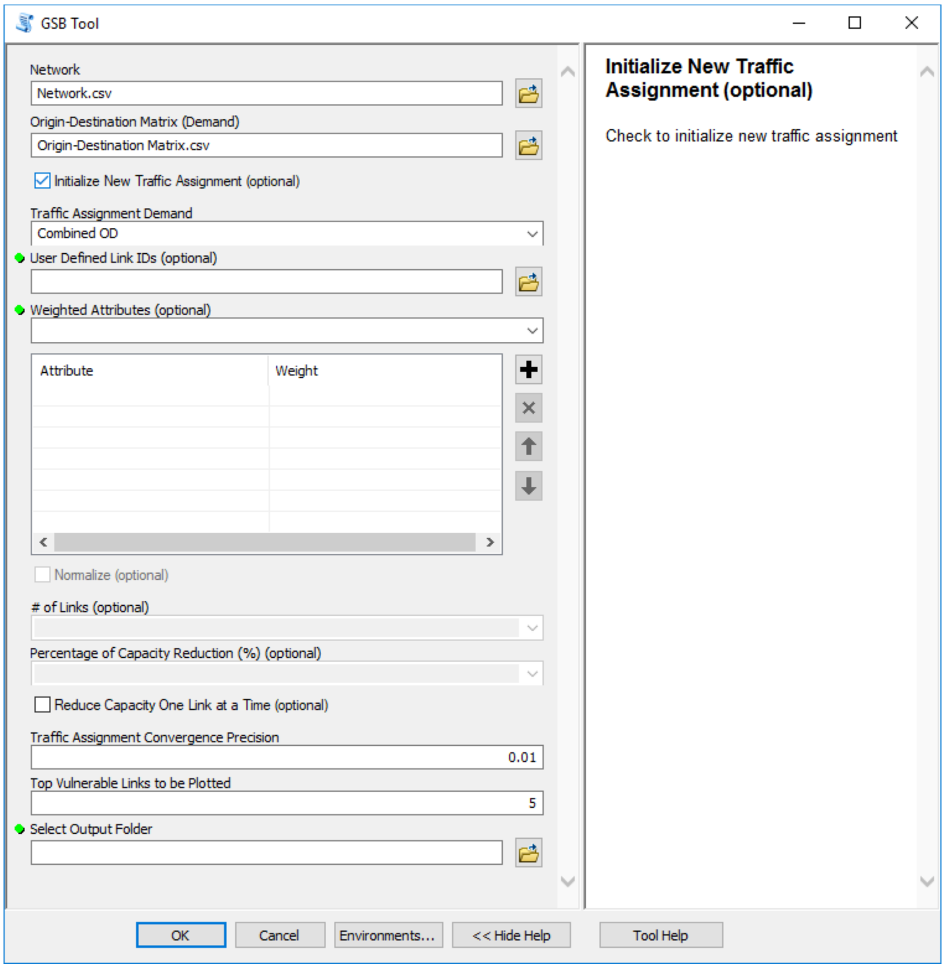


Figure A-12 Initialize New Traffic Assignment

STEP 5

Select the type of traffic assignment demand used for traffic assignment in input parameter Traffic Assignment Demand (see Figure A-13).

(A default selection of Combined OD will be set as input parameter.)

(Combined OD – First assigns traffic using passenger demand, then uses calculated passenger travel time as input to free flow travel time to assign traffic using truck demand, finally the calculated travel time using passenger demand is returned as output travel time.)

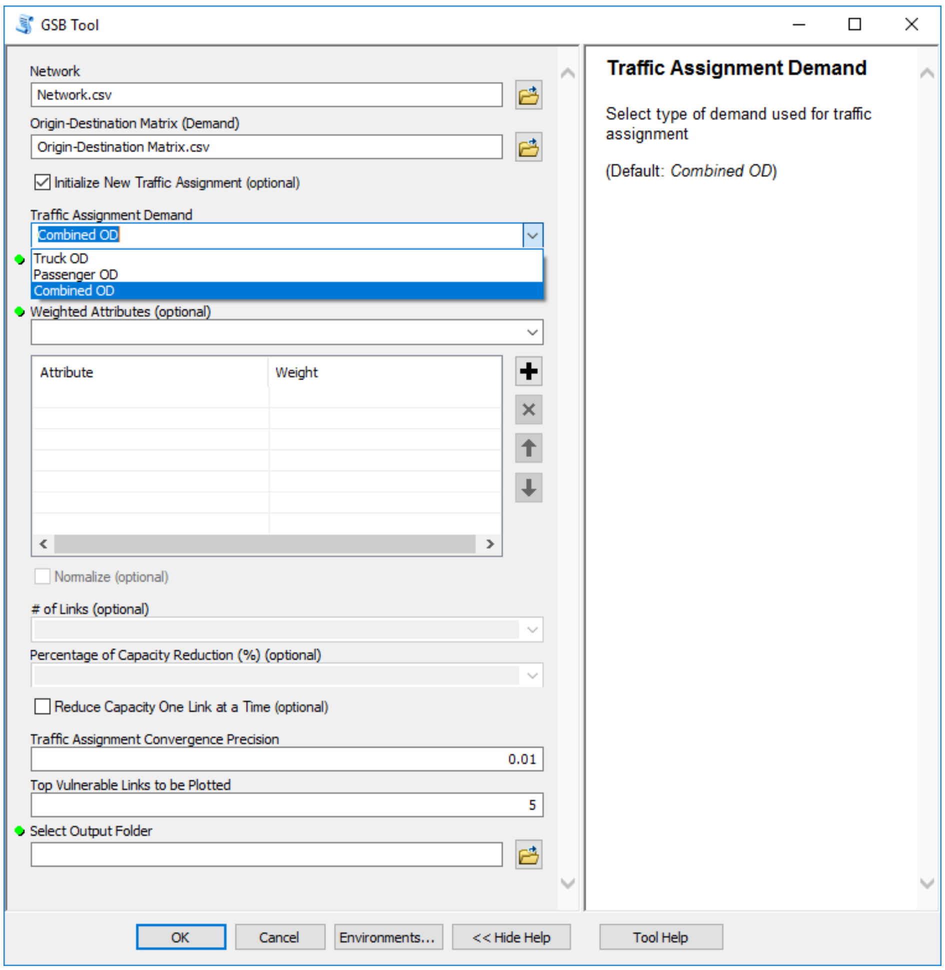


Figure A-13 Select Type of Demand Used for Traffic Assignment

STEP 6 (Option I)

Input path to User Defined Link IDs file in a form of (.csv) or (.dbf) into the input parameter User Defined Link IDs (see Figure A-14).

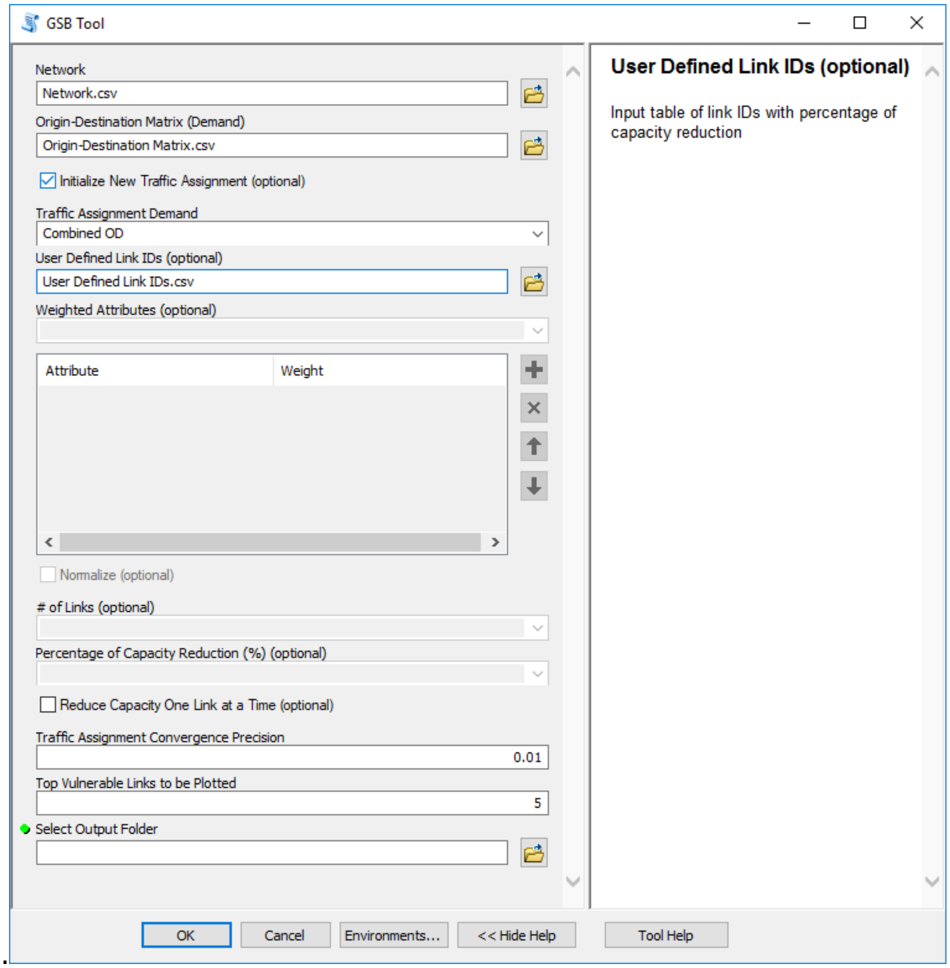


Figure A-14 Input User Defined Link IDs

STEP 6.1 (Option II)

Select attributes from input parameter Weighted Attributes drop down list (see Figure A-15).

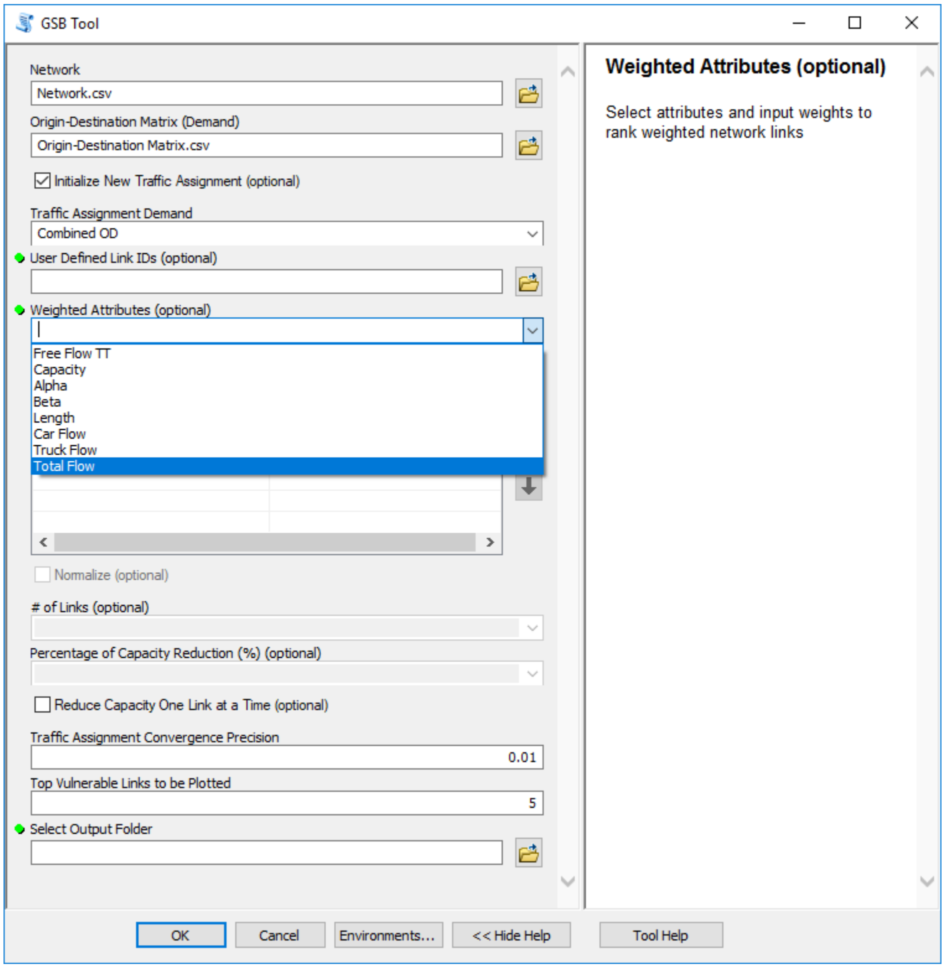


Figure A-15 Select Attributes

STEP 6.2 (Option II)

Input weights for selected field attributes in input parameter Weighted Attributes (see Figure A-16).

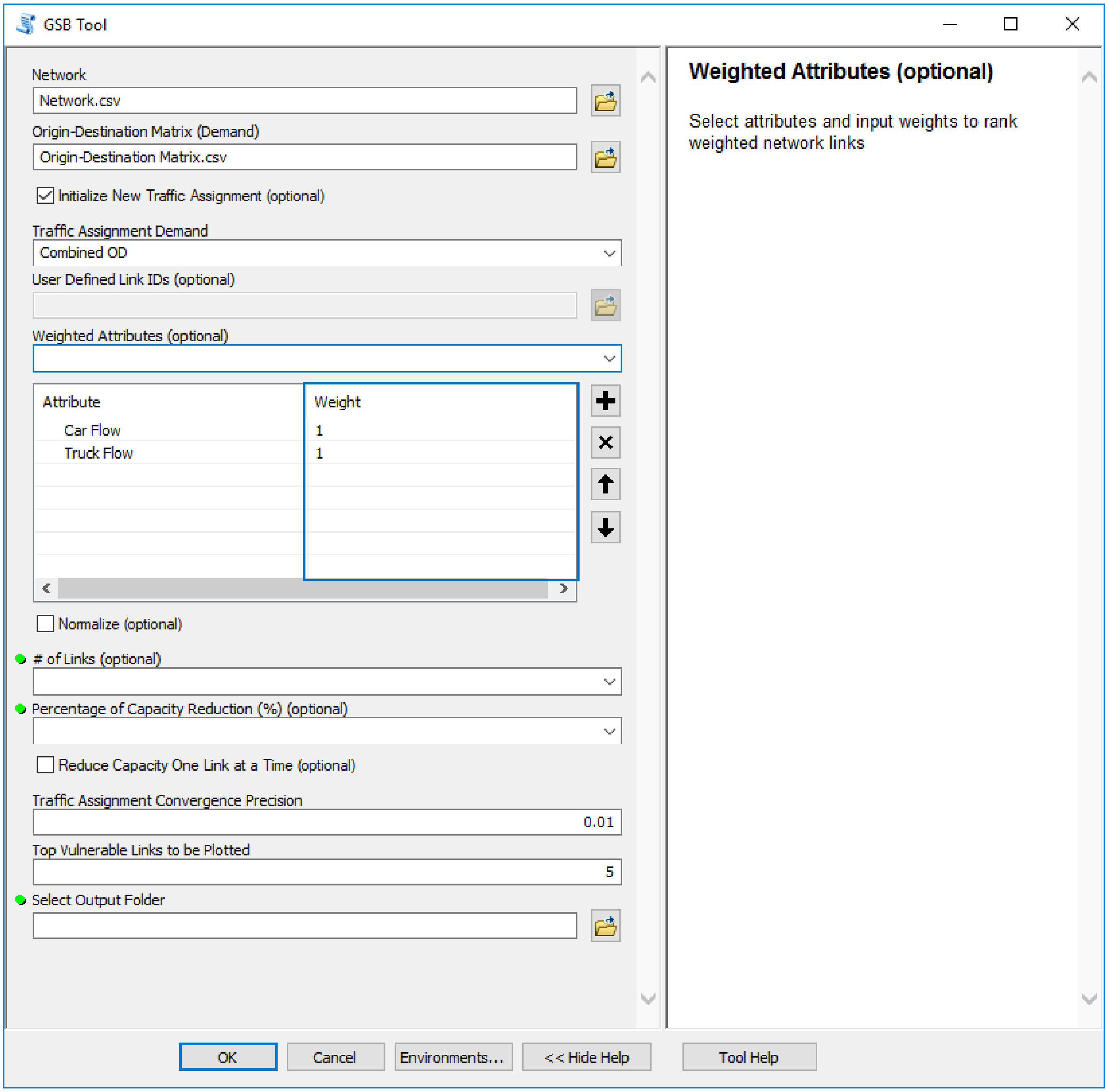


Figure A-16 Input Weights

STEP 6.3 (Option II) (Optional)

Select option Normalize to normalize user inputted weights (see Figure A-17).

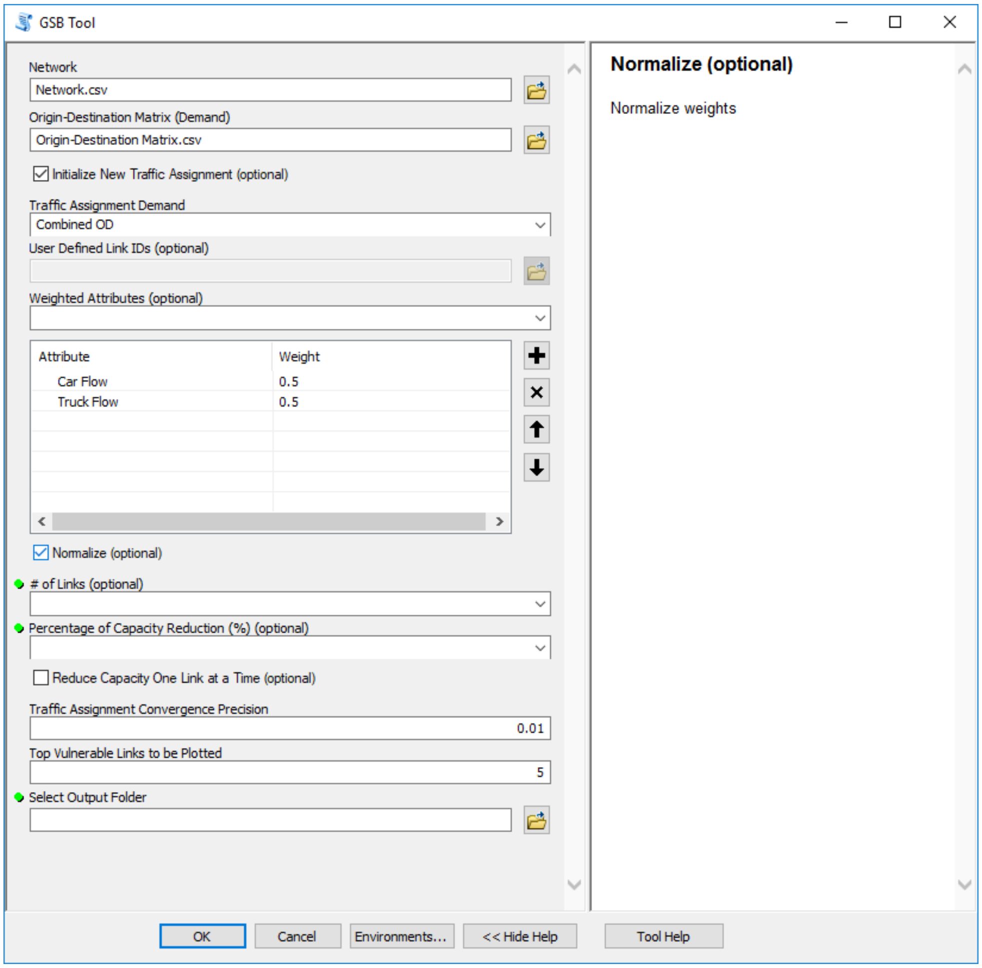


Figure A-17 Normalize Weights

STEP 7

Select the number of top ranked links used to reduce capacity in input parameter # of Links (see Figure A-18).

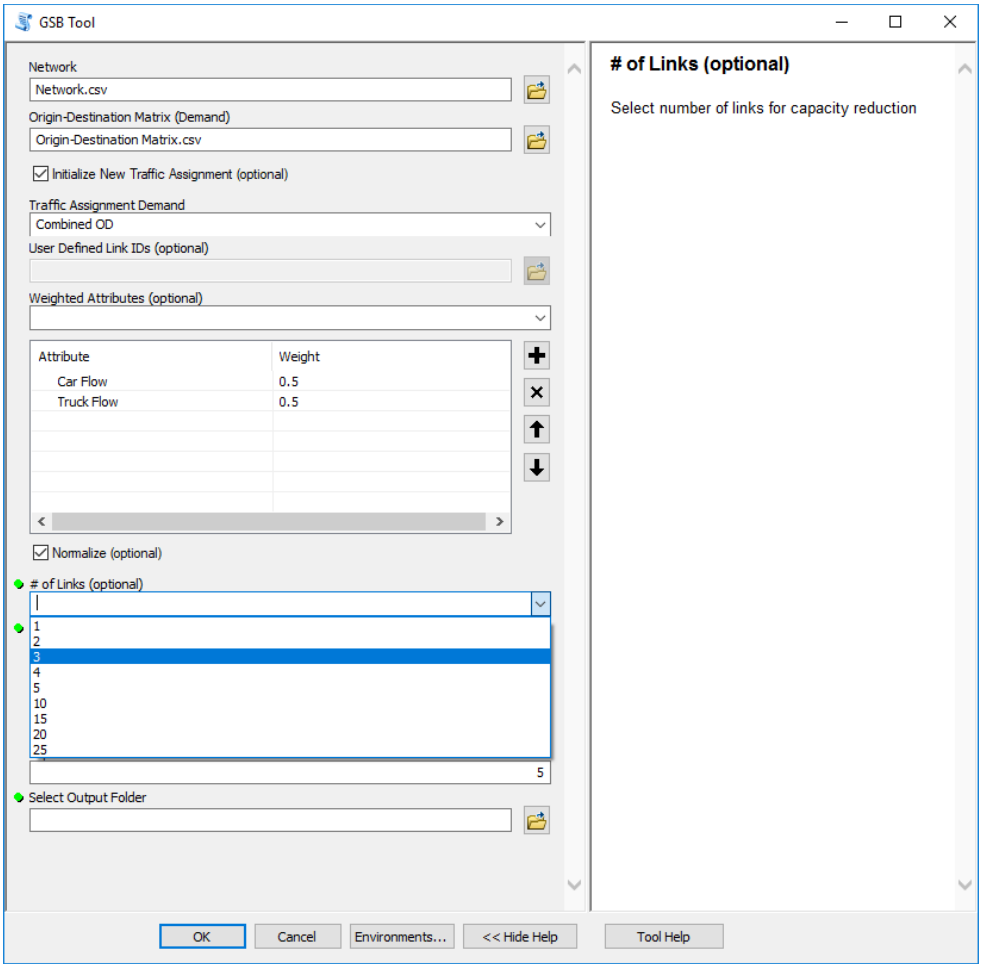


Figure A-18 Select # of Links

STEP 8 (Option II)

Select the percentage used to reduce capacity for the top ranked links in input parameter Percentage of Capacity Reduction (%) (see Figure A-19).

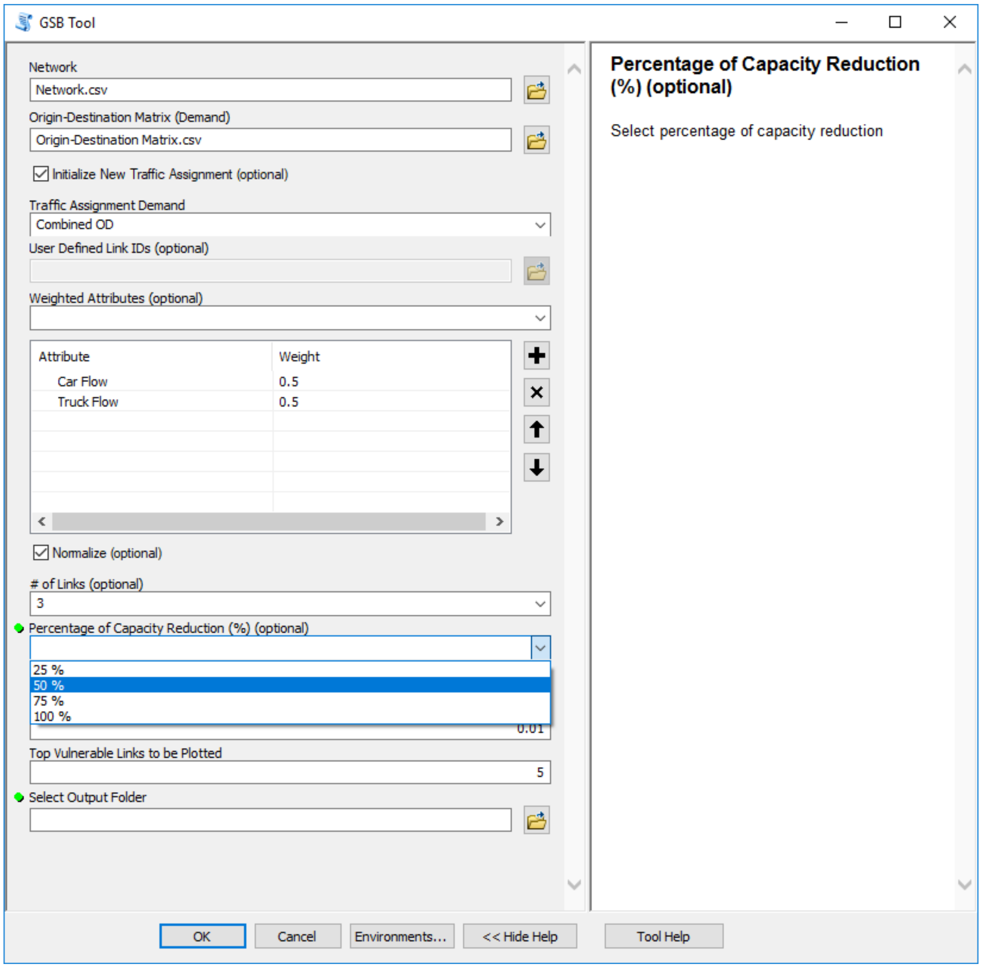


Figure A-19 Select the Percentage of Capacity Reduction (%)

STEP 9

Select option Reduce Capacity One Link at a Time to process files by reducing capacity for a single link (see Figure A-20)

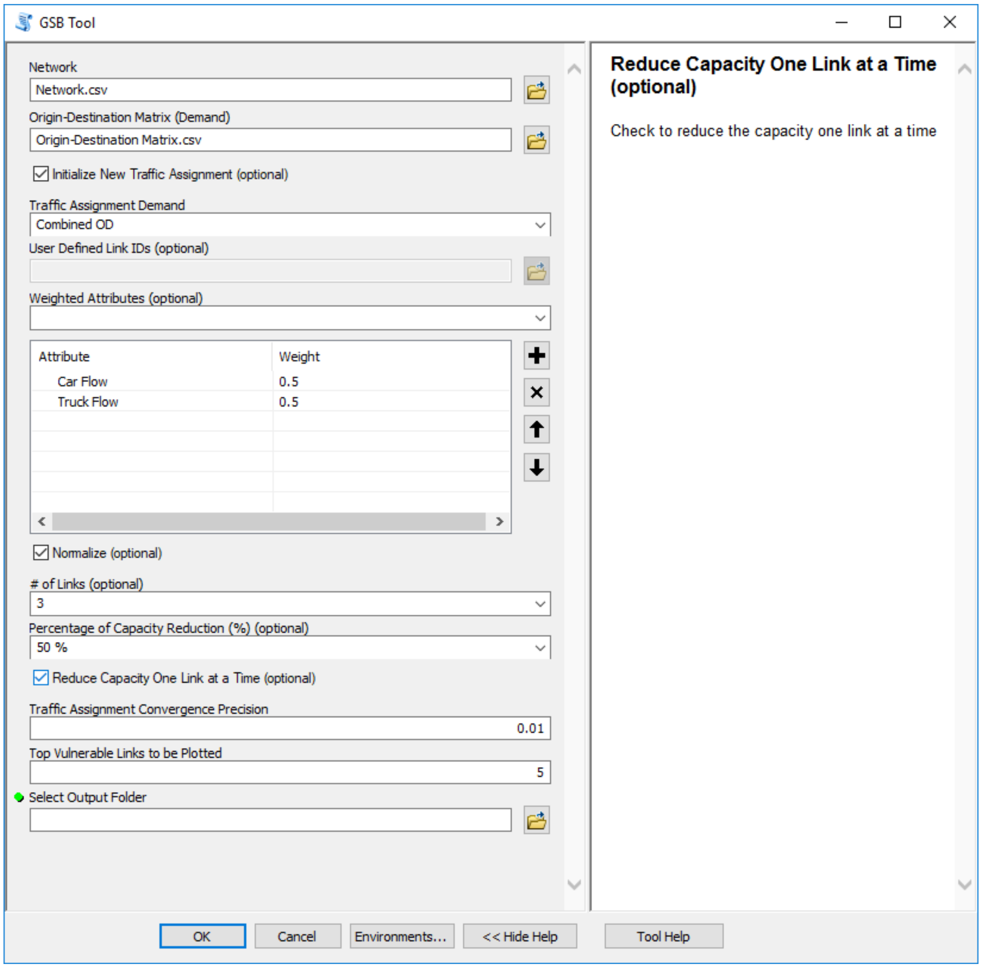


Figure A-20 Select Reduce Capacity One Link at a Time

STEP 10

Input Traffic Assignment Convergence Precision (see Figure A-21).

(A default value of 0.01 will be set as input parameter.)

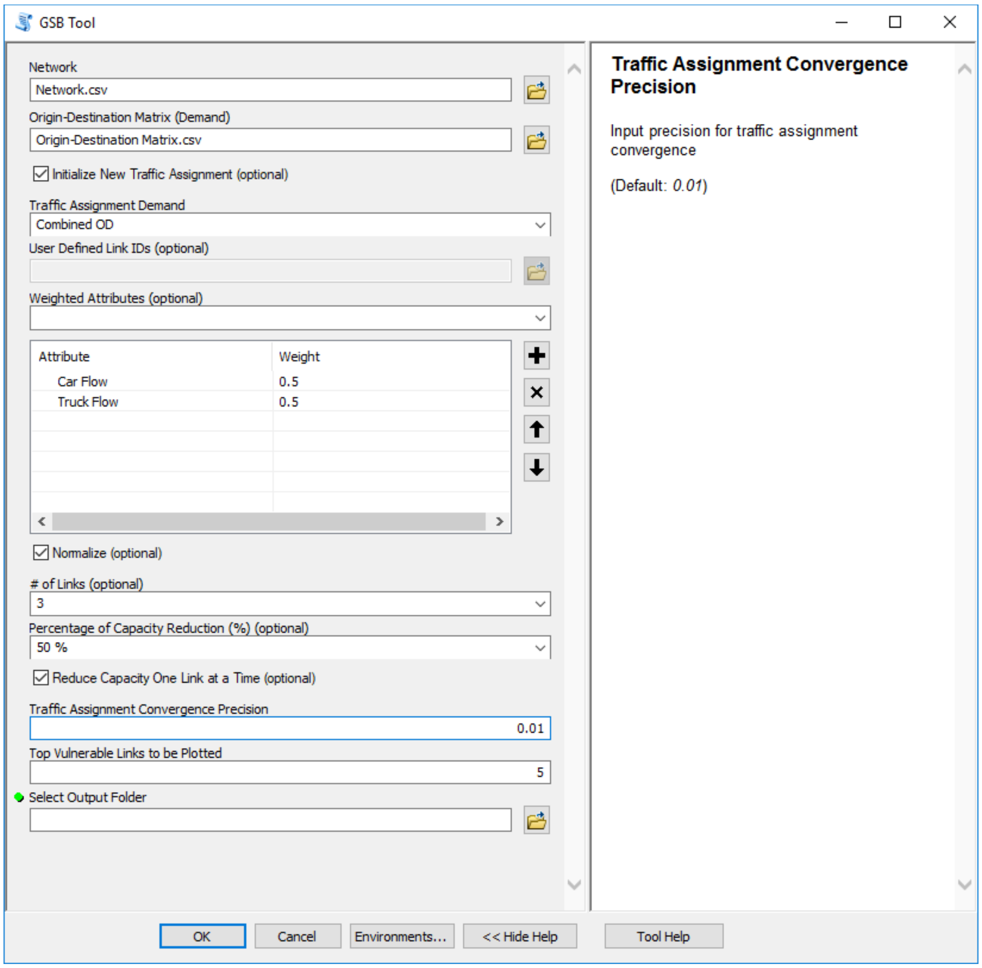


Figure A-21 Input Traffic Assignment Convergence Precision

STEP 11

Input the number of top vulnerable links (links that are most sensitive to changes in network) used to plot the difference in vehicle hours traveled (VHT) and vehicle miles traveled (VMT) in input parameter Top Vulnerable Links to be Plotted (see Figure A-22).

(A default value of 5 will be set as input parameter.)

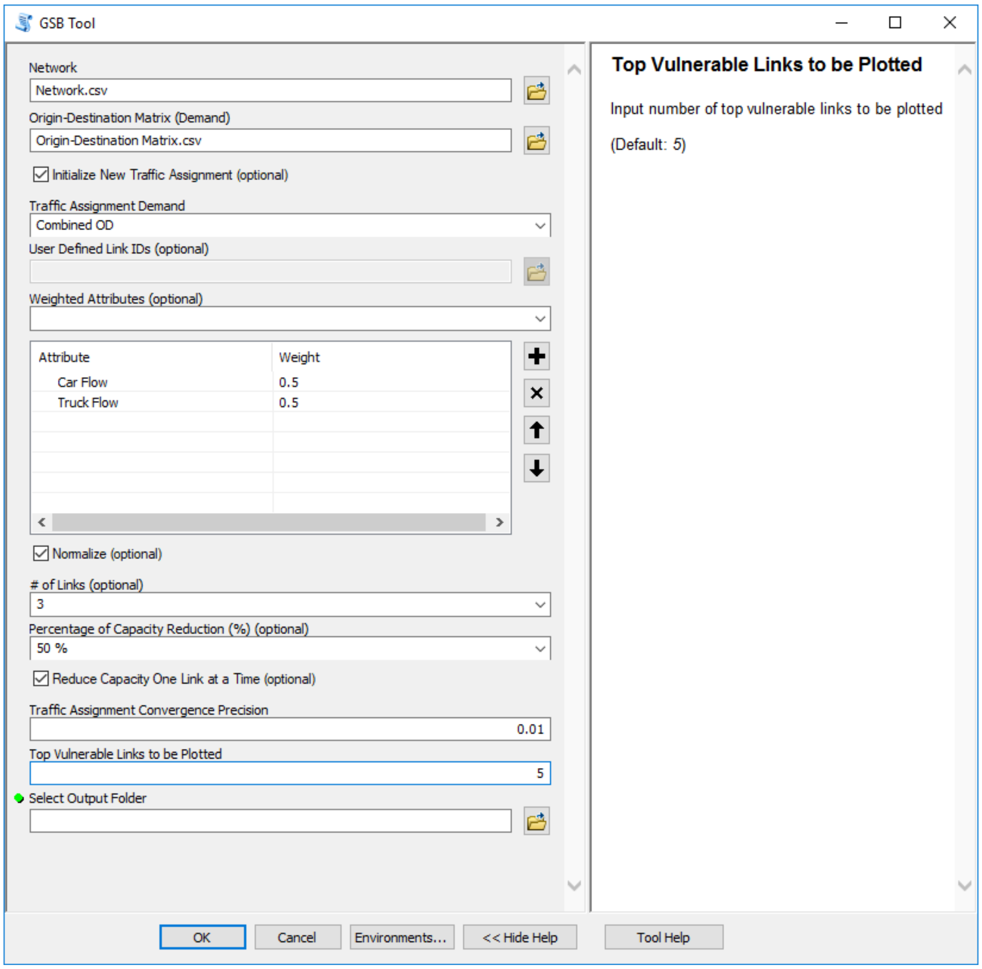


Figure A-22 Input Top Vulnerable Links to be Plotted

STEP 12

In toolbox Select Output Folder parameter input output folder path where processed files will be exported after toolbox analysis (see Figure A-23).

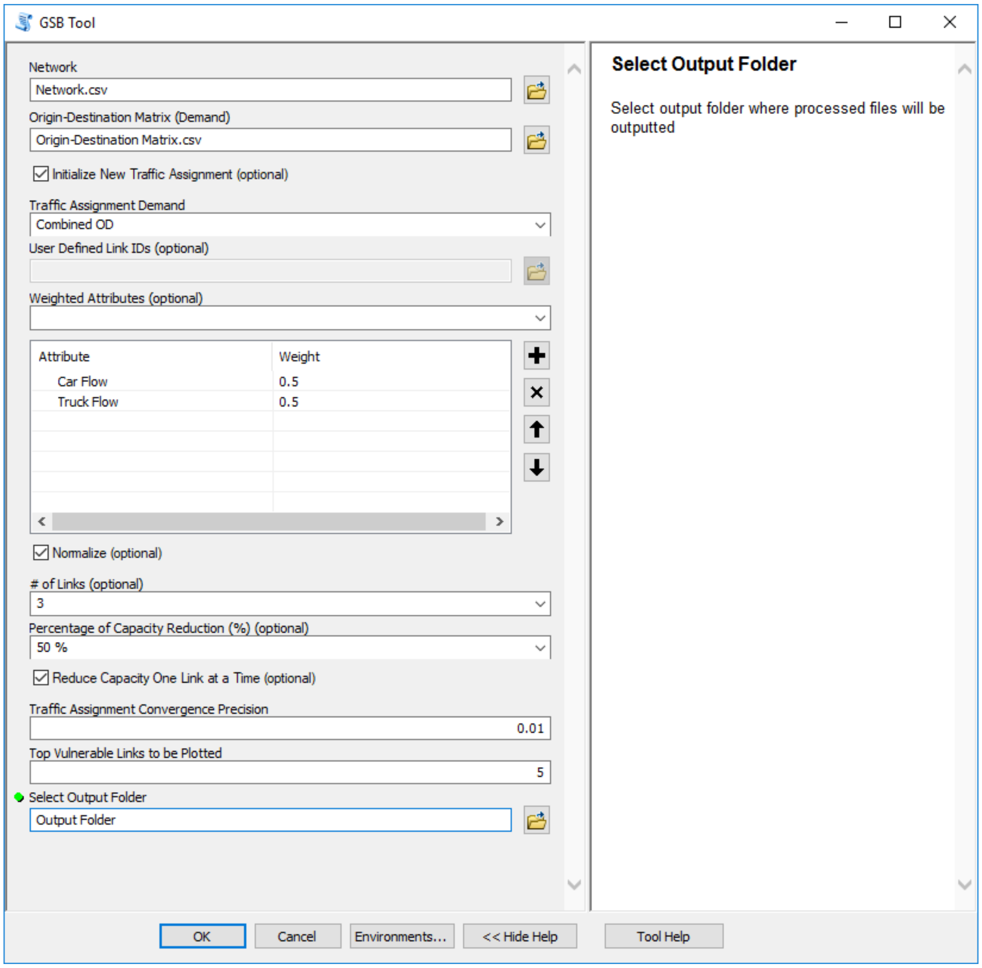


Figure A-23 Output Folder Selection

STEP 13

Once all required parameters are inputted, press OK to execute the application. The ArcGIS application invokes a task completion window, which reports status of each task (see Figure A-24). In addition, graph with the top vulnerable link differences in VMT and VHT will appear on a screen (see Figure A-25) in pdf format and the processed table (see Figure A-26) in (.dbf) format will be imported to ArcMap Display.

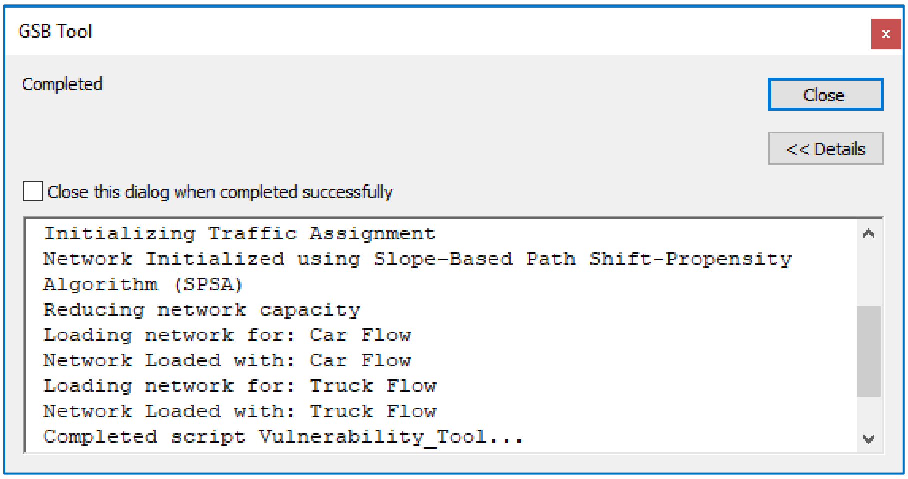


Figure A-24 Application Performance Task Window

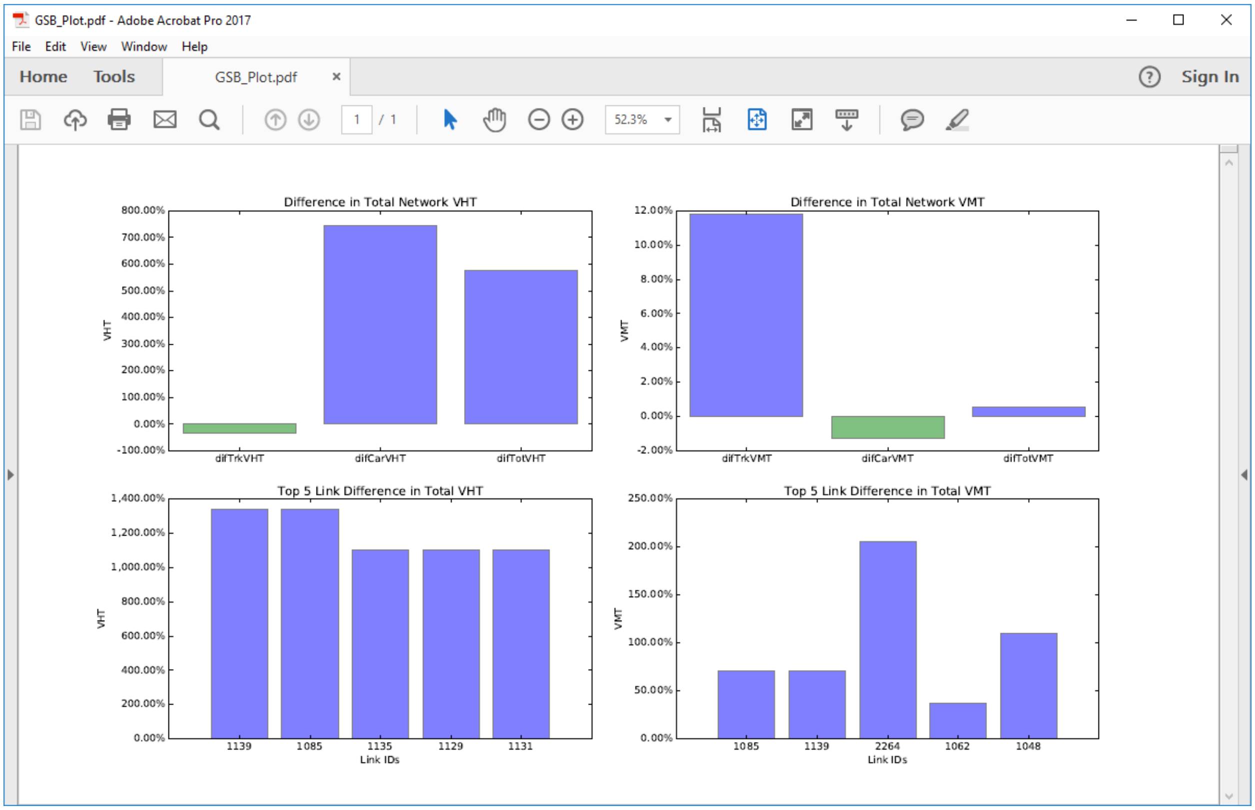


Figure A-25 GSB Plot

GSB_Output

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
848	849	45800	45856	0.237056	8169	0.15	4	0.238636	13321.765797	3835.641072	17157.406869	0.488542	0
1770	1771	23401	19784	0.139381	4024	0.15	4	0.14031	11607.718267	3559.897741	15167.616008	1.586987	0
2045	2046	45792	45784	0.197326	8169	0.15	4	0.198642	12948.884339	3303.676863	16252.561202	0.384192	0
0	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0
1	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0
2	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0
3	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0
4	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0
5	6	142446	142454	0.06596	3337	0.15	4	0.076074	2409.924037	401.908496	2811.832533	0.068651	0
6	7	126024	142446	0.017417	3337	0.15	4	0.020088	2409.924037	401.908496	2811.832533	0.018128	0
7	8	142454	142462	0.085637	3337	0.15	4	0.098768	2409.924037	401.908496	2811.832533	0.089131	0

0 (0 out of 2406 Selected)

Weights	RedCap	Selected	newTrkFlow	newCarFlow	newTT	difTrkFlow	newTrkVHT	newTrkVMT	difTrkVHT	difTrkVMT
0.001766	0	1	0	0	0	0	0	0	0	0
0.001589	0	1	0	0	0	0	0	0	0	0
0.001618	0	1	0	0	0	0	0	0	0	0
0	3337	0	0	0	0.041364	0	0	0	0	0
0	3337	0	0	0	0.027632	0	0	0	0	0
0	3337	0	0	0	0.086236	0	0	0	0	0
0	3337	0	0	0	0.077587	0	0	0	0	0
0	3337	0	0	0	0.010867	0	0	0	0	0
0.000252	3337	0	401.908496	2542.412384	0.069294	0	27.849847	30.574787	0.258427	0
0.000252	3337	0	401.908496	2542.412384	0.018297	0	7.35372	8.073538	0.067923	0
0.000252	3337	0	401.908496	2542.412384	0.089965	0	36.157698	39.695698	0.335192	0

difCarFlow	newCarVHT	newCarVMT	difCarVHT	difCarVMT	difTT	newTotFlow	newTotVHT	newTotVMT	difTotVHT	difTotVMT
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
132.488347	176.173924	193.41148	10.730229	10.078919	0.000643	2944.32088	204.023771	223.986267	10.988656	10.078919
132.488347	46.518519	51.07198	2.831416	2.661426	0.000169	2944.32088	53.872239	59.145518	2.899339	2.661426
132.488347	228.72813	251.108986	13.929191	13.085609	0.000834	2944.32088	264.885828	290.804684	14.264383	13.085609

Figure A-26 Network Link Vulnerability Ranking Tool Output

STEP 14

User then can add a network in format of shapefile (see Figure A-27) and join the Greedy Search Based Vulnerability Tool output using field attribute Edge (*Note: User will have add new join field and convert the Edge data attribute field to short integer data type*) and visualize the tool outputs (see Figure A-28).

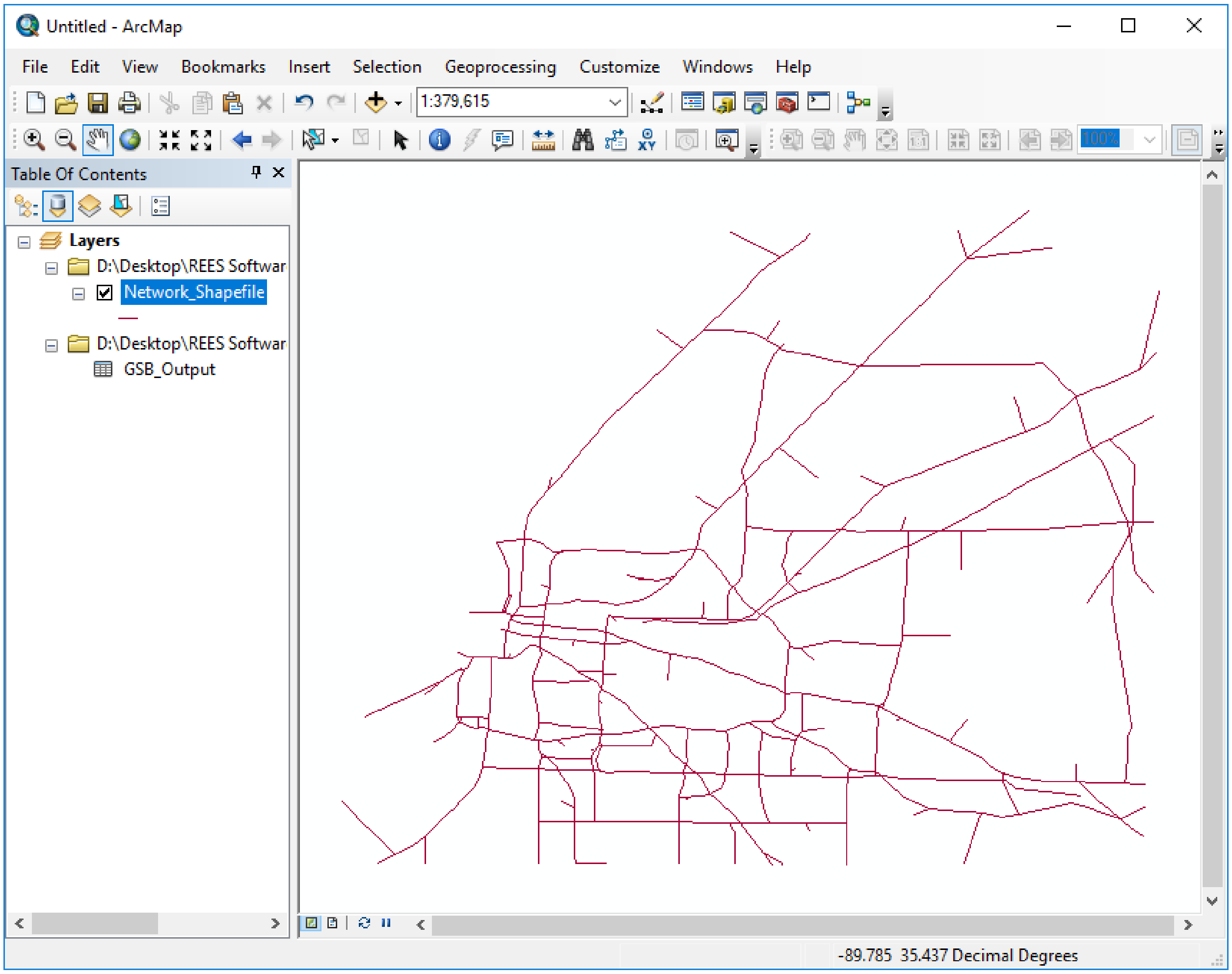
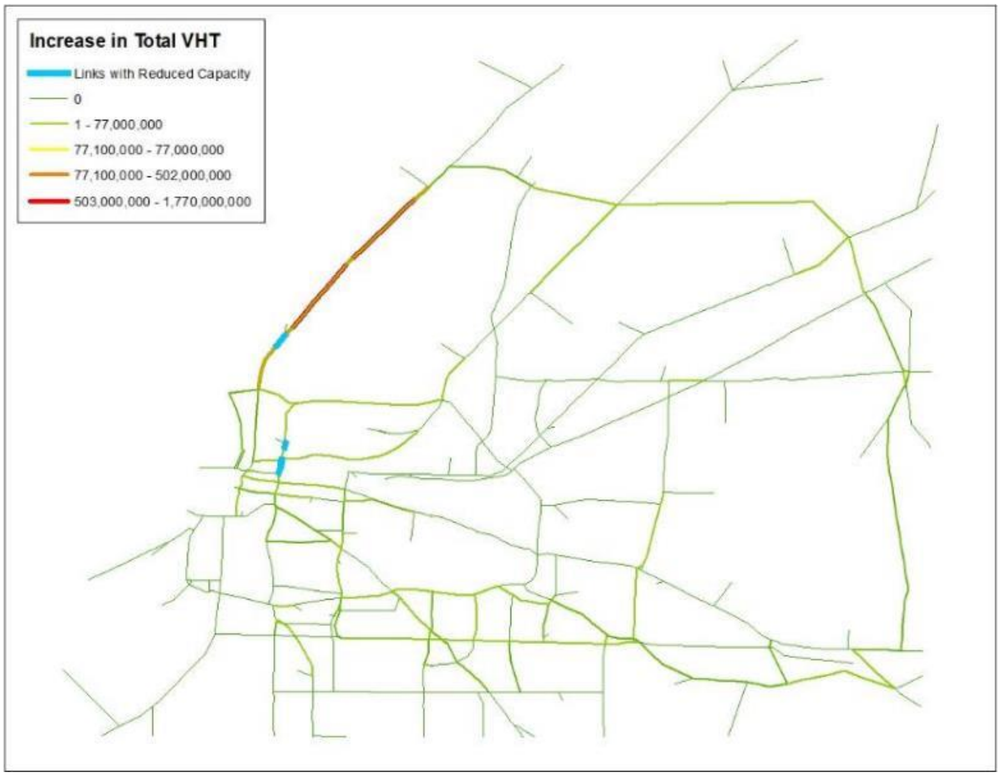


Figure A-27 Add Network in a Form of Shapefile



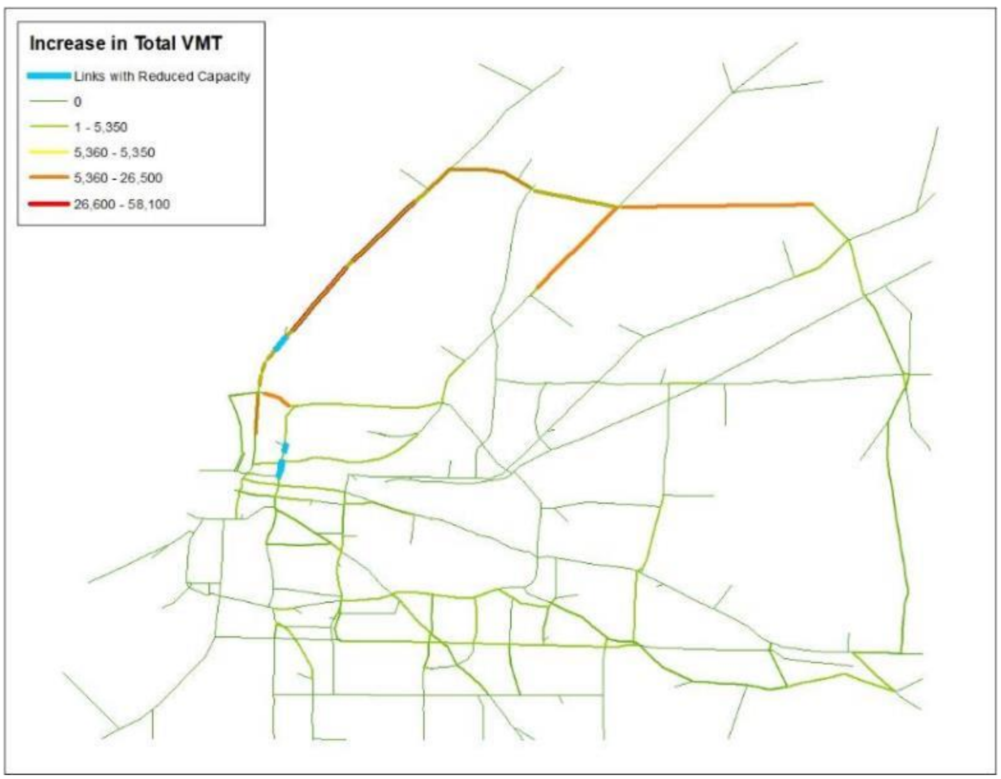


Figure A-28 Visualize the GSB Tool Output

Table A-9 GSB Tool Output Attribute Field Dictionary

Field Attribute	Description
Weights	Weighted attribute ratio
newTrkFlow	New truck flow
newCarFlow	New car flow
newTT	New travel time
difTrkFlow	Difference in truck flow
newTrkVHT	New truck vehicle hours traveled (VHT)
newTrkVMT	New truck vehicle miles traveled (VMT)
difTrkVHT	Difference in truck vehicle hours traveled (VHT)
difTrkVMT	Difference in truck vehicle miles traveled (VMT)
difCarFlow	Difference in car flow
newCarVHT	New car vehicle hours traveled (VHT)
newCarVMT	New car vehicle miles traveled (VMT)
difCarVHT	Difference in car vehicle hours traveled (VHT)
difCarVMT	Difference in car vehicle miles traveled (VMT)
difTT	Difference in travel time
newTotFlow	New total flow
newTotVHT	New total vehicle hours traveled (VHT)
newTotVMT	New total vehicle miles traveled (VMT)
difTotVHT	Difference in total vehicle hours traveled (VHT)
difTotVMT	Difference in total vehicle miles traveled (VMT)

THE RANDOM SEARCH HEURISTIC BASED VULNERABILITY TOOL (RSH TOOL)

Description

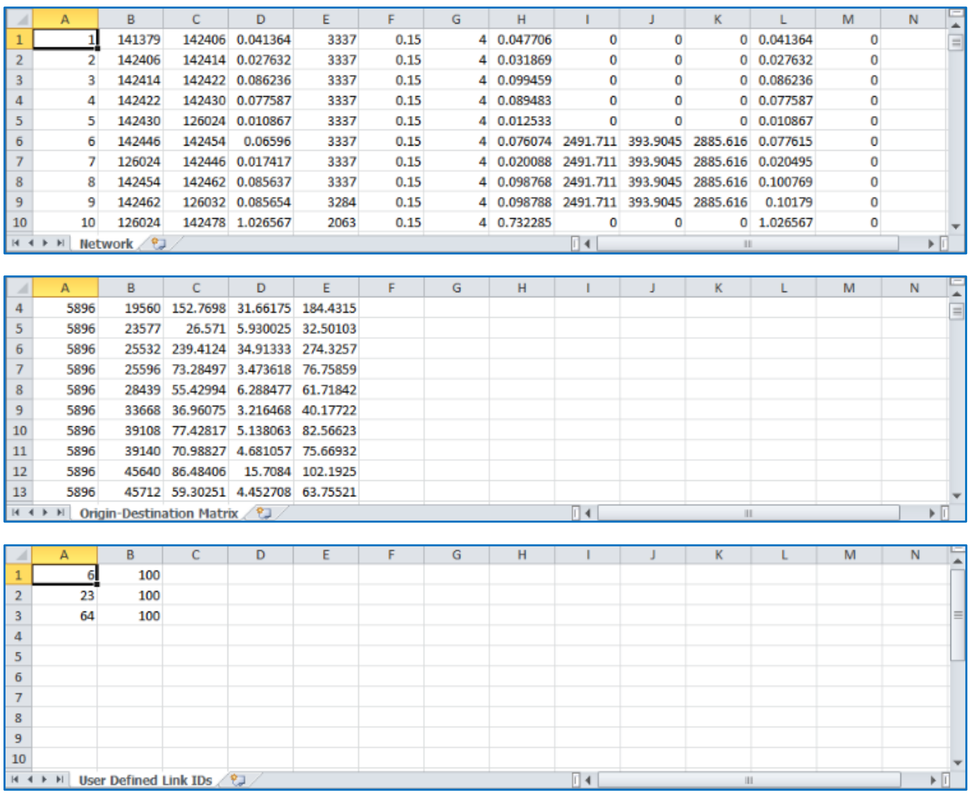
The Random Search Heuristic Based Vulnerability Tool (RSH Tool) has two options to identify the most critical links on a transportation network using Combined OD* traffic assignment demand. The first option involves of user providing a table in a form of (.csv) or (.dbf) of Edge IDs and their corresponding percentage of capacity reduction, following input the tool will randomly select number (selected by user) of user provided links, reduce the capacity and run shortest-path algorithm. Next, tool will rank the critical link sets by the total network cost increase and select the top (selected by user) critical link sets, after that for every instance of the top critical link set tool will reduce capacity and run a traffic assignment. Finally, networks where the instance of the critical link set provided the highest increase in total vehicle hours travelled (VHT) and total vehicle miles traveled (VMT) are outputted. The second option involves user selecting field attributes and inputting weights, following input the tool will rank links by first the product of weights and total volume to capacity ratio (v/c) then by total volume to capacity ratio (v/c) and finally by weighted attributes and will select the top weighted links by a percentage (selected by user), reduce the capacity by percentage (selected by user) and run shortest-path algorithm Next, tool will rank the critical link sets by the total network cost increase and select the top (selected by user) critical link sets, after that for every instance of the top critical link set tool will reduce the capacity and run a traffic assignment. Finally, networks where the instance of the critical link set provided the highest increase in total vehicle hours travelled (VHT) and total vehicle miles traveled (VMT) and table containing the top critical link sets with calculated total network costs are outputted.

**(Combined OD – First assigns traffic using passenger demand, then uses calculated passenger travel time as input to free flow travel time to assign traffic using truck demand, finally the calculated travel time using passenger demand is returned as output travel time.)*

Example Input Files

Following tables were used in executing RSH Tool example in format of (.csv) (see Figure A-29) and (.dbf) (see Figure A-30).

- **Network.csv** – Transportation network with the following order of field attributes: Link ID for one direction, From Node, To Node, Free Flow Travel Time, Capacity, Alpha, Beta, Length, Car Flow, Truck Flow, Total Flow, Travel Time, and Connector (0 - No, 1 - yes).
- **Origin-Destination Matrix.csv** – Origin-Destination Matrix with the following order of field attributes: From Node, To Node, Car Demand, Truck Demand, and Total Demand.
- **User Defined Link IDs.csv** – User defined Link ID table with the following order of field attributes: Link ID for one direction and percentage of capacity reduction.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0	
2	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0	
3	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0	
4	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0	
5	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0	
6	6	142446	142454	0.06596	3337	0.15	4	0.076074	2491.711	393.9045	2885.616	0.077615	0	
7	7	126024	142446	0.017417	3337	0.15	4	0.020088	2491.711	393.9045	2885.616	0.020495	0	
8	8	142454	142462	0.085637	3337	0.15	4	0.098768	2491.711	393.9045	2885.616	0.100769	0	
9	9	142462	126032	0.085654	3284	0.15	4	0.098788	2491.711	393.9045	2885.616	0.10179	0	
10	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	1.026567	0	

Network

	A	B	C	D	E
4	5896	19560	152.7698	31.66175	184.4315
5	5896	23577	26.571	5.930025	32.50103
6	5896	25532	239.4124	34.91333	274.3257
7	5896	25596	73.28497	3.473618	76.75859
8	5896	28439	55.42994	6.288477	61.71842
9	5896	33668	36.96075	3.216468	40.17722
10	5896	39108	77.42817	5.138063	82.56623
11	5896	39140	70.98827	4.681057	75.66932
12	5896	45640	86.48406	15.7084	102.1925
13	5896	45712	59.30251	4.452708	63.75521

Origin-Destination Matrix

	A	B
1	6	100
2	23	100
3	64	100
4		
5		
6		
7		
8		
9		
10		

User Defined Link IDs

Figure A-29 Example input tables in form of (.csv)

Network

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
0	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.249593	0
1	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.717664	0
2	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.095184	0
3	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.12022	0
4	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.069962	0
5	6	142446	142454	0.06596	3337	0.15	4	0.076074	2888.440965	401.908496	3290.349461	0.510468	0
6	7	126024	142446	0.017417	3337	0.15	4	0.020088	2888.440965	401.908496	3290.349461	0.019867	0
7	8	142454	142462	0.085637	3337	0.15	4	0.098768	2888.440965	401.908496	3290.349461	0.350355	0
8	9	142462	126032	0.085654	3284	0.15	4	0.098788	2888.440965	401.908496	3290.349461	0.158653	0
9	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	3.416619	0

1 (0 out of 2406 Selected)

Origin-Destination Matrix

OID	Pointer	Pointee	Car_Flow	Truck_Flow	Total_Flow
0	5896	5896	0	0	0
1	5896	6072	216.375015	124.732246	341.107261
2	5896	13777	844.064148	71.881973	915.946121
3	5896	19560	152.769791	31.661749	184.43154
4	5896	23577	26.571001	5.930025	32.501026
5	5896	25532	239.412354	34.91333	274.325684
6	5896	25596	73.284973	3.473618	76.758591
7	5896	28439	55.429943	6.288477	61.71842
8	5896	33668	36.960754	3.216468	40.177222
9	5896	39108	77.428169	5.138063	82.566232
10	5896	39140	70.988266	4.681057	75.669323

1 (0 out of 1936 Selected)

User Defined Link IDs

OID	Edge	CapRed
0	10	25
1	20	50
2	33	40
3	44	10
4	100	100

1 (0 out of 5 Selected)

Figure A-30 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and launch RSH Tool (see Figure A-31)

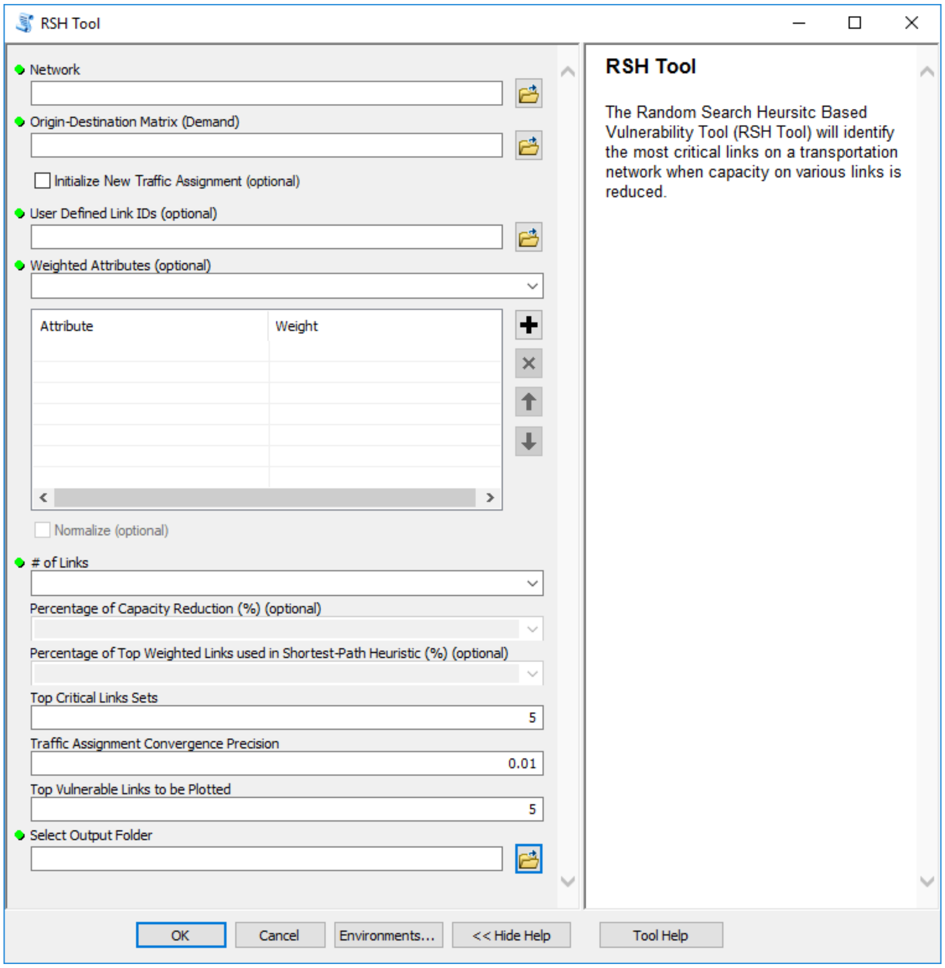


Figure A-31 RSH Tool

STEP 2

Input path to transportation network file in a form of (.csv) or (.dbf) into the tool first input parameter Network (see Figure A-32).

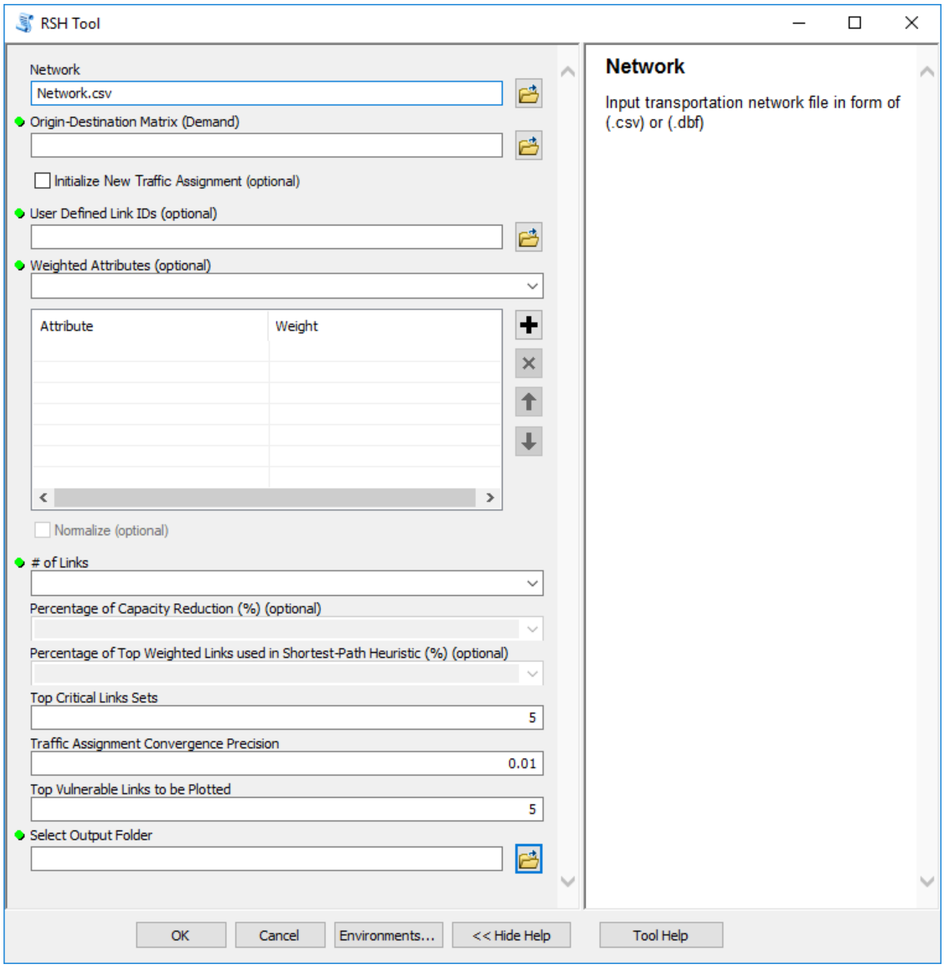


Figure A-32 Input Network

STEP 3

Input path to Origin-Destination Matrix (Demand) file in a form of (.csv) or (.dbf) into the tool second input parameter Origin-Destination Matrix (Demand) (see Figure A-33).

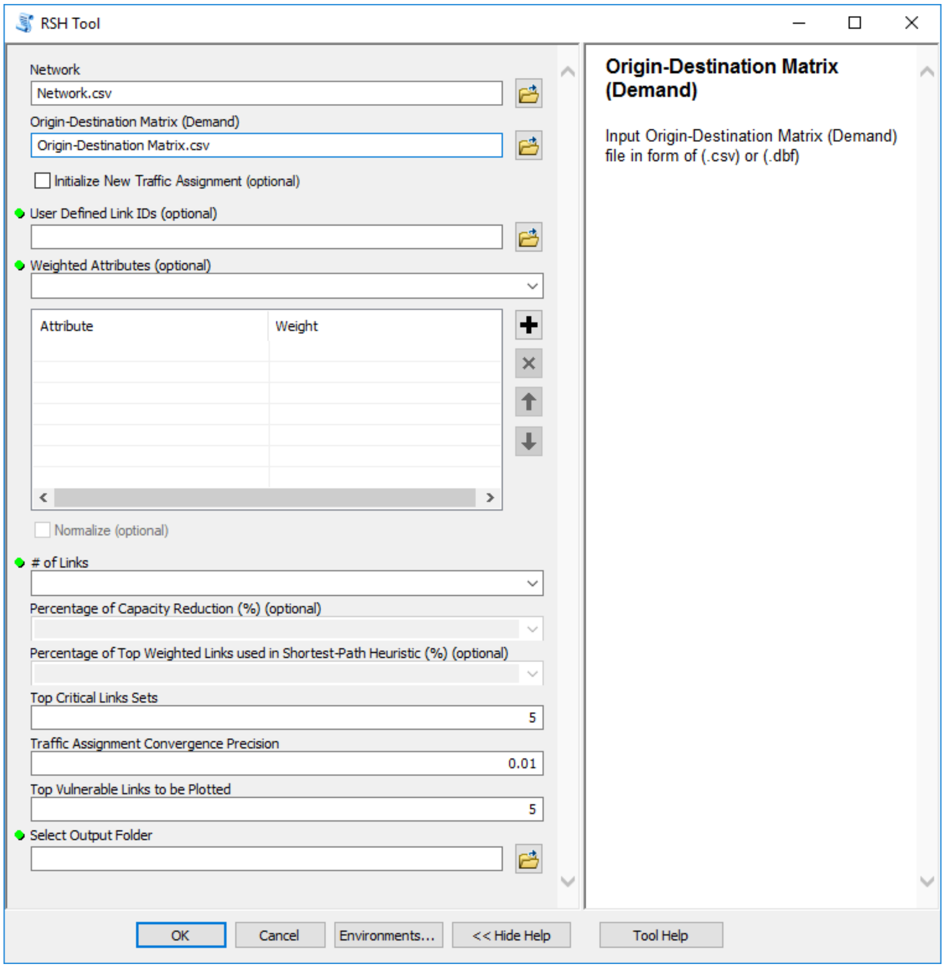


Figure A-33 Input Origin-Destination Matrix

STEP 4 (Optional)

Select option to Initialize New Traffic Assignment if user wishes to use a new traffic assignment initialized by Random Search Heuristic Based Vulnerability Tool (see Figure A-34).

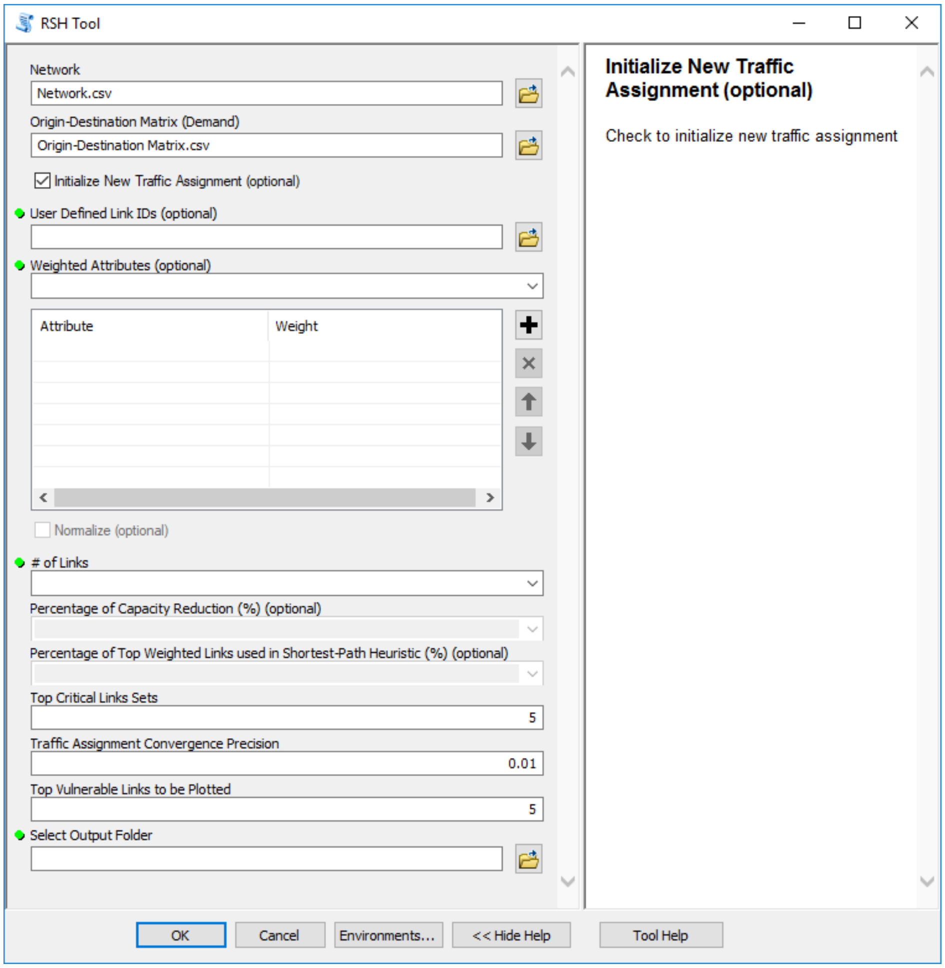


Figure A-34 Initialize New Traffic Assignment

STEP 5 (Option I)

Input path to User Defined Link IDs file in a form of (.csv) or (.dbf) into the input parameter User Defined Link IDs (see Figure A-35).

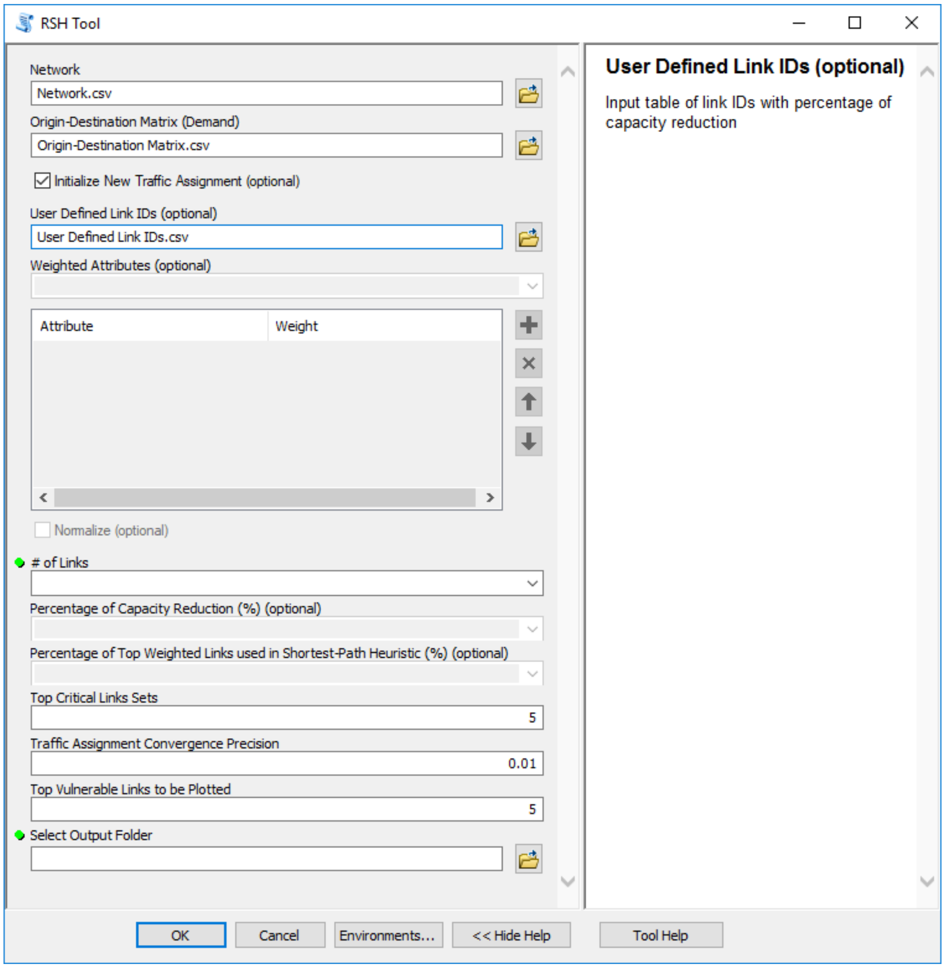


Figure A-35 Input User Defined Link IDs

STEP 5.1 (Option II)

Select attributes from input parameter Weighted Attributes drop down list (see Figure A-36).

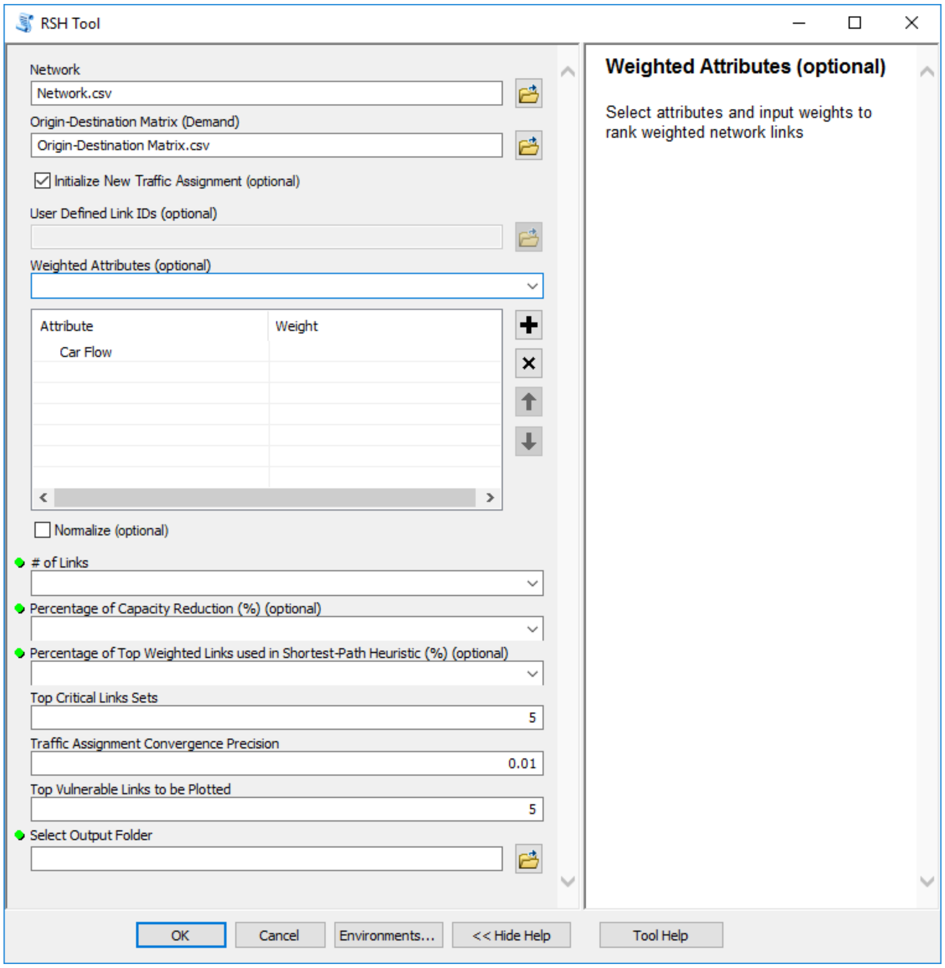


Figure A-36 Select Attributes

STEP 5.2 (Option II)

Input weights for selected field attributes in input parameter Weighted Attributes (see Figure A-37).

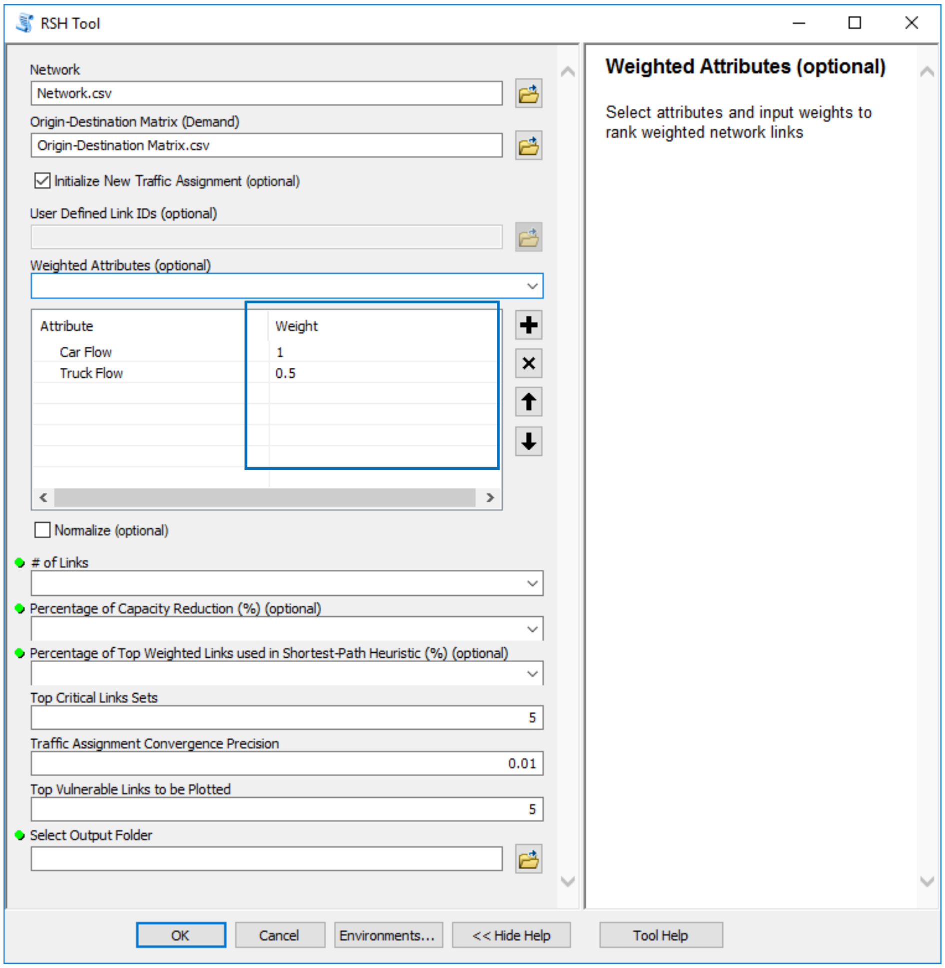


Figure A-37 Input Weights

STEP 5.3 (Option II) (Optional)

Select option Normalize to normalize user inputted weights (see Figure A-38).

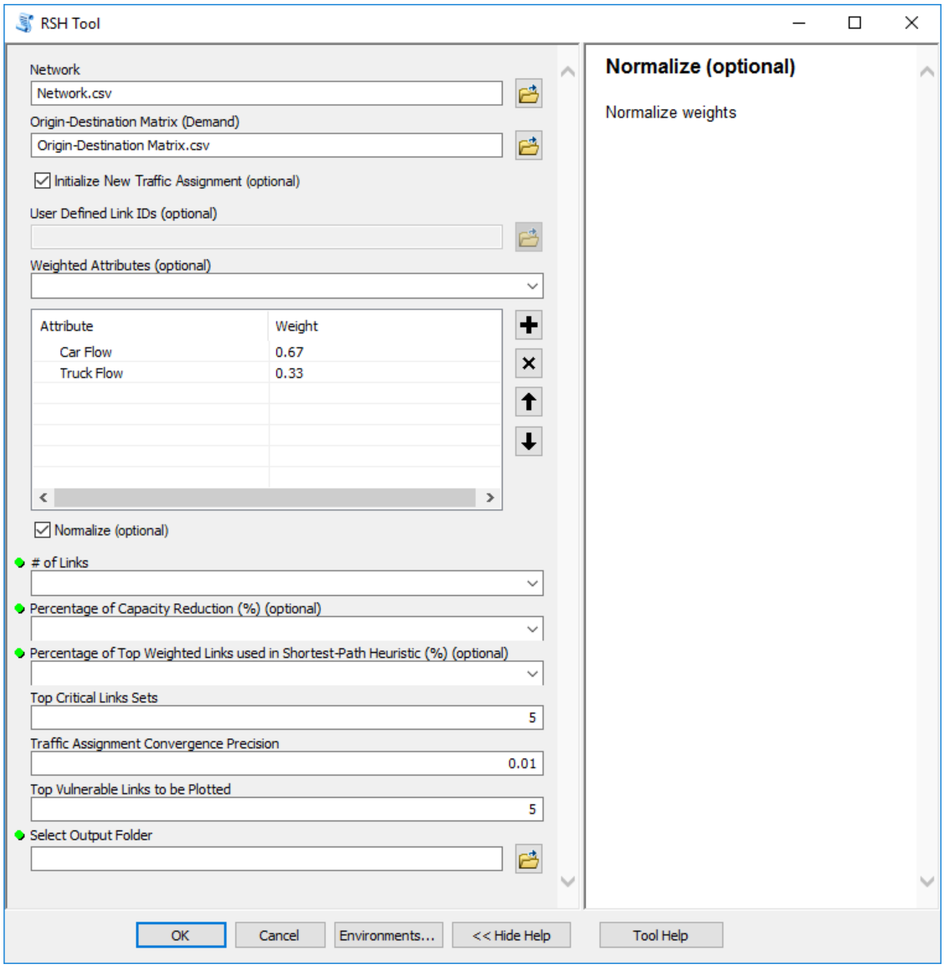


Figure A-38 Normalize Weights

STEP 6

Select the number of top ranked links used to reduce capacity in input parameter # of Links (see Figure A-39).

.

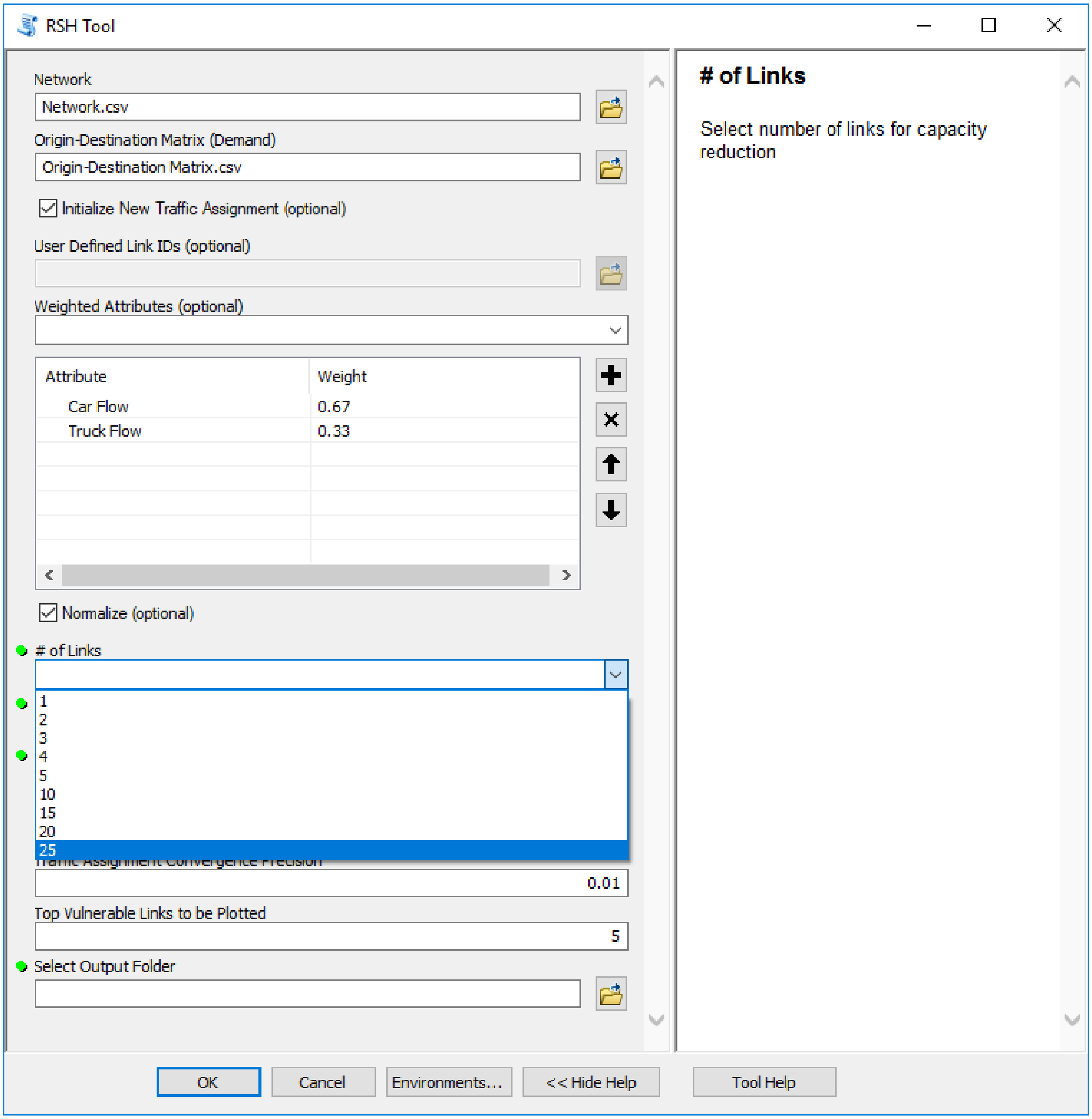


Figure A-39 Select # of Links

STEP 7 (Option II)

Select the percentage used to reduce capacity for the top ranked links in input parameter Percentage of Capacity Reduction (%) (see Figure A-40).

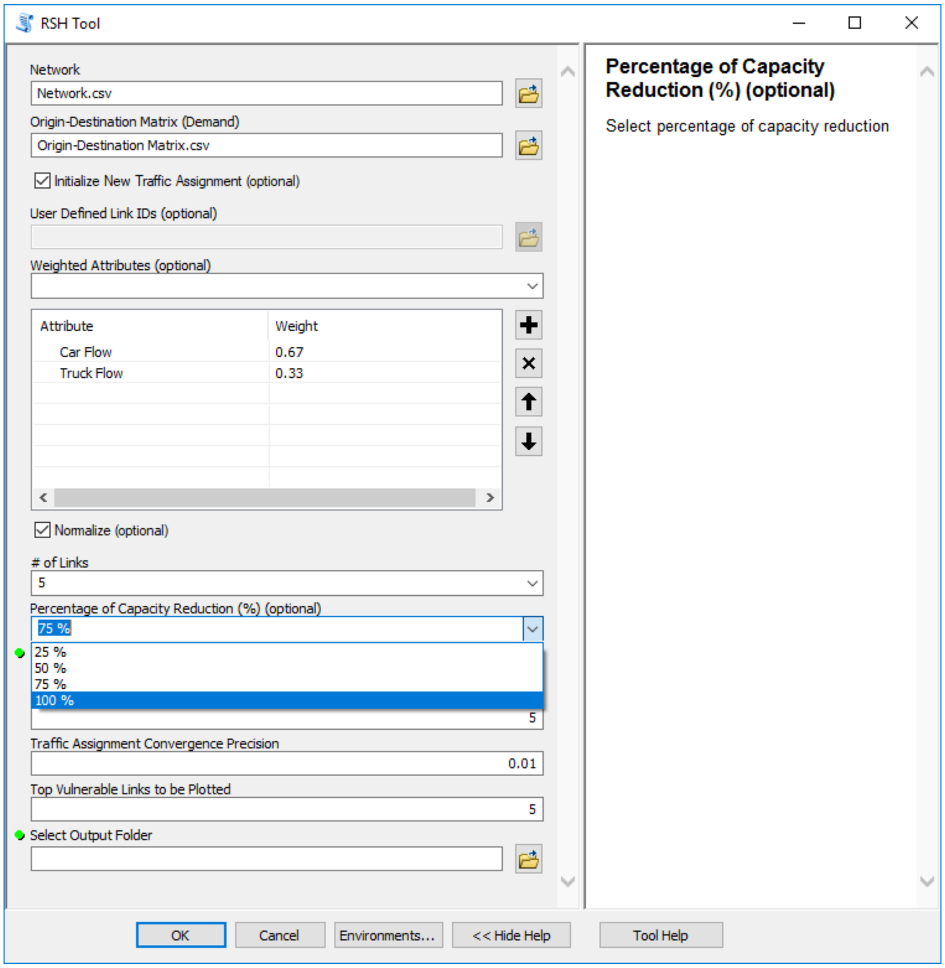


Figure A-40 Select the Percentage of Capacity Reduction

STEP 8

Select the percentage of top weighted links used in shortest-path heuristic (see Figure A-41).

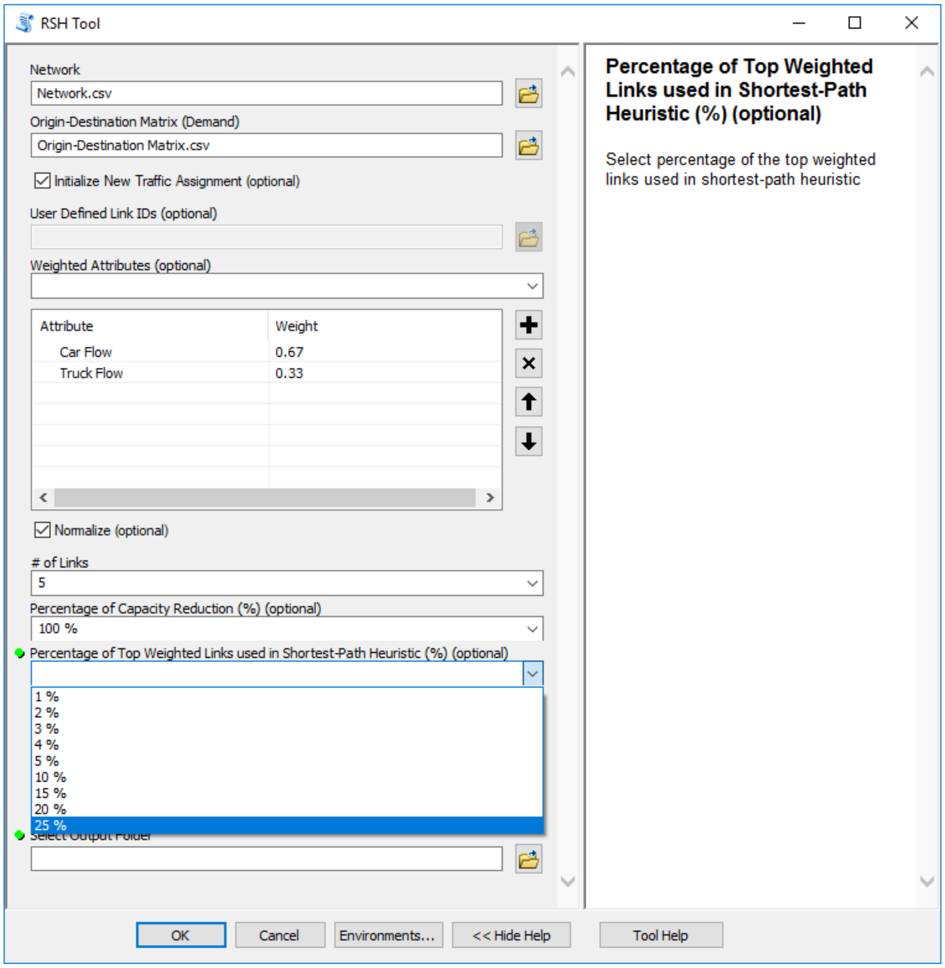


Figure A-41 Select the Percentage of Top Weighted Links Used in Shortest-Path Heuristic (%)

STEP 9

Input number of the top critical link sets used for applying traffic assignment in input parameter Top Critical Link Sets (see Figure A-42).

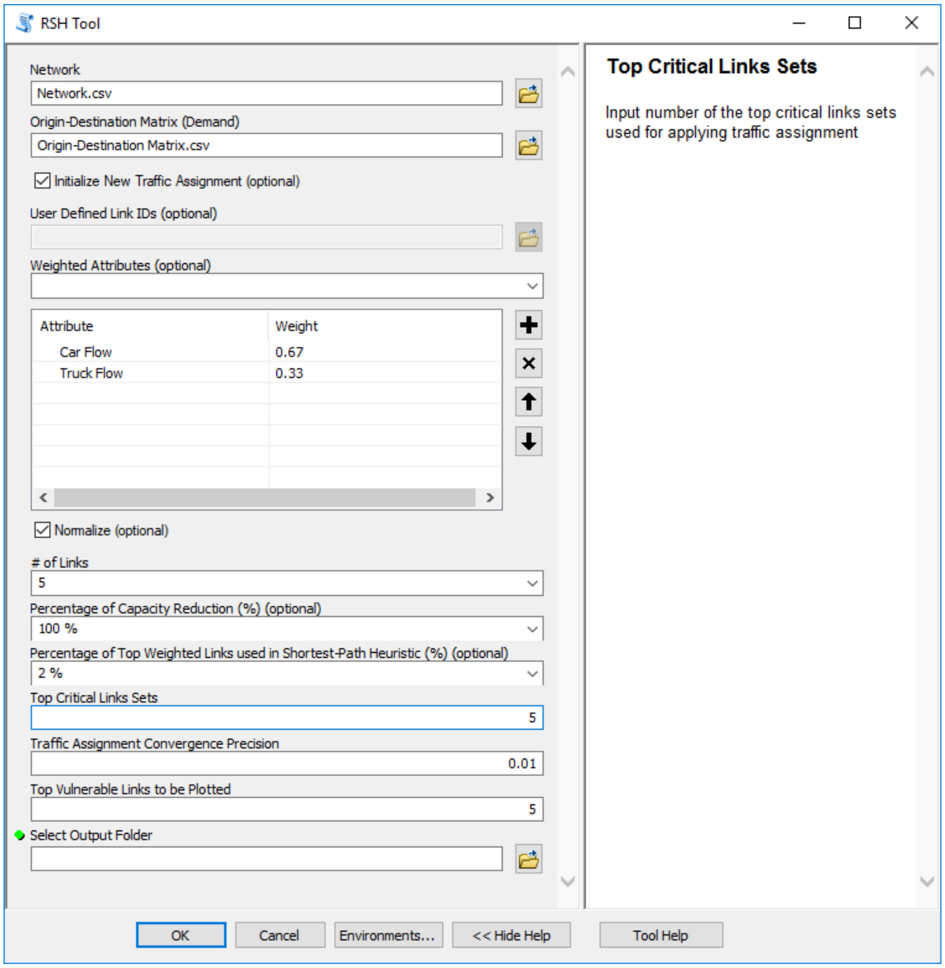


Figure A-42 Input Number of the Top Critical Link Sets

STEP 10

Input Traffic Assignment Convergence Precision (see Figure A-43).

(A default value of 0.01 will be set as input parameter.)

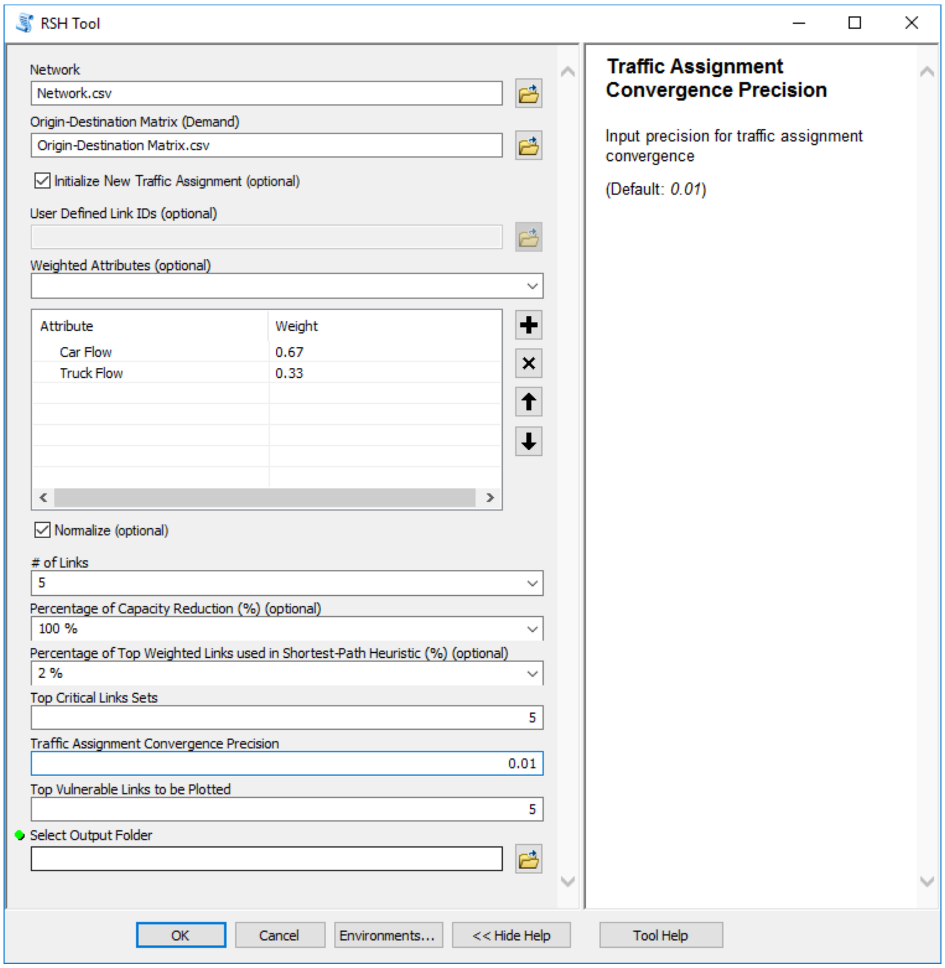


Figure A-43 Input Traffic Assignment Convergence Precision

STEP 11

Input the number of top vulnerable links used to plot the difference in vehicle hours traveled (VHT) and vehicle miles traveled (VMT) in input parameter Top Vulnerable Links to be Plotted (see Figure A-44).

(A default value of 5 will be set as input parameter.)

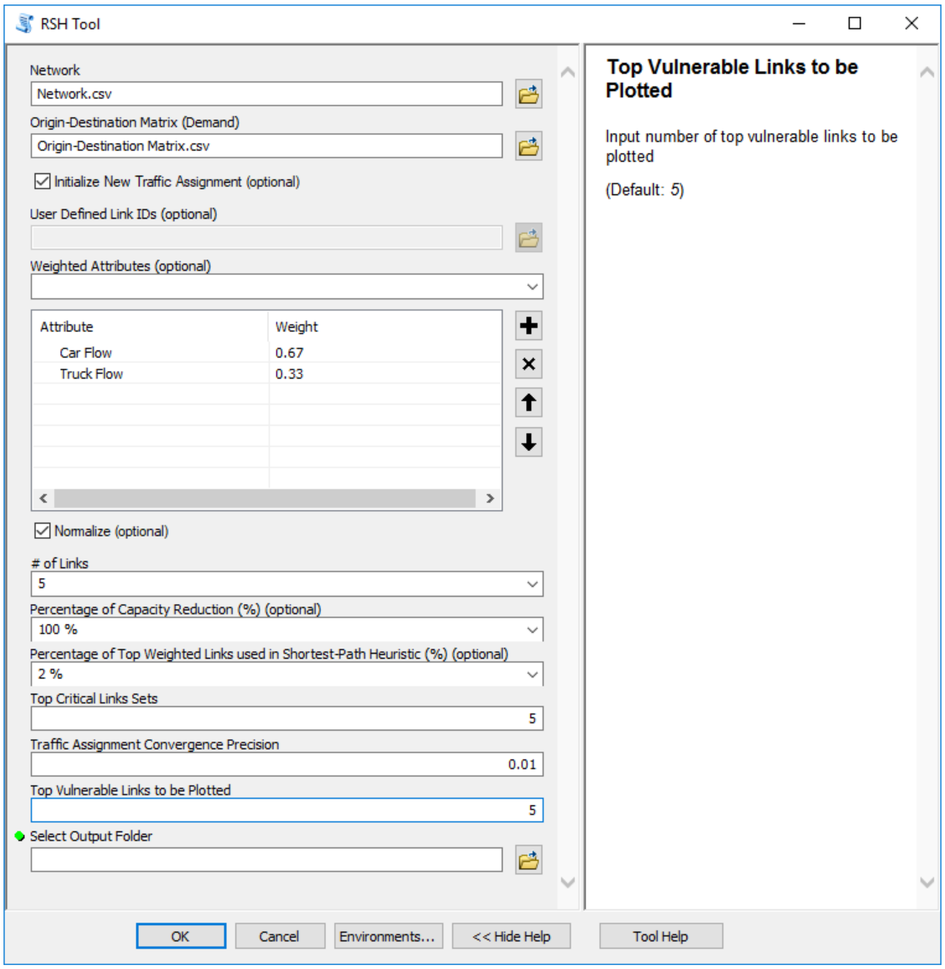


Figure A-44 Input Top Vulnerable Links to be Plotted

STEP 12

In toolbox Select Output Folder parameter input output folder path where processed files will be exported after toolbox analysis (see A-45).

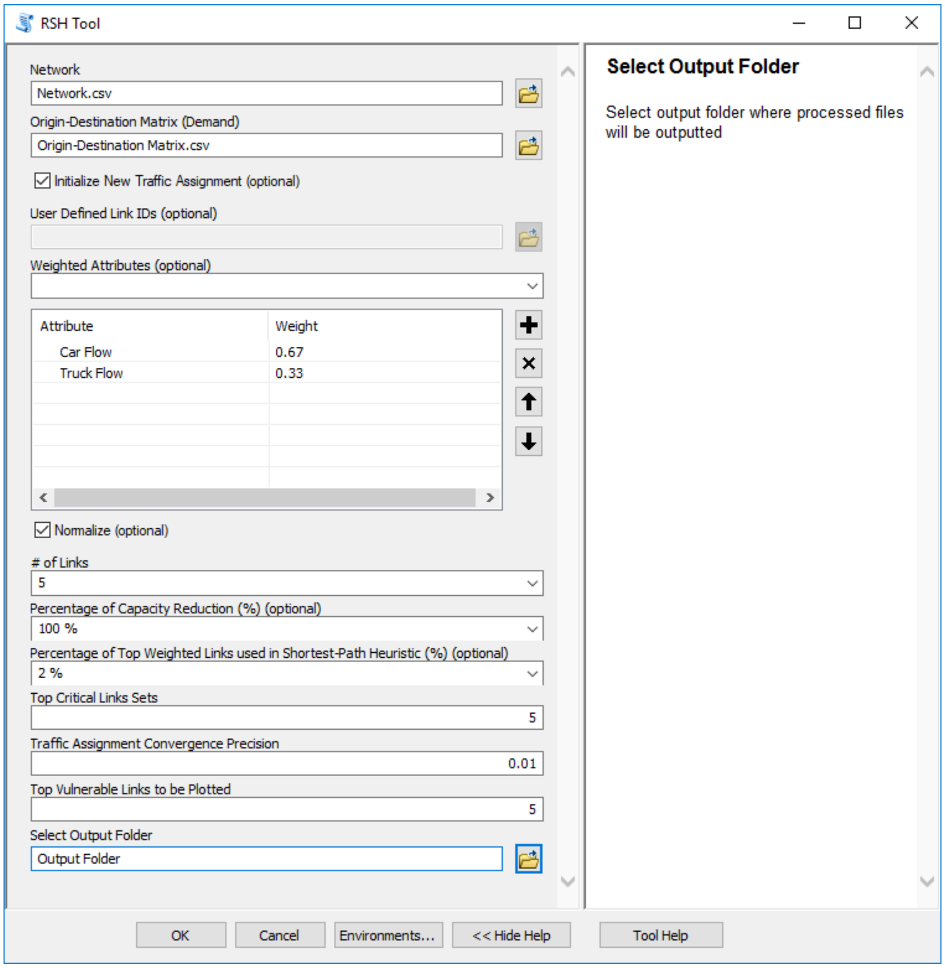


Figure A-45 Input Output Folder

STEP 13

Once all required parameters are inputted, press OK to execute the application. The ArcGIS application invokes a task completion window, which reports status of each task (see Figure A-46). In addition, graph with the top vulnerable link differences in VMT and VHT will appear on a screen (see Figure A-47) in pdf format and the processed tables (see **A-48** and Figure A-49) in (.dbf) format will be imported to ArcMap Display.

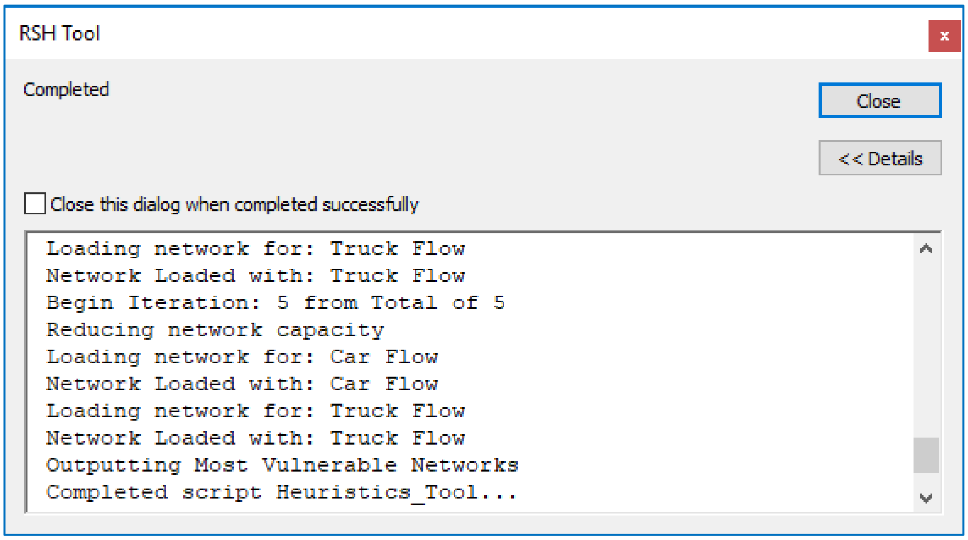


Figure A-46 Application Performance Task Window

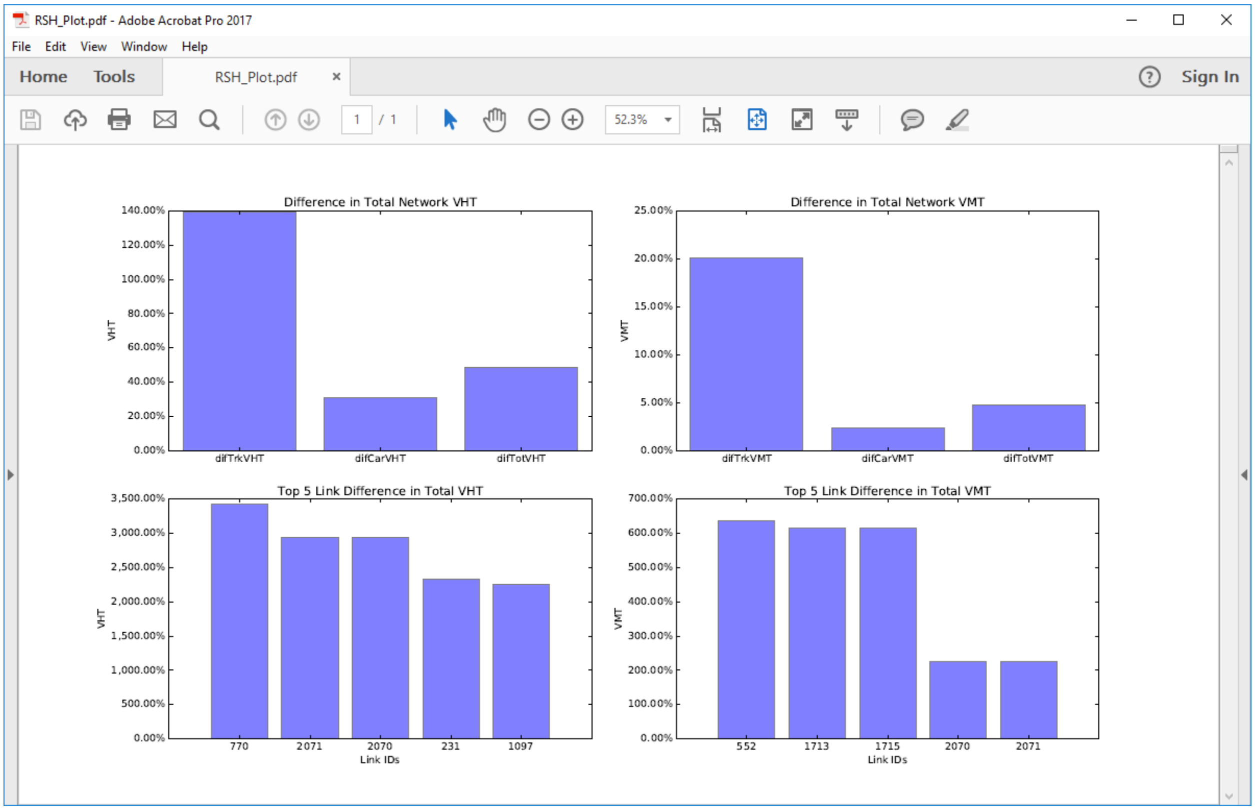


Figure A-47 RSH Plot

RSH_Output_VHT

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
848	849	45800	45856	0.237056	8169	0.15	4	0.238636	13321.765797	3835.641072	17157.406869	0.488542	0
1770	1771	23401	19784	0.139381	4024	0.15	4	0.14031	11607.718267	3559.897741	15167.616008	1.586987	0
2045	2046	45792	45784	0.197326	8169	0.15	4	0.198642	12948.884339	3303.676863	16252.561202	0.384192	0
0	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0
1	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0
2	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0
3	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0
4	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0
5	6	142446	142454	0.06596	3337	0.15	4	0.076074	2409.924037	401.908496	2811.832533	0.068651	0
6	7	126024	142446	0.017417	3337	0.15	4	0.020088	2409.924037	401.908496	2811.832533	0.018128	0
7	8	142454	142462	0.085637	3337	0.15	4	0.098768	2409.924037	401.908496	2811.832533	0.089131	0

0 (0 out of 2406 Selected)

Weights	RedCap	Selected	newTrkFlow	newCarFlow	newTT	difTrkFlow	newTrkVHT	newTrkVMT	difTrkVHT	difTrkVMT
0.001766	0	1	0	0	0	0	0	0	0	0
0.001589	0	1	0	0	0	0	0	0	0	0
0.001618	0	1	0	0	0	0	0	0	0	0
0	3337	0	0	0	0.041364	0	0	0	0	0
0	3337	0	0	0	0.027632	0	0	0	0	0
0	3337	0	0	0	0.086236	0	0	0	0	0
0	3337	0	0	0	0.077587	0	0	0	0	0
0	3337	0	0	0	0.010867	0	0	0	0	0
0.000252	3337	0	401.908496	2542.412384	0.069294	0	27.849847	30.574787	0.258427	0
0.000252	3337	0	401.908496	2542.412384	0.018297	0	7.35372	8.073538	0.067923	0
0.000252	3337	0	401.908496	2542.412384	0.089965	0	36.157698	39.695698	0.335192	0

difCarFlow	newCarVHT	newCarVMT	difCarVHT	difCarVMT	difTT	newTotFlow	newTotVHT	newTotVMT	difTotVHT	difTotVMT
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
132.488347	176.173924	193.41148	10.730229	10.078919	0.000643	2944.32088	204.023771	223.986267	10.988656	10.078919
132.488347	46.518519	51.07198	2.831416	2.661426	0.000169	2944.32088	53.872239	59.145518	2.899339	2.661426
132.488347	228.72813	251.108986	13.929191	13.085609	0.000834	2944.32088	264.885828	290.804684	14.264383	13.085609

Figure A-48 RSH Tool Output VHT

RSH_Output_Critical_Link_Sets

OID	CrtSets	NetCap	NetVHTCar	NetVHTTrk	NetVHTTot	NetVMTCar	NetVMTTrk	NetVMTTot
0	Base Network	11267246	56317591.1654	10968334.8661	67285926.0315	3919481.83483	616980.235974	4536462.0708
1	[2329, 1997, 1992, 2005, 1999]	11252391	56317591.1654	10968334.8661	67285926.0315	3919481.83483	616980.235974	4536462.0708
2	[2023, 2010, 2250, 2216, 2310]	11249782	73897606.2422	26241396.6494	100139002.892	4011298.18898	741100.014985	4752398.20397
3	[2005, 2010, 2329, 1948, 2120]	11252883	56317591.1654	10968334.8661	67285926.0315	3919481.83483	616980.235974	4536462.0708
4	[2009, 1995, 2123, 2216, 2215]	11249211	56077434.8123	10775051.7788	66852486.5911	3916714.60917	628764.108128	4545478.71729
5	[2246, 1991, 2216, 2006, 2002]	11250631	56077723.3702	10774426.6167	66852149.9869	3916716.12361	628767.260918	4545483.38453

1 (0 out of 6 Selected)

Figure A-49 RSH Tool Output Critical Link Sets

STEP 14

User then can add a network in format of shapefile (see Figure A-50) and join the RSH Tool output using field attribute Edge (*Note: User will have add new join field and convert the Edge data attribute field to short integer data type*) and visualize the tool outputs (see Figure A-51).

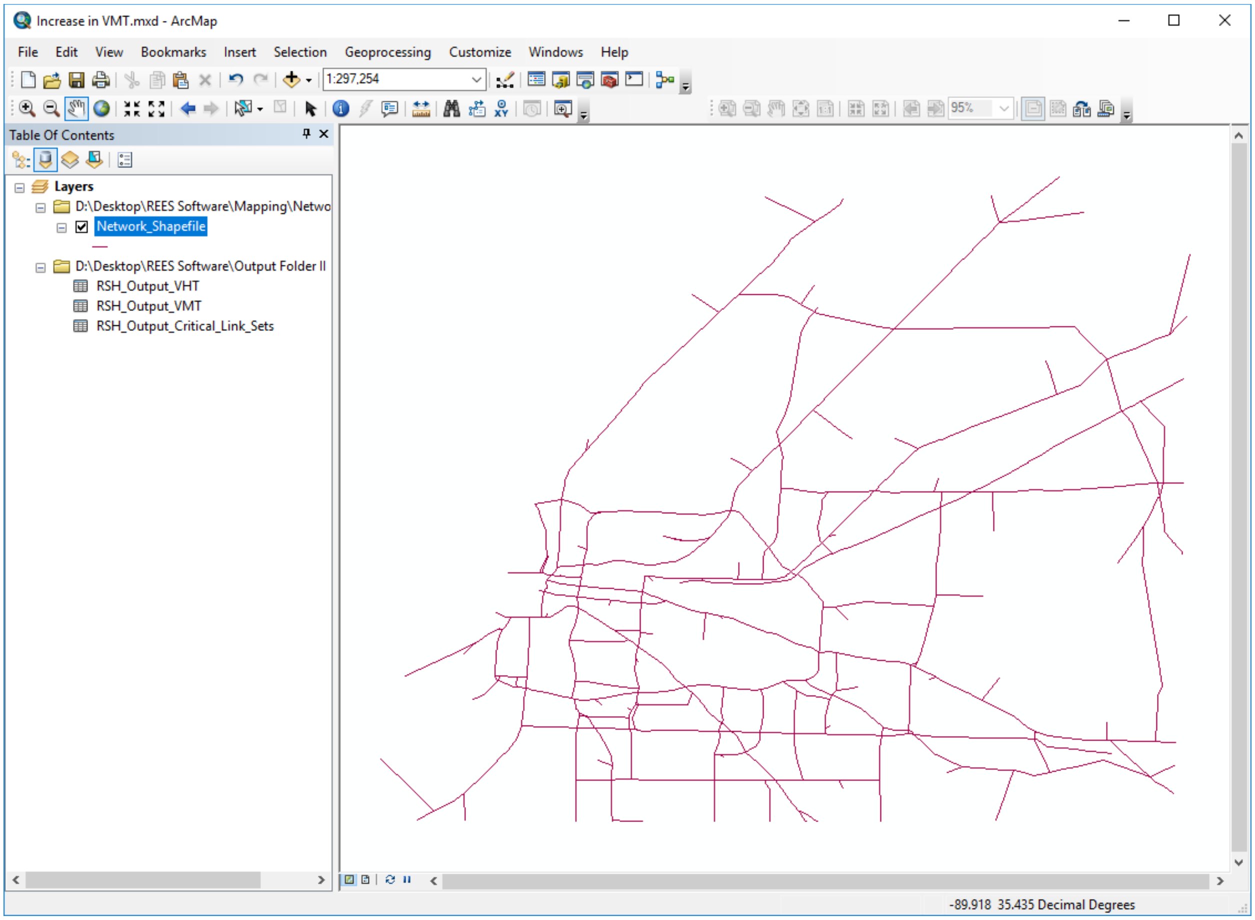
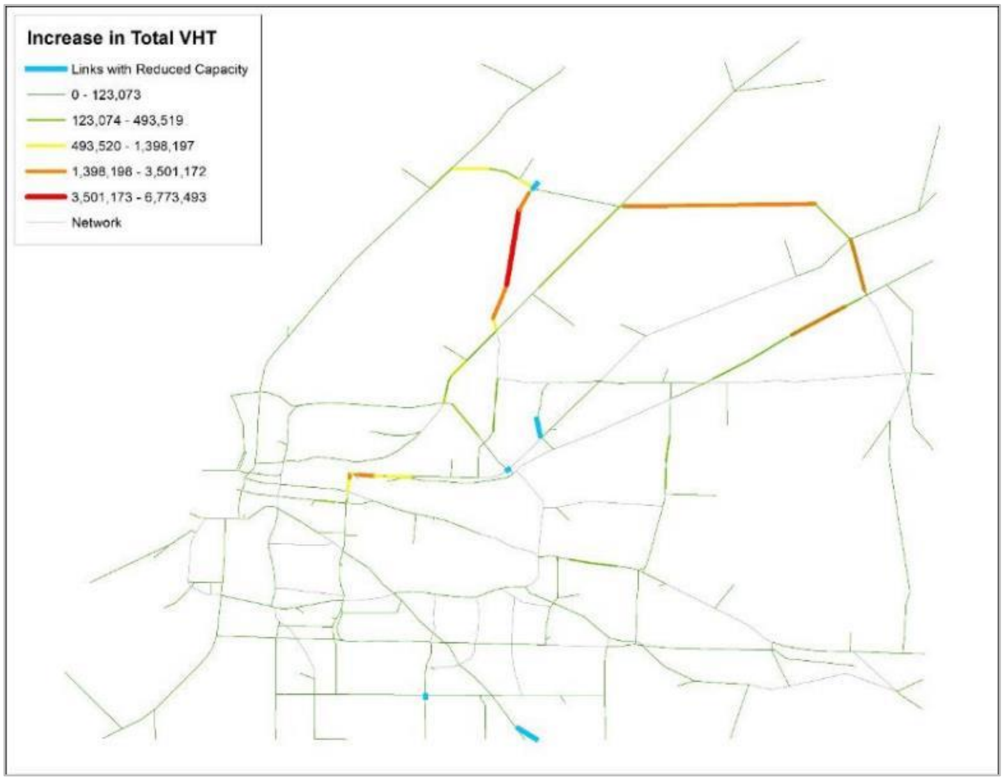


Figure A-50 Add Network in a form of Shapefile



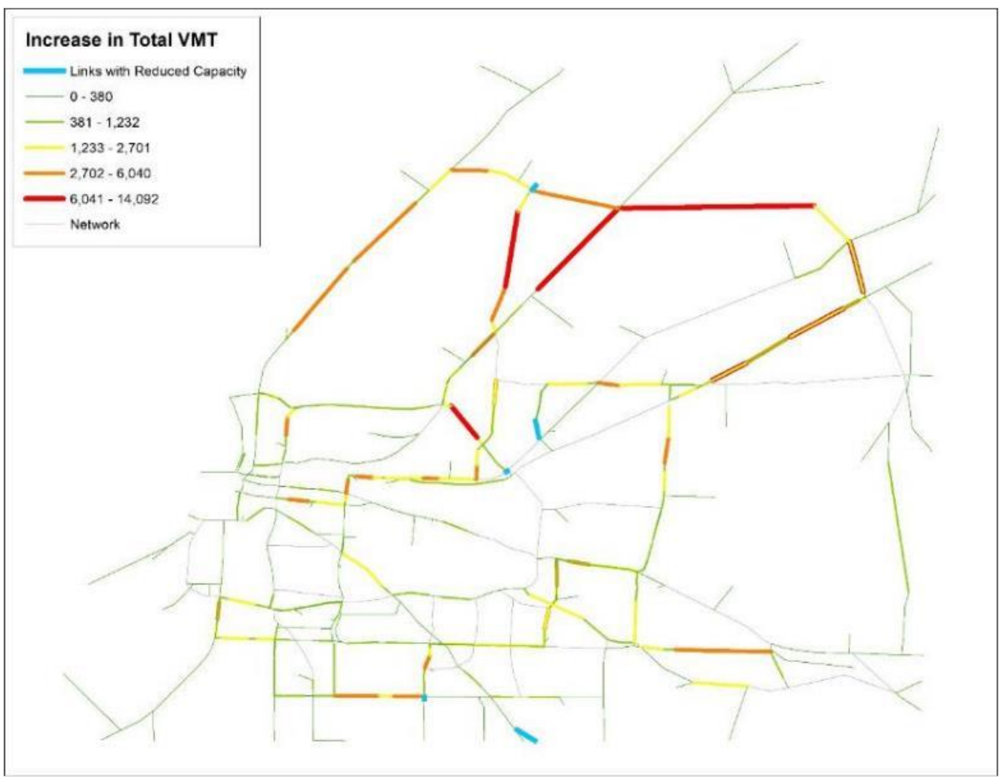


Figure A-51 Visualize the RSH Tool Output

Table A-10 RSH Tool Output Attribute Field Dictionary for VHT and VMT Tables

Field Attribute	Description
Weights	Weighted attribute ratio
newTrkFlow	New truck flow
newCarFlow	New car flow
newTT	New travel time
difTrkFlow	Difference in truck flow
newTrkVHT	New truck vehicle hours traveled (VHT)
newTrkVMT	New truck vehicle miles traveled (VMT)
difTrkVHT	Difference in truck vehicle hours traveled (VHT)
difTrkVMT	Difference in truck vehicle miles traveled (VMT)
difCarFlow	Difference in car flow
newCarVHT	New car vehicle hours traveled (VHT)
newCarVMT	New car vehicle miles traveled (VMT)
difCarVHT	Difference in car vehicle hours traveled (VHT)
difCarVMT	Difference in car vehicle miles traveled (VMT)
difTT	Difference in travel time
newTotFlow	New total flow
newTotVHT	New total vehicle hours traveled (VHT)
newTotVMT	New total vehicle miles traveled (VMT)
difTotVHT	Difference in total vehicle hours traveled (VHT)
difTotVMT	Difference in total vehicle miles traveled (VMT)

Table A-11 RSH Tool Output Attribute Field Dictionary for Critical Link Sets

Field Attribute	Description
CrtSets	A set of critical links used to reduce capacity and run traffic assignment
NetCap	A sum of total network capacity
NetVHTCar	A sum of total network car vehicle hours travelled (VHT)
NetVHTTrk	A sum of total network truck vehicle hours travelled (VHT)
NetVHTTot	A sum of total network total vehicle hours travelled (VHT)
NetVMTCar	A sum of total network car vehicle miles travelled (VMT)
NetVMTTrk	A sum of total network truck vehicle miles travelled (VMT)
NetVMTTot	A sum of total network total vehicle miles travelled (VMT)

K SHORTEST PATH TOOL (KSP TOOL)

Description

K shortest path tool (KSP Tool) for every link in a given transportation network, tool will output:

- The number of k shortest paths link belongs to
- The total (passenger and trucks), passenger and truck flow of link over sum of demand of ODs for which link is on the k shortest path
- The percentage of total (passenger and trucks), passenger and truck flow of link divided by maximum total (passenger and trucks), passenger and truck total flow of any link in the network

Example Input Files

Following tables were used in executing KSP example in format of (.csv) (see Figure A-52) and (.dbf) (see Figure A-53).

- **Network.csv** – Transportation network with the following order of field attributes: Link ID for one direction, From Node, To Node, Free Flow Travel Time, Capacity, Alpha, Beta, Length, Car Flow, Truck Flow, Total Flow, Travel Time, and Connector (0 - No, 1 - yes).
- **Origin-Destination Matrix.csv** – Origin-Destination Matrix with the following order of field attributes: From Node, To Node, Car Demand, Truck Demand, and Total Demand.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0	
2	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0	
3	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0	
4	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0	
5	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0	
6	6	142446	142454	0.06596	3337	0.15	4	0.076074	2491.711	393.9045	2885.616	0.077615	0	
7	7	126024	142446	0.017417	3337	0.15	4	0.020088	2491.711	393.9045	2885.616	0.020495	0	
8	8	142454	142462	0.085637	3337	0.15	4	0.098768	2491.711	393.9045	2885.616	0.100769	0	
9	9	142462	126032	0.085654	3284	0.15	4	0.098788	2491.711	393.9045	2885.616	0.10179	0	
10	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	1.026567	0	

Network

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	5896	19560	152.7698	31.66175	184.4315									
5	5896	23577	26.571	5.930025	32.50103									
6	5896	25532	239.4124	34.91333	274.3257									
7	5896	25596	73.28497	3.473618	76.75859									
8	5896	28439	55.42994	6.288477	61.71842									
9	5896	33668	36.96075	3.216468	40.17722									
10	5896	39108	77.42817	5.138063	82.56623									
11	5896	39140	70.98827	4.681057	75.66932									
12	5896	45640	86.48406	15.7084	102.1925									
13	5896	45712	59.30251	4.452708	63.75521									

Origin-Destination Matrix

Figure A-52 Example input tables in form of (.csv)

Network

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector
0	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.249593	0
1	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.717664	0
2	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.095184	0
3	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.12022	0
4	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.069962	0
5	6	142446	142454	0.06596	3337	0.15	4	0.076074	2888.440965	401.908496	3290.349461	0.510468	0
6	7	126024	142446	0.017417	3337	0.15	4	0.020088	2888.440965	401.908496	3290.349461	0.019867	0
7	8	142454	142462	0.085637	3337	0.15	4	0.098768	2888.440965	401.908496	3290.349461	0.350355	0
8	9	142462	126032	0.085654	3284	0.15	4	0.098788	2888.440965	401.908496	3290.349461	0.158653	0
9	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	3.416619	0

1 (0 out of 2406 Selected)

Origin-Destination Matrix

OID	Pointer	Pointee	Car_Flow	Truck_Flow	Total_Flow
0	5896	5896	0	0	0
1	5896	6072	216.375015	124.732246	341.107261
2	5896	13777	844.064148	71.881973	915.946121
3	5896	19560	152.769791	31.661749	184.43154
4	5896	23577	26.571001	5.930025	32.501026
5	5896	25532	239.412354	34.91333	274.325684
6	5896	25596	73.284973	3.473618	76.758591
7	5896	28439	55.429943	6.288477	61.71842
8	5896	33668	36.960754	3.216468	40.177222
9	5896	39108	77.428169	5.138063	82.566232
10	5896	39140	70.988266	4.681057	75.669323

1 (0 out of 1936 Selected)

Figure A-53 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and launch KSP Tool (see Figure A-54)

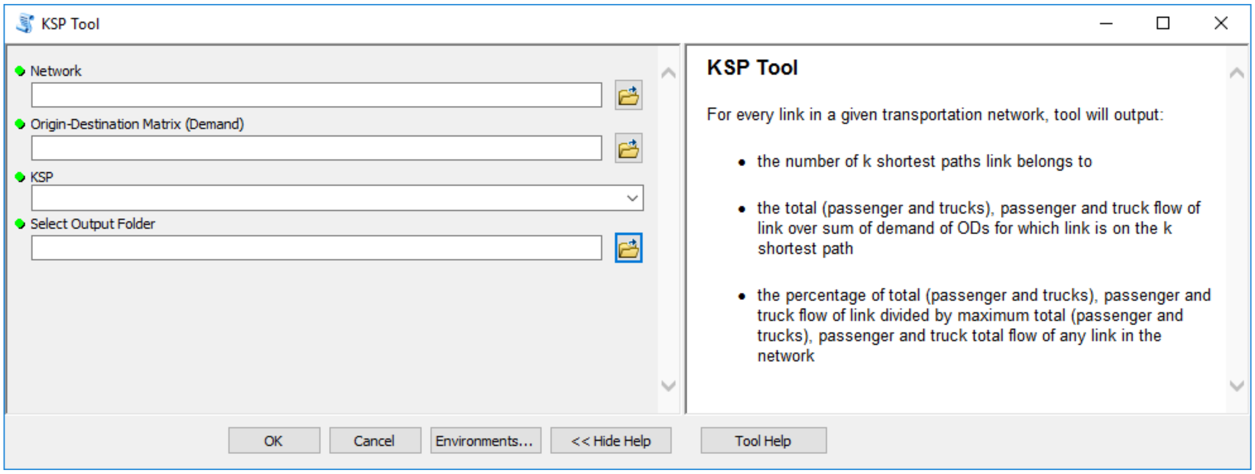


Figure A-54 KSP Tool

STEP 2

Input path to transportation network file in a form of (.csv) or (.dbf) into the tool first input parameter Network (see Figure A-55).

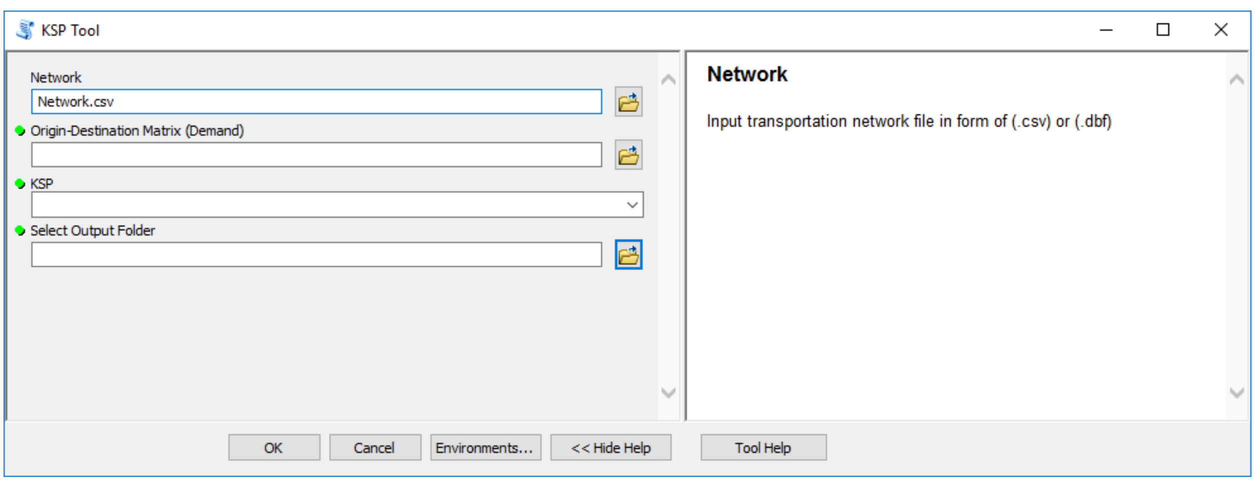


Figure A-55 Input Network

STEP 3

Input path to Origin-Destination Matrix (Demand) file in a form of (.csv) or (.dbf) into the tool second input parameter Origin-Destination Matrix (Demand) (see Figure A-56).

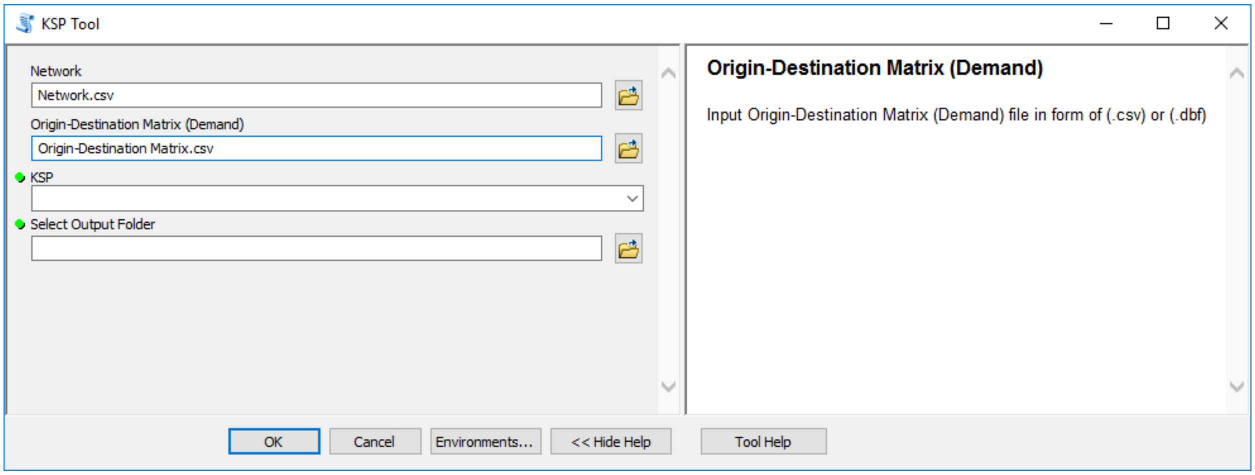


Figure A-56 Input Origin-Destination Matrix

STEP 4

Select k shortest paths in input parameter KSP (see Figure A-57).

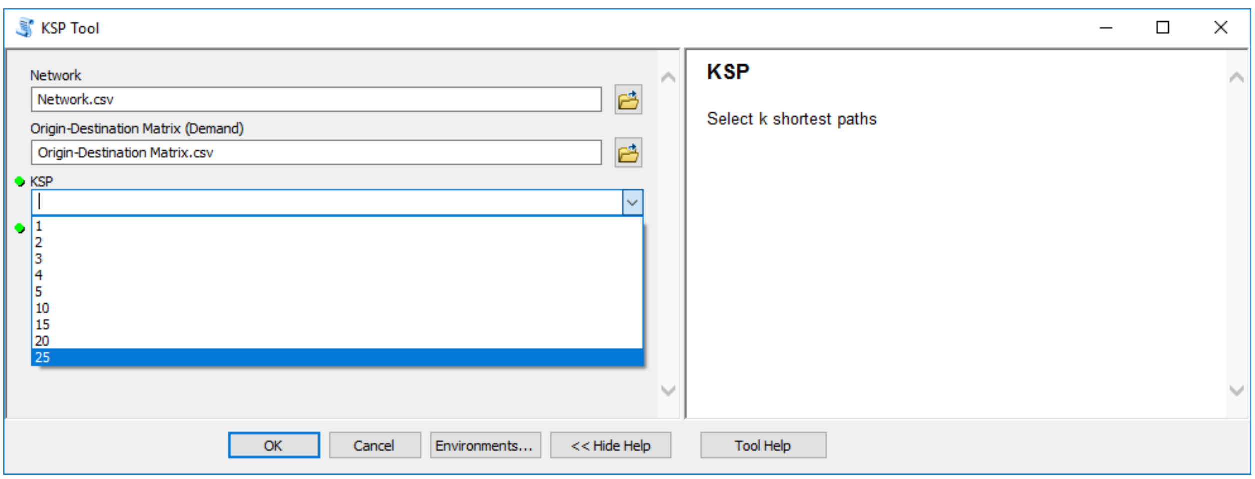


Figure A-57 Select k Shortest Paths

STEP 5

In toolbox Select Output Folder parameter input output folder path where processed files will be exported after toolbox analysis (see Figure A-58).

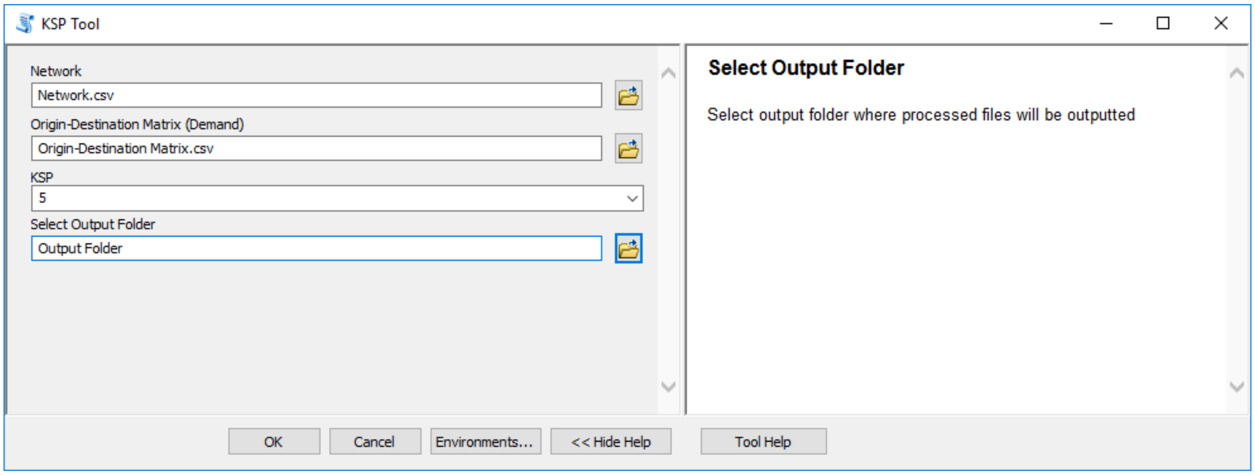


Figure A-58 Input Output Folder

STEP 6

Once all required parameters are inputted, press OK to execute the application. The ArcGIS application invokes a task completion window, which reports status of each task (see Figure A-59). In addition, the processed table (see Figure A-60) in (.dbf) format will be imported to ArcMap Display.

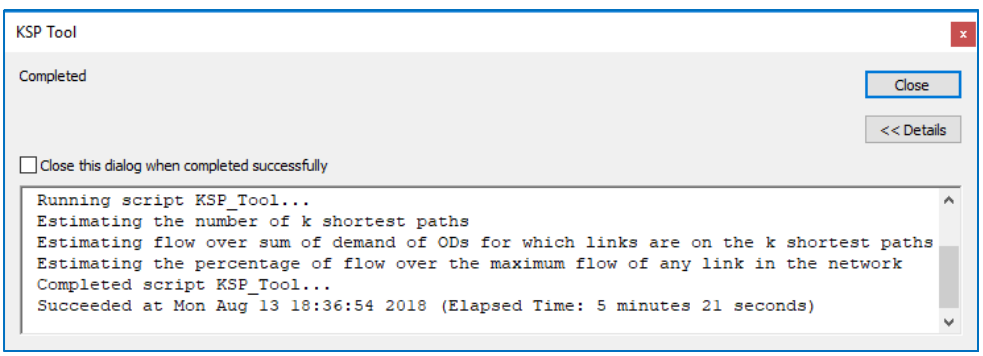


Figure A-59 Application Performance Task Window

KSP_Tool_Output

OID	Edge	1st_KSP	2nd_KSP	3rd_KSP	4th_KSP	5th_KSP	1st_Tot	2nd_Tot	3rd_Tot	4th_Tot	5th_Tot
1581	6	42	42	42	41	43	0.9106	0.9106	0.9106	0.9189	0.8299
813	7	42	42	62	69	61	0.9106	0.9106	0.6141	0.6768	0.5114
1582	8	42	42	42	41	43	0.9106	0.9106	0.9106	0.9189	0.8299
1583	9	42	42	42	41	43	0.9106	0.9106	0.9106	0.9189	0.8299
1912	19	43	43	43	45	47	1	1	1	0.9973	0.9982
1538	23	5	5	5	6	4	2.8149	2.8149	2.8149	2.7247	5.0858
1539	24	5	7	5	6	4	2.8149	2.4153	2.8149	2.7247	5.0858
11	52	16	16	16	16	16	0.7734	0.7734	0.7734	0.7734	0.7734

0 (0 out of 1913 Selected)

1st_Car	2nd_Car	3rd_Car	4th_Car	5th_Car	1st_Trk	2nd_Trk	3rd_Trk	4th_Trk	5th_Trk	TotToMax	CarToMax	TrkToMax
0.9005	0.9005	0.9005	0.9092	0.8202	0.9801	0.9801	0.9801	0.985	0.897	10.149	10.4758	8.4764
0.9005	0.9005	0.6058	0.6616	0.5097	0.9801	0.9801	0.6721	0.7921	0.5227	10.149	10.4758	8.4764
0.9005	0.9005	0.9005	0.9092	0.8202	0.9801	0.9801	0.9801	0.985	0.897	10.149	10.4758	8.4764
0.9005	0.9005	0.9005	0.9092	0.8202	0.9801	0.9801	0.9801	0.985	0.897	10.149	10.4758	8.4764
1	1	1	0.9966	0.9978	1	1	1	0.9999	0.9997	18.4778	17.4229	23.8769
2.7705	2.7705	2.7705	2.6788	4.9118	3.2288	3.2288	3.2288	3.1562	7.0938	6.9953	7.4317	4.7617
2.7705	2.3446	2.7705	2.6788	4.9118	3.2288	3.1811	3.2288	3.1562	7.0938	6.9953	7.4317	4.7617
0.7502	0.7502	0.7502	0.7502	0.7502	0.8459	0.8459	0.8459	0.8459	0.8459	23.8325	20.9431	38.6212

Figure A-60 KSP Tool Output

STEP 7

User then can add a network in format of shapefile (see Figure A-61) and join the KSP Tool output using field attribute Edge (*Note: User will have add new join field and convert the Edge data attribute field to short integer data type*) and visualize the tool outputs (see Figure A-62).

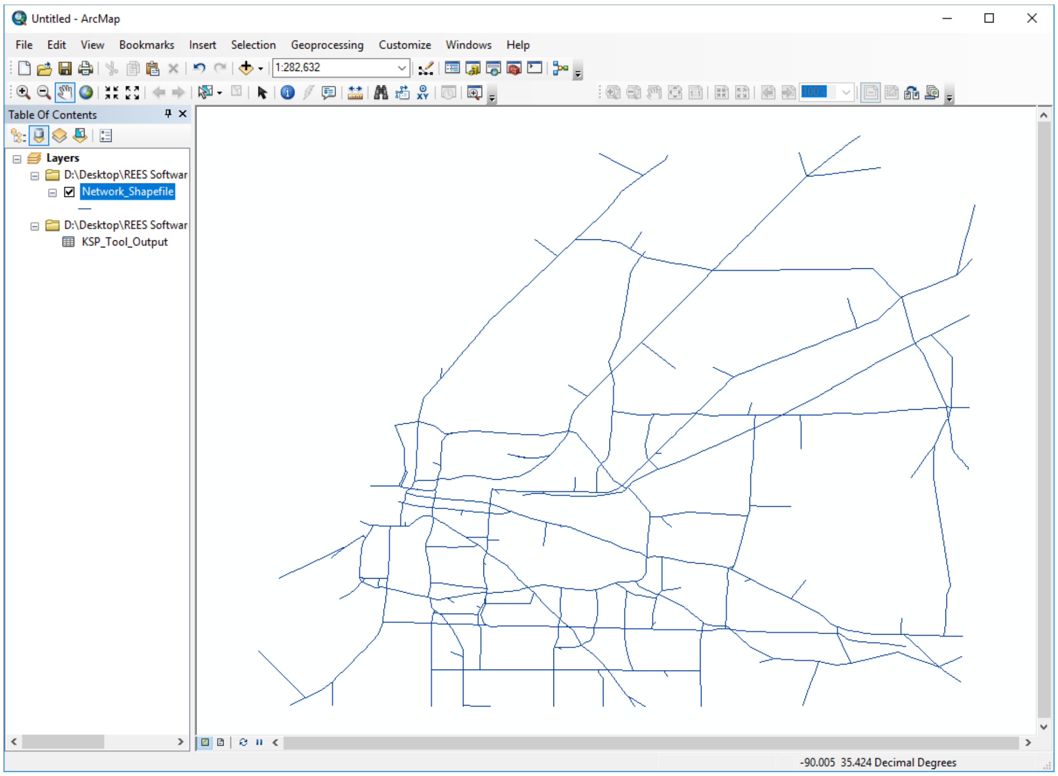
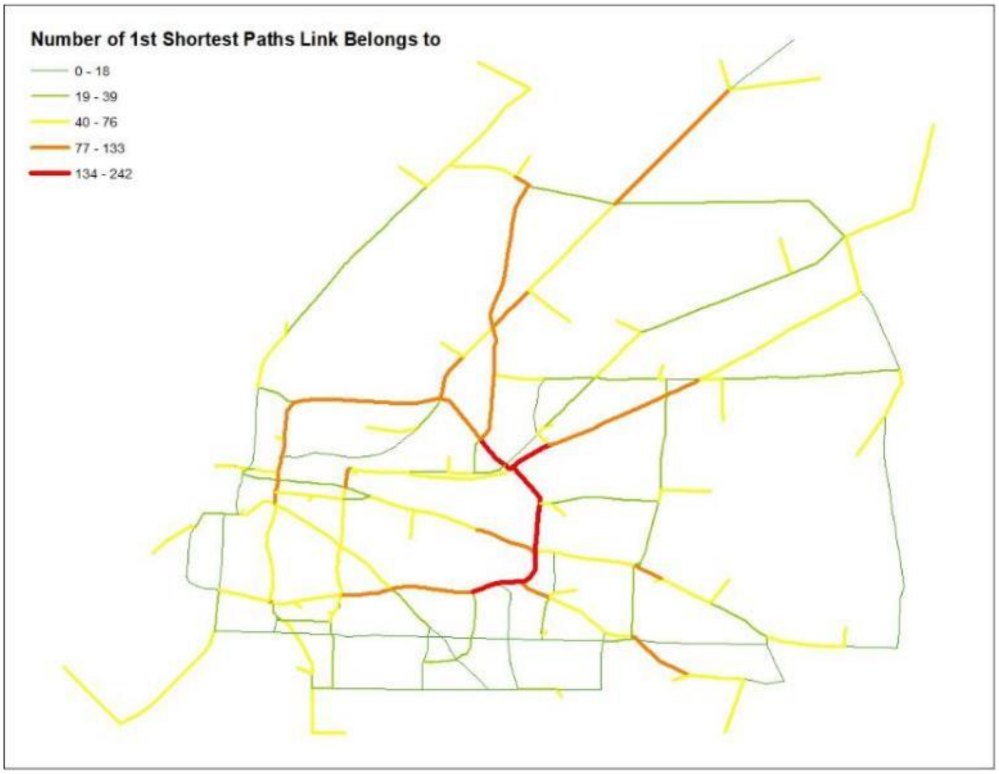


Figure A-61 Add Network in a form of Shapefile



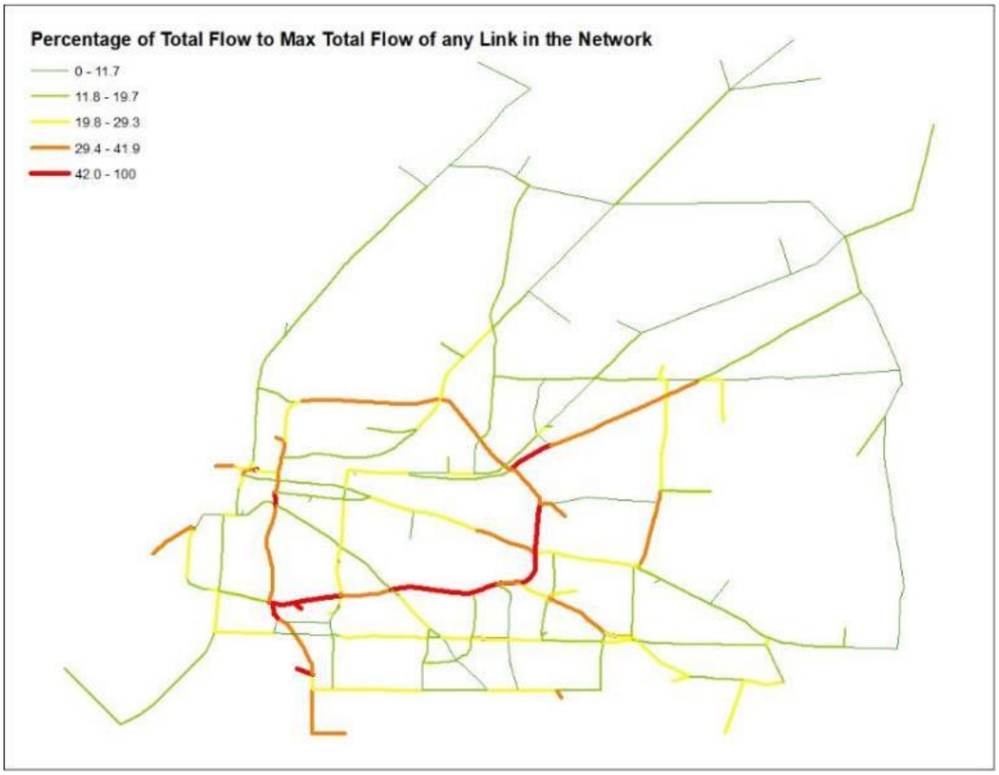


Figure A-62 Visualize the KSP Tool Output

Table A-12 KSP Tool Output Attribute Field Dictionary

Field Attribute	Description
#_KSP	Number of # shortest paths link belongs to
#_Tot	Total flow of link over sum of demand of ODs for which link is on the # shortest path
#_Car	Passenger flow of link over sum of demand of ODs for which link is on the # shortest path
#_Trk	Truck flow of link over sum of demand of ODs for which link is on the # shortest path
TotToMax	Percentage of total flow of link over the maximum total flow of any link in the network
CarToMax	Percentage of passenger flow of link over the maximum passenger flow of any link in the network
TrkToMAX	Percentage of truck flow of link over the maximum truck flow of any link in the network