TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. FMRI-Y3R7- 19	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle IDENTIFYING CRITICAL AND VULNERABLE FREIGHT ROUTES IN ROADWAY NETWORKS: A GAME THEORY FRAMEWORK AND APPLICATION IN THE STATE OF FLORIDA		5. Report Date: April 2021 6. Performing Organization Code:
7. Author(s) Mihalis Golias, Sabyasachee Mishra, Evangelos Kaisar, Ioannis Hourdos, Hana Takhtfiroozeh, Aline Machatto, Dimitris Giampouranis, and Vasileios Liatsos		8. Performing Organization Report No.
9. Performing Organization Name and Address University of Memphis, Florida Atlantic University, University of Minnesota, Freight Mobility Research Institute		10. Work Unit No. (TRAIS) 11. Contract or Grant No. 69A3551747120
12. Sponsoring Agency Name and Address Freight Mobility Research Institute Florida Atlantic University 777 Glades Rd., Bldg. 36, Boca Raton, FL 33431		13. Type of Report and Period: Final 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

Transportation networks form the backbone of economic and sustainable development in a society and need to be functional and efficient to provide appropriate services to people during their normal daily life (e.g., providing the means for travel, production logistics, and delivery of services). All transportation networks are vulnerable to disruptions such as natural disasters and/or man-made incidents (e.g., accidents) to some extent, with temporary or permanent effects. 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 ability to detect the critical components in a transportation network is fundamental to the design of resilient networks as well as making improvements in the traffic conditions in cases such as the partial or full capacity of link disruptions. The objective of this project is presenting methodologies and tools to identify the critical links and routes in the real size network. Based on the complexity of the project, different methodologies have been developed to cover all the disruption scenarios.

17. Key Words Freight Vehicles, Freight Routes, Critical Corridors, Game Theory	18. Distribution Statement No restrictions. This document is available to the public through Fmri.fau.edu

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

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

FREIGHT MOBILITY RESEARCH INSTITUTE

College of Engineering & Computer Science

Florida Atlantic University

Project ID: Y3R7-19

IDENTIFYING CRITICAL AND VULNERABLE FREIGHT ROUTES IN ROADWAY NETWORKS: A GAME THEORY FRAMEWORK AND APPLICATION IN THE STATE OF FLORIDA

Final Report

by

Mihalis Golias, Sabyasachee Mishra, Evangelos Kaisar, Ioannis Hourdos, Hana Takhtfiroozeh, Aline Machatto, Dimitris Giampouranis, and Vasileios Liatsos

for

Freight Mobility Research Institute (FMRI)
Florida Atlantic University
777 Glades Rd.
Boca Raton, FL 33431

April, 2021

ACKNOWLEDGEMENT

This project was funded by the Freight Mobility Research Institute (FMRI), one of the twenty TIER University Transportation Centers that were selected in this nationwide competition, by the Office of the Assistant Secretary for Research and Technology (OST-R), U.S. Department of Transportation (US DOT).

DISCLAIMER

CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

Transportation networks form the backbone of economic and sustainable development in a society and need to be functional and efficient to provide appropriate services to people during their normal daily life (e.g., providing the means for travel, production logistics, and delivery of services). All transportation networks are vulnerable to disruptions such as natural disasters and/or man-made incidents (e.g., accidents) to some extent, with temporary or permanent effects. 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 ability to detect the critical components in a transportation network is fundamental to the design of resilient networks as well as making improvements in the traffic conditions in cases such as the partial or full capacity of link disruptions.

The objective of this project is presenting methodologies and tools to identify the critical links and routes in the real size network. Based on the complexity of the project, different methodologies have been developed to cover all the disruption scenarios. This research used the demand/supply of the passenger and freight road network of the Broward County in the state of Florida. Broward county was chosen due to its significance in the freight scenario, with Port Everglades, Fort Lauderdale International Airport, I-95, Florida Turnpike, I-595, and an important commercial travel district.

In this project all the links and routes are ranked based on three criticality measures developed by Takhtfiroozeh and Golias (1) by combining their characteristics of traffic equilibrium and network topology. Ranking links and routes using these hybrid measures, can help decision makers identify critical links and routes based on a combination of their centrality and traffic attributes. To identify the most critical combination of critical links in a roadway network with focusing on both day-to-day and major disruptions, the solution algorithm and modeling framework developed by Higgs and Golias (2) with multiple decision makers and objectives is modified to fit the testbed network under consideration in the state of Florida. The modifications of the solution algorithm consist of introducing network topology characteristics to reduce the feasible search space and complexity. In this project, the GIS based tool to identify vulnerable freight links and routes developed by Higgs and Golias (2) was modified to include network topology characteristics in the identification of vulnerable links and routes.

1. INTRODUCTION

Every society is highly dependent on several numbers of critical infrastructures, such as electrical power, communication networks, water distribution systems, and transportation network, which form the pillars of economic and sustainable development in any country. With technological advancements in the past few decades along with improvements in the efficiency of these infrastructure systems, their vulnerability has also increased as the systems become more complicated and interdependent.

A functional and efficient transportation infrastructure significantly contributes to economic growth and prosperity by providing the means for travel, production logistics, and delivery of service in normal daily life. During disasters such as earthquakes and floods, a functional transportation network is a critical lifeline for damage assessment, search and rescue, emergency medical care, emergency restoration of essential services, firefighting, emergency communications, crisis decision-making, evacuation, protection of lives and property, provision of emergency shelter for victims, and debris removal. Transportation systems, and particularly roadway infrastructures, must be functional to provide service for people during normal daily life and should be robust against disruptions and disasters.

The inkling of the study of transportation network vulnerability started after the Tasman Bridge disaster in 1975, which Lock and Gelling (3) studied the impacts of the failure or loss of critical components of transportation Infrastructure. Over the years, researchers have realized the importance of characterizing the performance of roadway systems, and the literature review reveals several published articles identifying the vulnerability of roadway networks against different disruptions. Network vulnerability has a direct relationship with performance of the degraded network and, consequently, significant social and economic impacts. However, it took decades to expand research interests in this area from academia and finally getting attentions from transport modelers. Great Kobe earthquake in 1994 where substantial parts of the infrastructure was destroyed and caused more than $150 billion economic losses, might be the first time that resilience and vulnerability of the transportation infrastructure gained attentions from government and transportation agencies as a vital interest topic. Over the last decades, vulnerability emerged as a significant area in transportation planning research and received more attentions from researchers and planners for two main reasons: first; developing the theory of the vulnerability and, second; applying the new approach for large-scale transportation networks.

In the area of transportation systems, vulnerability analysis focuses on identifying and ranking infrastructure elements that would have the highest effect in case of failure (4). Resilience, on the other hand, reflects the dynamic performance of the network after a disruption (5) and is another term with definition and interpretation akin to the term of vulnerability. Resilience encompasses vulnerability and, focuses on decision making (operational, tactical, and planning levels for individuals and communities) to develop a transportation system that can withstand disruptions, continue to operate within an acceptable level of efficiency during and right after a disruption and return to normal operating conditions within the shortest possible time.

The fundamental goal of vulnerability analysis can be disaggregated in many sub-goals. One of the essential parts of this analysis is identifying critical components in the network where some incidents may lead to particularly severe consequences and could result in possibilities for severe consequences in these regions. These potentials for severe consequences under such incidents cannot be neglected. Vulnerability analysis and discovering the critical components in the road network may assist the road authorities and agencies to counteract the identified vulnerabilities before they occur. This knowledge is valuable in both the planning stage (e.g., preventing locating a new roadway in the neighborhood of potential hazards) and the operating stage (e.g., actions to reduce the likelihood of incidents depending on the type of identified hazard or threat via some practical examples. For example, traffic accident cases might be avoided by straightening or widening the road or decreasing the speed limit on the road segment; or flood natural hazard cases may be avoided by upgrading the road structures such as switching to larger drainpipes to handle floods).

Knowing the structure of the network and how its components connect is necessary for studying the vulnerability of the network. In fact, it helps to understand the basic knowledge about how flow moves through the network and how any network will function. Also, in order to study the transport flow, it is necessary to have good knowledge about theories and models for analyzing traffic flow. The macroscopic flow diagram helps to illustrate volume and destiny of the traffic characteristics of the network. It can also reveal the observed phenomenon of the “capacity drop” and substantially the “density drop” in the system, which can result in lower demand for using the road. The main component of the travel demand is origin-destination matrices (the number of trips for a given origin point to an assigned destination), and the first step of travel demand analysis in vulnerability studies is route choice, which is modeled as “traffic assignment” models.

Certain parts of the network may be considered more important than the others due to the topological factors, links usage, or presence of important origin destinations. In other words, some links are more critical than the others and any damage or in the worst-case scenario failure of these links may have more severe damage to the system and can result in increasing the travel cost by a large amount. Therefore, identifying and ranking the links that have the most significant effects on the overall performance of the network disruptions is an important consideration for operators and planners. In fact, it is crucial to know and be aware of the outcomes deriving from reducing capacities on critical links. Vulnerability and Resilience analysis aims to evaluate and predict the consequence of the disruptions and ranking links based on different indices. A single factor cannot solely determine the criticality of a link, while different factors with various weights in different situations can determine the criticality of a link or a set of links. Therefore, strengthening and maintaining the links of a transportation network need to be based on a prioritization methodology incorporating multiple factors given the differences in criticality of various links and budgetary limitations.

2. LITERATURE REVIEW

This literature review is divided into two main parts: (1) vulnerability, (2) game theory. The vulnerability part is divided into three sections that are structured around the many answers to the three questions that Kaplan and Garrick (6) associate with vulnerability. The first section is a collection of the various threats to transportation networks that have appeared in literature. The second section is a collection of the literature that has used likelihood or probabilities in the analysis of threats to a network. The third section is a collection of the various ways that impacts of events can be measured and the methods used to find vulnerabilities to these measures. 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 multi-objective optimization part of this review focuses on the many algorithms and methods that have been used to solve problems that have multiple objectives that can conflict. The traffic assignment part of the review focuses on the methods and algorithms used to apply artificial traffic to simulated networks.

2.1 VULNERABILITY

Investigations of the vulnerabilities of systems have been an increasingly popular area of research. The research articles in this area can be drastically different 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. Kaplan and Garrick (6) define vulnerability as risk associated with four questions:

1. What can happen?
2. How likely is it that that will happen?
3. If it does happen, what are the consequences?
4. Which measures can be used to quantify the vulnerability?

This presents a very amenable framework that can lend itself to multiple different interpretations of the meaning of vulnerability.

2.1.1 What can happen?

Transportation networks are open to a wide variety of threats that can be divided into two main categories: intentional and unintentional. Intentional threats are man-made with the objective of disrupting the network. Unintentional threats are both natural and man-made.

2.1.1.1 Intentional Threats

Intentional threats, listed in Table 2. 1.1 are deliberate attacks on a network with a clear goal of disrupting the network. Unlike unintentional threats, intentional threats are intelligent and attempt to exploit known vulnerabilities. Construction on roadways falls into this category because it is an intentional intelligent action that can temporarily lower performance on a network. This also creates a paradox where in order to protect certain infrastructure against vulnerability, construction must create a temporary vulnerability.

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

Table 2. 1 List of Intentional Threats

Threat	Description
Terrorist Attack (7,8)	A terrorist attack is a very focused and deliberate attack to damage or destroy a particular infrastructure
Construction (9)	Partial or full road closures are very common occurrences when maintaining or improving roadways

2.1.1.2 Unintentional Threats

Unintentional threats usually pertain to the consequences of human error or the damage caused by acts of nature. Human errors like negligence and traffic accidents can have drastic consequences for a network. This review distinguishes between weather events (rain, snow, etc.) and natural disasters (earthquake, hurricane, etc.) by considering that weather events occur often, and natural disasters are rare. Extreme weather events can be classified as natural disasters because they present dangers that are on the same scale as other natural disasters. For example, excessive rainfall can cause flooding that can wash away roadways and excessive snowfall can prevent roadways from being used safely.

2.1.1.3 Weather Events

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

Table 2. 2 List of Weather Events

Weather Event	Description
Rain (10)	Precipitation in the form of liquid water
Snow and Ice (11,12)	Precipitation in the form of frozen water

2.1.1.4 Natural Disasters

Natural disasters have been responsible for billions of dollars of damage in the United States. From 1980 to 2011, there have been 133 disasters designated as billion-dollar disasters for totaling damages more than one billion dollars. These disasters included: hurricanes, droughts, severe local storms, non-tropical floods, winter storms, wildfires, and freezes. There are many other natural disasters (listed in Table 2. 3) that are destructive but are not designated as billion-dollar disasters.

Table 2. 3 List of Natural Disasters

Natural Hazard	Description
Earthquakes (13,14)	The sudden release of energy in the Earth's crust that creates seismic waves
Volcanic Activity (15)	This can be an eruption or lava flow associated with an active volcano
Sea Level Rise (16)	The gradual rise of sea level over time (8 inches in the past century)
Flooding (14,17)	An overflow of water that submerges land that is typically dry
Tsunamis (17)	A sea wave caused by the displacement of a large volume of a body of water.
Hurricane (18)	A large tropical storm system with high-powered circular winds
Tornado (19)	A funnel cloud of violently rotating winds
Wildfires (19)	A large, destructive fire that spreads quickly
Blizzard (19)	A severe snowstorm with high winds and low visibility

2.1.1.5 Human Related Events

Humans can make choices that have unintended consequences for the performance of a roadway network. Table 2. 4 lists the events that fall under unintended consequences of human actions. In the worst of cases, improper maintenance of a bridge can led to a collapse as was the case for I-35 W in Minnesota. Traffic accidents are much more common than bridge failures with 10.8 million crashes occurring in 2009.

Table 2. 4 List of Humen Error Events

Human Error	Description
Traffic Accidents (20)	Traffic accidents can result in temporary partial or full road closures leading to unexpected delay in a network.
Improper Maintenance (21)	Improper maintenance can result in failures that can be catastrophic in some cases (Minnesota Bridge)

2.1.1.6 Generic Events

Although there are many different threats that exist for a transportation network, they can all be summarized by their effects on roadway network links. Thus, a vast amount of research into transportation network vulnerabilities focuses on mimicking the effects of events by reducing the capacity of links, decreasing travel speed, etc. The research in this area has five main focus areas, listed in Table 2. 5.

Table 2. 5 List of Generic Events

Event	Description
Full closure of one link (12)	Studies in this category focus on the effects generated by the closure of a single roadway link
Full closure of multiple links (22)	Studies in this category focus on the effects generated by the closure of multiple roadway links
Partial closure of one link (12)	Studies in this category focus on the effects of closing only part one link (lane closure)
Partial Closure of Multiple Links (12)	Studies in this category focus on the effects of closing only part of multiple links (lane closures)
Increased Traffic Volume (12)	Studies in this category focus on the performance of a network using higher than normal traffic volumes (future traffic growth)

There are also two categories that exist that consider the manner of the attack: random and target attacks. Random attacks (23) mimic unintentional threats and target attacks (24) mimic intentional threats. While differing greatly in manner, these two attacks result in the same effects listed in Table 2. 5.

2.1.2 How likely is it that that will happen?

All of the different events that can happen have an associated likelihood of happening. This likelihood can be expressed in two ways: a time period for occurrence and probability. Time periods for occurrence are usually associated with weather events and earthquakes and can easily be converted to probabilities. For example, a 100-year flood event has an annual probability of 1%. The likelihood of an event can be dependent upon the situation and can vary greatly over time. For example, if a decision maker is trying to protect against an intentional threat, then the probabilities would be associated with the type of attacker and the size of attack while weather events would become increasingly probable as a storm approach. The quantity and accuracy of information available is key to determining the probability associated with a specific threat. Decision makers have a very difficult task to consider all of the different threats and their probabilities while making a decision that will have consequences on the performance of a network.

2.1.3 If it does happen, what are the consequences?

The impact of any event to a transportation system is measured by the impact to the users. The measures of these impacts are typically summed or averaged due to the fact that not all users are impacted in the same fashion and that the decision maker is responsible for the effects on all network users. There are two different types of measures used to evaluate transportation networks: (1) link measures 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 link and network measures have 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, of which travel time and its derivative measure of travel delay, are used in the vast majority of research and practice applications. Accessibility refers to the connectivity of the network and are typically the number of transportation facilities that are within a certain travel radius or time. Reliability is also derivative of mobility in that it is typically a measure of the fluctuations that exist in mobility measures. Resilience measures are usually observed by comparison of mobility before and after events. Link measures of resilience restrict the event to the removal of a single link and reveal the value or importance of that link to the function of the network while network measures of resilience only reveal the impact of damaging a set of links. The key difference is that in calculating link resilience measures, links are fully removed where network measures can evaluate the impacts of the partial removal of links. In an attacker-defender game theory framework, the attacker and defender typically evaluate their decisions using network measures.

2.1.3.1 *Link Measures*

Link vulnerability measures found in the published literature are listed in Table 2. 6 along with function of the measure and the definition of the terms.

Table 2. 6 Link Vulnerability Measures

Measures	Function	Definitions
	Mobility	
Congestion Index (25)	$CI = \frac{t_c}{t_f}$	t_c Is the travel time under congested traffic conditions t_f is the travel time under free-flow conditions
User Lost Time (26)	$tt - t_f$	tt is the travel time t_f is the travel time under free-flow conditions
Travel Time (12)	$t(V,l) = \left[\frac{V}{k_1} + k_2\left(1+\left(\frac{V}{k_3}\right)^n\right)\right] * l + k_4$ if $V \leq \bar{V}$ $t(V,l) = t(\bar{V},l) + k_5(V - \bar{V})$ if $V \geq \bar{V}$	t is the travel time on each link V is the traffic volume on each link $\bar{V}$ is the capacity of each link l is the link length (km) k_i are speed limit and traffic condition dependent parameters n is the polynomial parameter
Travel Time (27)	$S_a(v_a) = t_a\left(1 + 0.15\left(\frac{v_a}{c_a}\right)^4\right)$	$S_a(v_a)$ 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 (12)	$segment\ length$	
Travel Speed (12)	$\frac{segment\ length}{tt}$	tt is the travel time
Travel Rate (28,29)	$\frac{tt}{segment\ length} = (speed^{-1}) - 1$	tt is the travel time
Speed of Person Movement (28,29)	$Passenger\ vol. \times average\ travel\ speed$	
Corridor Mobility Index (28,29)	$\frac{Speed\ of\ Person\ Movement}{Standard\ Value}$	
	Accessibility	
Serviceability (29)	Possibility to use that link/route/network during a given time period	
Accessibility (30,31)	Average travel time to objectives or percentage of objectives within a specified time	
	Reliability	
Delay Rate (28,29)	$(atr - dtr) = \frac{(att - dtt)}{length}$	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 (28,29)	$dr \times people\ vol. \times length$ $= (att - dtt) \times people\ vol.$	att is the actual travel time dtt is the desired travel time
Relative Delay Rate (28,29)	$\frac{dr}{dtr} = \frac{atr}{dtr} - 1$	dr is the delay rate atr is the actual travel rate dtr is the desired travel rate
Delay Ratio (28,29)	$\frac{dr}{atr} = 1 - \frac{dtr}{atr}$	dr is the delay rate atr is the actual travel rate dtr is the desired travel rate
Resilience		
Redundancy Importance (15)	$RI_{flow}(k;l) = (f_k^l - f_k^0)$	*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 (15)	$RI_{impact}(k;l) = \left(\Delta T_k^l - \Delta T^l\right)$	*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 (32,33)	$q_a = c_a - c$ $c = \sum_a t_a x_a$ $c_a = \sum_a t_a x_a \delta_a$	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 (34)	$D_a = \sum_{r,s} M_a^{r,s}$ $M_a^{r,s} = \chi_a^{r,s} V_a^{r,s}$ $\chi_a^{r,s} = \left(\frac{x_a^{r,s}}{q^{r,s}}\right)$ $V_a^{r,s} = \begin{cases} 1.0 & if\ k^{r,s} > K^{r,s} \\ 1.0 - \sum_{j=1}^{k^{r,s}} g_j^{r,s} \frac{X_{a,j}}{x_a^{r,s}} & otherwise \end{cases}$ $g_j^{r,s} = \left(\frac{C_j^{r,s}}{\rho h_j}\right)\left(\frac{T_j^0}{\tau_j}\right)$ $C_j^{r,s} = \min_{l \in L_j} c_l \left(\frac{x_l^{r,s}}{\sum_{r',s'} x_l^{r',s'}}\right)$	D_a is the disruption index of link *a* *r* is the origin index *s* is the destination index $M_a^{r,s}$ 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 $x_a^{r,s}$ 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 (35)	$VUL_a^l = \frac{E_0(G_a) - E_a(G_a)}{E_0(G_a)}$ $E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	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 (23)	$Importance_{net}^{dem}(k) = \frac{\sum_i \sum_{j \neq i} x_{ij}(c_{ij}^{(k)} - c_{ij}^{(0)})}{\sum_i \sum_{j \neq i} x_{ij}}, k \in E^{nc}$	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 (23)	$Importance_{net}^{uns}(k) = \frac{\sum_i \sum_{j \neq i} u_{ij}^{(k)}}{\sum_i \sum_{j \neq i} x_{ij}}, k \in E$ $u_{ij}^{(k)} = \begin{cases} x_{ij} \ if \ c_{ij}^{(k)} = \infty \\ 0 \ if \ c_{ij}^{(k)} < \infty \end{cases}$	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 (36)	$PBC(e) = \frac{\sum_{o \in S_{OD}} \sum_{d \in S_{OD}} E[\lvert N_{ode}(\sigma_0, t_s, \tau_s) \rvert]}{\sum_{o \in S_{OD}} \sum_{d \in S_{OD}} E[\lvert N_{od}(t_s, \tau_s) \rvert]}$	*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 (37,38)	$I^1 = \frac{q}{(1-\frac{q}{C})}$ $I^2 = \frac{1}{T_b}$ $I^3 = I_i^1 * \vartheta(q - 2500)$ $I^4 = I^1 \times q$ $I_i^5 = I_i^2 \times q_i \times \sum I_j^1$ $I_i^6 = I_i^3 \times q_i \times \sum I_j^1$ $I_i^7 = \sum I_j^1$ $I^8 = \frac{q}{C}$ $I^9 = q_i - C_i^b$	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* 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 (32)	$NRI_k = \sum_i t'_i \times v'_i - \sum_i t_i \times v_i$	kIs the link blocked $t'_i$is the travel time of link i when link $k$is blocked 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

2.1.3.2 Network Manager Objectives

2.1.3.2.1 Passenger Network Objectives

The objective functions for a manager in charge of a passenger network found in the published literature are listed in Table 2. 7 along with the function of the objective, the term definitions, and the desired direction of optimization for the objective.

Table 2. 7 Network Manager Objectives for Passenger Networks

Measures	Function	Definitions	Direction of Optimization
		Mobility	
Average Travel Time (12,39)	$\frac{\sum_{i\in O, j\in D} t_{ij}x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	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 (12)	$\frac{\sum_{i\in O, j\in D} d_{ij}x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	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 (12)	$\frac{\sum_{i\in O, j\in D} s_{ij}x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	s_{ij} is the travel speed between node *i* and node *j*	Minimize

		x_{ij} is the demand from node *i* to node *j*	
Congested Travel (28,29)	$\sum(congested\ segment\ length \times people\ vol.)$		Minimize
	Reliability		
L-M Network Efficiency Measure (40)	$E(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}$	*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 (40)	$\varepsilon = \varepsilon(G,d) = \frac{\sum_{w \in W} \frac{d_w}{\lambda_w}}{n_W}$	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 (35)	$E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	*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* 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	Maximize
	Resilience		
Fraction of Satisfied Demand (41)	$\propto = E\left(\frac{\sum_{w \in W} d_w}{\sum_{w \in W} D_w}\right) = \left(\frac{1}{\sum_{w \in W} D_w}\right) \cdot \left(\sum_{w \in W} d_w\right)$	d_w is the post-disaster demand D_w is the pre-disaster demand	Minimize

2.1.3.2.2 Freight Network Objectives

The objective functions for a manager in charge of a freight network found in the published literature are listed in Table 2. 8 along with the function of the objective, the term definitions, and the desired direction of optimization for the objective.

Table 2. 8 Network Manager Objectives for Freight Networks

Measures	Function	Definitions	Direction of Optimization
	Mobility		
Average Travel Time Per Mile (12,39)	$T = \frac{\sum_{i \in O, j \in D} v_{i,j} t_{i,j}}{\sum_{i \in O, j \in D} v_{i,j} l_{i,j}}$	*T* is the average travel time per mile (min/mi) *O* is the set of origins *D* is the set of destinations *i*,*j* is the origin and destination pair $v_{i,j}$ is the average daily truck volume between origin *i* and destination *j*	Minimize

		$t_{i,j}$ is the average travel time between origin *i* and destination *j* $l_{i,j}$ is the link length between origin *i* and destination *j*	
Average Truck Trip Length (42)	$L = \frac{\sum_{i\in O,j\in D} v_{i,j} l_{i,j}}{n}$	*L* is the average truck trip length (mi) $v_{i,j}$ is the average daily truck volume between origin *i* and destination *j* $l_{i,j}$ is the link length between origin *i* and destination *j* *n* is the total truck trips per day	Minimize
Mobility Performance Index (42)	$PI = \frac{\sum_{i\in O,j\in D} \frac{s_{i,j} v_{i,j} l_{i,j}}{FFS_{i,j}}}{\sum_{i\in O,j\in D} v_{i,j} l_{i,j}}$	$s_{i,j}$ is the actual travel speed between origin *i* and destination *j* $v_{i,j}$ is the average daily truck volume between origin *i* and destination *j* $l_{i,j}$ is the link length between origin *i* and destination *j* *n* is the total truck trips per day $FFS_{i,j}$ is the free flow speed between origin *i* and destination *j*	Maximize
	Accessibility		
Percentage of Highway Open to Freight (42)	$L_t = \frac{L_O}{L_T} \times 100\%$	L_t is the percentage of total length of highway that is open to freight traffic in the network L_O is the total length of highway that is open to freight traffic in the network L_T is the total length of highway in the network	Maximize
Availability of Intermodal Terminals (42)	$I_t = \frac{I_O}{I_T} \times 100\%$	I_t is the availability of intermodal terminals I_O is the number of intermodal terminals open to freight traffic in the network I_T is the total number of intermodal terminals in the network	Maximize
Percentage of Freight Travel Below Acceptable Speed (42)	$T_u = \frac{T_U}{T_T} \times 100\%$	Acceptable travel speed = 0.85*speed limit T_u is the percentage of freight vehicles traveling under the acceptable travel speed T_U is the number of freight vehicles traveling under the acceptable travel speed T_T is the total number of freight vehicles in the network	Minimize
	Reliability		

Delay Reliability (42)	$d_{i,j} = v_{i,j} \max\left[\frac{l_{i,j}}{s_{i,j}} - \frac{l_{i,j}}{Acceptable\ Travel\ Speed}\right] \times 60$ $R = \frac{\sum_{i\in O, j\in D} d_{i,j}}{n}$	$d_{i,j}$ is the delay time between origin *i* and destination *j* $l_{i,j}$ is the link length between origin *i* and destination *j* $s_{i,j}$ is the actual travel speed between origin *i* and destination *j* R is the average delay time per trip	Minimize
	Resilience		
MOR (42)	$MOR = \frac{(RI_{before} - RI_{after})(1 + t^{\propto})}{RI_{before}}\%$	RI_{before} is the resilience indicator before a disaster (mobility, accessibility, reliability) RI_{after} is the resilience indicator after a disaster *t* is the total time required to restore the capacity (years) $\propto$ is a system parameter	Minimize
Fraction of Satisfied Demand (41)	$\propto = E\left(\frac{\sum_{w\in W} d_w}{\sum_{w\in W} D_w}\right) = \left(\frac{1}{\sum_{w\in W} D_w}\right) \cdot \left(\sum_{w\in W} d_w\right)$	d_w is the post-disaster demand D_w is the pre-disaster demand	Minimize

2.1.3.3 Intelligent Attacker Network Objectives

2.1.3.3.1 Passenger Network Objectives

The objective functions for an intelligent attackers' intent on disrupting a passenger network found in the published literature are listed in Table 2. 9 along with the function of the objective, the term definitions, and the desired direction of optimization for the objective.

Table 2. 9 Intelligent Attacker Objectives for Passenger Networks

Measures	Function	Definitions	Direction of Optimization
	Mobility		
Average Travel Time (12,39)	$\frac{\sum_{i\in O, j\in D} t_{ij} x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	t_{ij} is the travel time between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Maximize
Average Trip Length (12)	$\frac{\sum_{i\in O, j\in D} d_{ij} x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	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 (12)	$\frac{\sum_{i\in O, j\in D} s_{ij} x_{ij}}{\sum_{i\in O, j\in D} x_{ij}}$	s_{ij} is the travel speed between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Minimize
	Reliability		

L-M Network Efficiency Measure (40)	$E(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}$	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 (40)	$\varepsilon = \varepsilon(G,d) = \frac{\sum_{w \in W} \frac{d_w}{\lambda_w}}{n_W}$	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 (35)	$E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	*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* 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	Maximize
	Resilience		
Fraction of Satisfied Demand (41)	$\propto = E\left(\frac{\sum_{w \in W} d_w}{\sum_{w \in W} D_w}\right) = \left(\frac{1}{\sum_{w \in W} D_w}\right) \cdot \left(\sum_{w \in W} d_w\right)$	d_w is the post-disaster demand D_w is the pre-disaster demand	Minimize

2.1.3.3.2 Freight Network Objectives

The objective functions for an intelligent attacker intent on disrupting a passenger network found in the published literature are listed in Table 2. 10 along with the function of the objective, the term definitions, and the desired direction of optimization for the objective.

Table 2. 10 Intelligent Attacker Objectives for Freight Networks

Measures	Function	Definitions	Direction of Optimization
	Mobility		
Average Travel Time (12,39)	$\frac{\sum_{i \in O, j \in D} t_{ij} x_{ij}}{\sum_{i \in O, j \in D} x_{ij}}$	t_{ij} is the travel time between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Maximize
Average Trip Length (12)	$\frac{\sum_{i \in O, j \in D} d_{ij} x_{ij}}{\sum_{i \in O, j \in D} x_{ij}}$	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 (12)	$\frac{\sum_{i \in O, j \in D} s_{ij} x_{ij}}{\sum_{i \in O, j \in D} x_{ij}}$	s_{ij} is the travel speed between node *i* and node *j* x_{ij} is the demand from node *i* to node *j*	Minimize
	Reliability		

L-M Network Efficiency Measure (40)	$E(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}$	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 (40)	$\varepsilon = \varepsilon(G,d) = \frac{\sum_{w \in W} \frac{d_w}{\lambda_w}}{n_W}$	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 (35)	$E(G) = \frac{\sum_i \sum_{rs} \frac{u_i^{rs} q_{rs}}{\pi_i^{rs}}}{\sum_{rs} q_{rs}}, \forall rs \in RS, \forall i \in I$	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 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	Maximize
	Resilience		
Fraction of Satisfied Demand (41)	$\propto = E\left(\frac{\sum_{w \in W} d_w}{\sum_{w \in W} D_w}\right) = \left(\frac{1}{\sum_{w \in W} D_w}\right) \cdot \left(\sum_{w \in W} d_w\right)$	d_w is the post-disaster demand D_w is the pre-disaster demand	Minimize

2.1.3.4 Real World Examples

Table 2. 11 provides a list of studies of transportation networks that have been used to evaluate the impacts of different types of disruptions. Some of the networks shown in table 12 have experienced real events such as bridge collapse or a terrorist attack and the research of these networks mainly consists of studies of the aftermath of the events. The study of networks that have experienced events can provide three main insights: (i) how big was the impact, (ii) what was the decision maker's response, and (iii) how long did it take for the network to reach an equilibrium after the event.

Table 2. 11 List of Real World Examples

Network	Description
Swedish Road Network (15,22)	This network was used to test the impacts of events that cover large areas (weather)
Stockholm Road Network (12)	This network was used to evaluate the impacts of the closure of select links and bridges
Hat Yai City (14)	This network was used to find critical locations of the network using an accessibility measure

Minnesota Bridge Failure (21,43)	Studies in this category examine the effects of a catastrophic bridge collapse on I-35W
New York City Terrorist Attack (44)	Studies in this category examine the effects of the 9/11 terrorist attack in New York
Washington D.C. Terrorist Attack (44)	Studies in this category examine the effects of the 9/11 terrorist attack in Washington D.C.
Northridge, CA Earthquake (44)	Studies in this category examine the effects of the earthquake in Northridge California

2.1.3.4.1 Impacts of Real-World Events

The impacts of an attack or disruption can be widespread and are not limited to the link or facility that was attacked. Table 2. 12 shows that many types of transportation modes (i.e., road, rail, river, bicycle, pedestrian, and air) were affected by the collapse of the I-35 W Mississippi Bridge in Minneapolis, Minnesota on August 1st, 2007. Also, the effect to road transportation went beyond the collapsed bridge to include a parallel bridge and two roads at the ends of the bridge.

Table 2. 12 Impacts of I-35 W Bridge Collapse on Transportation

Affected Transportation	Effect
River Navigation	Closed near the collapse
Rail	Blocked rail spur
Air	Restricted for 3 nautical miles around collapse
Bicycle	Disrupted a bike path
Pedestrian	Closed a parallel bridge to pedestrians
Road	Closed a parallel bridge to traffic and disrupted two roads

2.1.4 Vulnerability indicators

The value of the vulnerability index will be utilized to quantifying the impact of the disruption on the network and evaluating the system performance. Mattsson and Jenelius (45) divided indices into two distinct traditions and characterized them as topological-based or traffic-based.

Topological-based analyses the transport network and is generally a method for analyzing social network and telecommunication network, however, it is also applicable to the transportation network. In this method, the real network will be presented as a graph with a set of nodes and set of links which can be directed (there are a start and end for each link) or undirected (there is no order between the nodes connected by a link), unweighted (all the links have the same length), or weighted (links have their actual length). The graph's topological characteristics such as the degree of the distribution, cluster, centrality measures, and efficiency are used to rank the nodes and links in the network.

In most of the studies in the literature, transport network is modeled in graph theory as a set of links and nodes, and a vulnerability index is defined, and the network is analyzed against that index. This type of measures is called traffic-based, and the procedure is commonly includes removing a link (node) or a set of links (nodes) from the network and then measuring the network characteristics.

2.1.4.1 Topological-Based Analysis

Network topology is the general topic relating to the structure and connections in a network (of nodes and links), with the form, shape, and connectivity of a particular network affecting the ease of movement through it, the potential for alternative paths between nodes, and the vulnerability of the network in the face of loss or degradation of some parts. Vulnerability analysis is concerned in large part with identifying those components or regions within a network where failure or degradation will have the most important effects.

Network topology is concerned with the structure of a network, especially the connections between the nodes. The existence of a link between node *i* and *j* is the basic knowledge in topological case that is required, and is identified in the incidence matrix $\Delta = [\delta_{ij}]$ which:

$$\delta_{ij} = \begin{cases} 1 \; If \; link \; a_{ij} \; exists \; in \; the \; network \\ 0 \; otherwise \end{cases}$$

Particularly, there are three main measures for identifying a network, the average geodesic distance, the clustering coefficient, and the degree distribution.

The geodesic path or shortest path between two nodes in a graph is a path with the minimum number of links for traveling between the two nodes. The length of this path is called the shortest path.

The clustering coefficient can be used to measure the robustness of a network, which is assessing the extent that the nodes of the network are forming a small, tightly connected group. The extent that this coefficient increases can show a lower average travel distance and fewer number of legs.

The degree distribution is defined as the probability distribution of the degree of nodes in a network. The degree of nodes or connectivity will be defined as the number of connections that a node has to the other nodes.

Topological based in transportation network analysis considers the network structure and connectivity. It represents the transport network in the form of a graph with a set of nodes (vertices) and a set of links (edges). It mainly considers two main aspects of the network structure: network efficiency and node centrality. This analysis can provide a good understanding of the network structure and its connections but fails to account for the behavior of the user. There are several studies that evaluate network vulnerability using topological-related factors; however, only a few numbers have been published in transportation-focused journals. For example, an accessibility index based on distance-only and distance-traffic volume criteria is defined by Sohn (46). Demsar et al. (47) studied the urban street network of the Helsinki Metropolitan Area in Finland defining links with the high value of betweenness and cut links as more critical ones. By taking into account the alternative links, a topological indicator is presented by Knoop et al. (24). In another study, degree and betweenness centrality indicators for six real city road networks with simulating attacks with remaining nodes was calculated (48). Table 2.13 summarized the topological based measures presented by researchers for assessing the roadway network.

Table 2. 13. Topological-based Vulnerability Measures

Ref.	No. of degraded components	Approach	Indicator(s) to capture consequences	Method	Conclusions
(49)	Network	Distance	Network efficiency Global and Local efficiency	-Shortest path -Weighted and unweighted network	Global efficiency is a measure of the directness of the connections between all node pairs, however, local efficiency indicates the average directness of the connections between the neighbors of a node.
(46)	Single link	Distance & flow	Accessibility index	-Shortest path -Distance-traffic volume indicated a link with heavy traffic (efficiency-oriented)	These two criteria give accessibility loss to completely different links
(50)	Nodes	Distance	-Degree distribution -Degree correlations -Clustering coefficient	-A dual graph is presented -A comparison between primal and dual graph	A complex network approach to the urban street networks has advantages with compare to syntax formalism

(51)	Single link	generalized cost	Accessibility measure	Analyzing the network vulnerability in terms of topological configuration and socio-economic impacts	more efficient algorithm for applying on large network is needed and calculating sets of critical links is needed.
(47)	Single link	Shorter Distance	-Cut vertices measure, -Betweenness measure, clustering coefficient measure	-Combining dual graph modeling with connectivity analysis and betweenness and clustering coefficient -Undirected and unweighted network	Links with the high value of betweenness and cut links are more critical ones. locations have one or more of the following three properties: • Cut links • High betweenness • Low clustering coefficient
(48)	Nodes	Shorter Distance	-Betweenness centrality -Degree of Distribution	-undirected graph -choose three types of road granularities, -four successive attack strategies applied	Topological structure such as betweenness centrality distribution is more essential to the robustness of a network that geographical features of the network. the robustness pattern was quite similar for different cities
(52)	Nodes	Shorter Distance	Betweenness centrality	Developed an algorithm for computation of BC for real-time	Prove the existing a significant correlation between global efficiency and BC. Ranking Nodes based on their metric

2.1.4.2 Traffic-Based Analysis

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

The first group of studies concentrates on evaluating the effects of events (e.g., economic impacts of Earthquake or floods disruption on the road network) utilizing an integrated transport network and multiregional trade models (53–55).

The second category proposes metrics and indices for assessing vulnerability. Most of these studies provide indices based on travel time, flow, or generalized costs due to link failures. A full-scan analysis of the network will be performed by removing links one-by-one and recalculating the performance measure in each step and ranking the links based on the changes in the selected measure. Such indicators need to take traffic assignment flow into account, which makes them more detailed and so true to the nature of the road network dynamic, However, with less widely applicability for big networks. High computational time due to performing multiple traffic assignments and dis-connectivity that might happen during removing the links in the network are the most important concerns for applying these indicators to evaluate the large-scale transportation network. A game theoretic technique for assessing the transportation network vulnerability started by Bell (58) which proposed a mixed strategy non-cooperative game which in on hand, the network user is attempting to find the paths with minimum travel costs and on the other hand, an attacker which seeking to maximize the cost of these paths. The game theory technique for assessing the vulnerability of the transportation network was continued by some researchers. MurrayTuite and Mahmassani (34) by developing a bi-level formulation and considering four different game scenarios between an attacker and the traffic management agency tried to identify the most vulnerable links in the network. To evaluating the vulnerability of a system Lownes (59) adopted a mixed-strategy stochastic game-theoretical and applied heuristic to solve levels of the problem. Their method was designed to incorporate all O_Ds in a computationally efficient manner for a small network such as Sioux Falls.

Yates and Sanjeevi (60) developed the shortest path network interdiction problem and modeled the network as a two-players game for analyzing attacks on critical infrastructure. The model was applied to a subset of the California highway network. Wang et al. (61) presented a global optimization framework for identifying the most combination of critical links and concluded that the crucial combination of vulnerable links is not necessarily connected or even placed in neighborhood of each other. Higgs et al. (2) identified vulnerable routes in a network using a multi-level multi-objective framework. To tackle the problem of dimensionality, each level was converted to a single objective by using the weighted sum method with weight determination based on heuristic methods. Candelieri et al. (62) evaluate the performance of bus network in Florence, Italy, and the transportation network in the Attika region, Greece under targeted attack. Their analysis implements a topological approach based on graph theory and analyze vulnerabilities with respect to the removal of one or more of their components for simulating the direct attack and cascading failure. In order to finding the most important sets of links which lost of them will create the worst user equilibrium congestion for Sioux Falls and Berlin roadway network, Starita (63) formulate a game theoretical model as bi-level problem. They formulated their model via a customized version of Greedy Randomized Adaptive Search Procedure (GRASP) meta-heuristic.

give a summary of the presented indicators based on this analysis. Based on (56,57), the proposing ranking measures utilizing this method is called traffic-based vulnerability measures. The traffic-based measures can accurately recognize critical links in the network but calculating them require to conducting traffic assignment under all disruption links scenarios which make them be computationally infeasible for applying on large scale real road network.

The last group of traffic-based vulnerability analysis adopts a game-theory approach for identifying the most critical links under worst-case scenarios. A game theoretic technique for assessing the transportation network vulnerability started by Bell (58) which proposed a mixed strategy non-cooperative game which in on hand, the network user is attempting to find the paths with minimum travel costs and on the other hand, an attacker which seeking to maximize the cost of these paths. The game theory technique for assessing the vulnerability of the transportation network was continued by some researchers. MurrayTuite and Mahmassani (34) by developing a bi-level formulation and considering four different game scenarios between an attacker and the traffic management agency tried to identify the most vulnerable links in the network. To evaluating the vulnerability of a system Lownes (59) adopted a mixed-strategy stochastic game-theoretical and applied heuristic to solve levels of the problem. Their method was designed to incorporate all O_Ds in a computationally efficient manner for a small network such as Sioux Falls.

Yates and Sanjeevi (60) developed the shortest path network interdiction problem and modeled the network as a two-players game for analyzing attacks on critical infrastructure. The model was applied to a subset of the California highway network. Wang et al. (61) presented a global optimization framework for identifying the most combination of critical links and concluded that the crucial combination of vulnerable links is not necessarily connected or even placed in neighborhood of each other. Higgs et al. (2) identified vulnerable routes in a network using a multi-level multi-objective framework. To tackle the problem of dimensionality, each level was converted to a single objective by using the weighted sum method with weight determination based on heuristic methods. Candelieri et al. (62) evaluate the performance of bus network in Florence, Italy, and the transportation network in the Attika region, Greece under targeted attack. Their analysis implements a topological approach based on graph theory and analyze vulnerabilities with respect to the removal of one or more of their components for simulating the direct attack and cascading failure. In order to finding the most important sets of links which lost of them will create the worst user equilibrium congestion for Sioux Falls and Berlin roadway network, Starita (63) formulate a game theoretical model as bi-level problem. They formulated their model via a customized version of Greedy Randomized Adaptive Search Procedure (GRASP) meta-heuristic.

Table 2. 14. Traffic-based Transport Vulnerability Measures

Ref.	Single	Approach	Indicator(s) to capture consequences	Method

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

(67)	Single	Generalized Cost	Accessibility Index	Deprivation cost and logistics cost Optimization-based, Find the worst-case scenario

2.1.4.3 Hybrid Analysis

Topological models do not consider traffic flow dynamics and fail to capture the non-linearity performance function on transport systems, so they do not necessarily present realistic results for transportation planners. However, as shown previously, most of the literature has been conducted using only traffic-based factors, ignoring the topological character of the system. The importance of network structure in evaluating the performance of a network is undeniable. Also, traffic assignment is costly to perform on large networks, especially when it is needed to perform traffic assignments multiple times for each link. A few studies have been published trying to incorporate traffic assignment characteristics (e.g., flow, travel time, etc.) into existing topological measures (e.g., centrality measures, efficiency, etc.) and develop new criteria which could be called hybrid measures. These approaches try to reduce computational and time requirements while retaining accuracy in ranking the critical links in transportation networks.

A simulation-based criticality measure called Stress Test Criticality developed to capture the effect of day-to-day disruptions (i.e., reduced link capacity instead of removing the link from the network) was proposed by Gauthier et al. (68) and considered four different link criticality measures based on Betweenness-Centrality i.e., Unweighted BC, Travel-time weighted BC, unweighted BC on entry/exit nodes only (BC entries–exits), and Travel-time weighted BC from entry to exit nodes only. Results of their study suggested that the proposed measures adequacy is highly variable. A Link Criticality Index proposed by Almotahari and Yazici (57) is based on the link marginal cost and utilizing the convex combination solution of the UE problem. They compared ranking links using their proposed measure, three existing traffic-based measure (23,32,33), and one hybrid measure (68) with UE link flow. While ranking links using their proposed index had a very low correlation with the UE link flows (correlation = 0.2), the other measures were outperformed better by showing correlations ranged from 0.31 (for the hybrid measure) to 0.9 (for the traffic-based measures). Li et al (69), proposed an approach which by considering traffic flow betweenness index is able to identify the critical links in large scale network. The traffic flow betweenness index is calculated based on traffic flow betweenness and rerouted travel demand. The proposed index performed better in identifying critical facilities (e.g., bridges) when compared to the Hansen accessibility index. Takhtfiroozeh et al. (1) proposed nine new criticality measures for roadway network by combining characteristics of traffic equilibrium and network topology proposed. They evaluated their hybrid measures with three existing traffic-based measures using three case study transportation networks from the literature. three out of the nine proposed measures showed very promising results compare with the traffic-based measures and the authors concluded that these measures can be utilized by planners and decision makers as reliable ranking measures for ranking links in large-scale road network, where due to computational burden applying the full-scan analysis is infeasible.

2.2 GAME THEORY

The variety of choices available to network users and decision makers creates a game where each side tries to choose the optimum choice based on their own objectives. Game theory models are specifically designed to solve these situations by finding equilibriums. There are two main components considered by game theory models which are discussed in this section: the players and the formulation. The players are the different viewpoints of the game each with their own objective. The formulation is how the game is arranged which includes who goes first, how many moves can that player make, etc.

2.2.1 Players of the Game

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

2.2.1.1 Decision Makers

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

2.2.1.2 Intentional or Unintentional Threats

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

2.2.1.3 Network Users

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

2.2.2 Game Theory Formulations

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

Attacks on transportation networks are primarily sequential games and thus the focus of this section is the various formulations of sequential games. The majority of the formulations focus on the dynamics of the interactions of an attacker and a defender. Two large areas of interest in these interactions are: attacker-defender and defender-attacker-defender games. Attacker-defender games represent cases where the actions of the attacker are not anticipated, and the defender can only respond after the attack. Defender-attacker-defender games represent cases where the actions of the attacker are anticipated, and the defender can take preemptive actions as well as respond after the attack.

2.2.2.1 Attacker-Defender

Attacker-defender is a hierarchical game, where an attacker attempts to damage a network and a defender attempts to thwart the attacker. Attacker-defender can be a zero-sum game when the attacker and defender have opposite views of changes to the performance of a network where the benefit to the attacker is the detriment to the defender or vice versa (58).

2.2.2.1.1 Attacker-Defender Example

Consider a transportation network consisting of two nodes and two links connecting the nodes with link 1 having twice the capacity of link 2. In an attacker-defender game, the attacker would decide to attack link 1 or link 2 depending on the impact of the attack. Also, the defender will choose a response to the action of the attacker. Figure 2. 2 shows the impacts of the actions of the attacker and defender on the capacity for each link. Given this framework, the attacker assigns unequal probability to the actions of the defender thus the expected outcome for choosing link 1 is (-500*1+-1000*0 =-500) and the expected outcome for choosing link 2 is (-500*0+-200*1=-200). In this case, the defender always chooses the same link as the attacker because the defender knows the action of the attacker when making their decision.

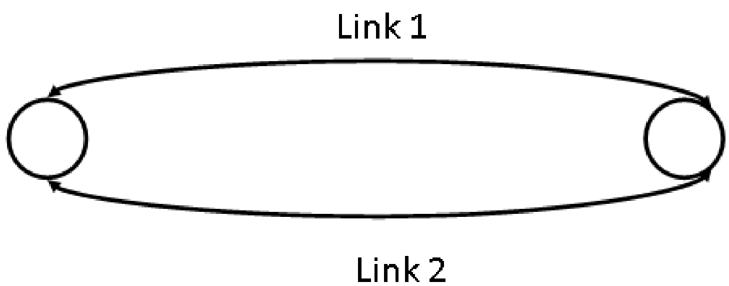


Figure 2. 1 Example Network

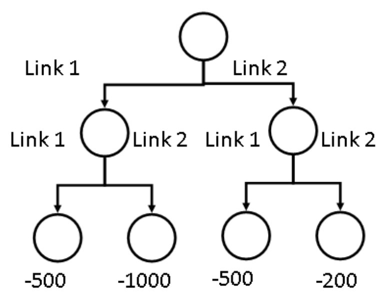


Figure 2. 2 Game Theory Tree for Example

2.2.2.2 Defender-Attacker-Defender

Defender-attacker-defender games are three level hierarchical games that begin with the defender choosing an investment in the network. On the next level, the attacker sees the investment of the defender and then chooses a method of attack. On the last level, the defender sees the actions from both previous levels and then chooses how to operate the system (39). This presents a game where the decision maker is allowed two actions: one preemptive action and one reactive action. The preemptive action is a decision that occurs with minimal information about the attacker. The reactive action is a decision based on a survey of the effects of the attacker's action. The optimal strategy in this game would be for the decision maker's preemptive action to force the attacker to an action with a minimal impact or an impact that can be easily countered by the decision maker's reactive action.

2.2.2.2.1 Defender-Attacker-Defender Example

Consider the same network used in the Attacker-Defender example, in a defender-attacker-defender game the tree becomes larger as shown in Figure 2. 3. In this case, the defender must decide which link to fortify without knowing the intention of the attacker thus there is a 50% probability that the attacker will attack link 1 or link 2. Also, the defender responds to the action of the attacker which would be to fortify link 1 if link 1 was attacked or link 2 if link 2 was attacked. The expected value of this game is -250 for link 1 (0*0.5*1+-200*0.5*0+-1000*0.5*0+-500*0.5*1) and -100 for link 2 (-200*0.5*1+-500*0.5*0+-300*0.5*0+0*0.5*1).

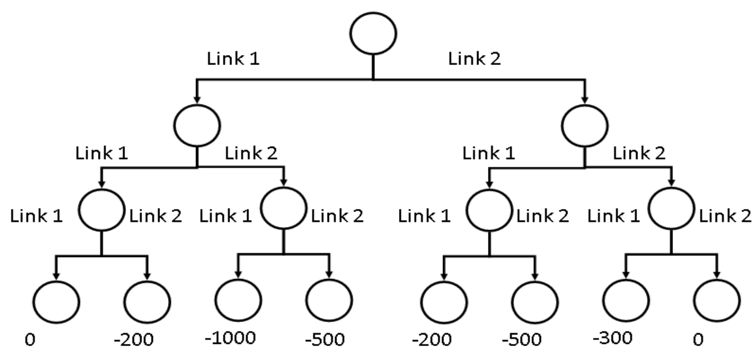


Figure 2. 3 Defender-Attacker-Defender Game Example

2.2.3 Nash Equilibrium

Another important type of games, especially in transportation, are Nash equilibrium games. Nash equilibrium games are sequential games in which each player knows the other's strategy and the equilibrium is reached when neither can improve its outcome by changing strategies. In transportation, a good example of a Nash equilibrium is how traffic is assigned to a network with multiple route choices. In Figure 2.4 we present a simple example of such a case with three route choices (ABD, ACD, and ABCD). If 100 vehicles were to travel from A to D, then the Nash equilibrium would be for 25 vehicles to use ABD, 25 vehicles to use ACD, and 50 vehicles to use ABCD resulting a travel time of 3.75. It is interesting to note that if BC was removed, then the new Nash equilibrium would be to evenly split the traffic between ABD and ACD resulting in a travel time of 3.5 which is lower than the network with link BC. This also shows that if the users made an agreement to not use the link BC (cooperative game) then they could experience a lower travel time.

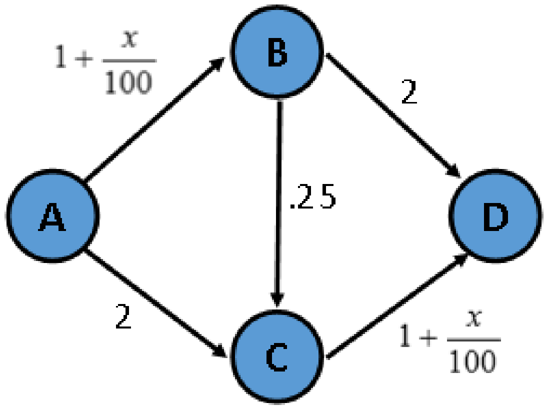


Figure 2. 4 Nash Equilibrium Example Network

3. DATA COLLECTION

This section summarizes the task of collecting and compiling all the necessary data needed to develop the testbed network. The final testbed location was selected in consultation with Florida DOT and local transportation agencies. The Broward County was chosen as the site to develop the project because of its significance on the freight scenario. A snapshot of the network can be seen in Figure 3.1. This county was chosen due to its significance in the freight scenario, with Port Everglades, Fort Lauderdale International Airport, I-95, Florida Turnpike, I-595, and an important commercial travel district.

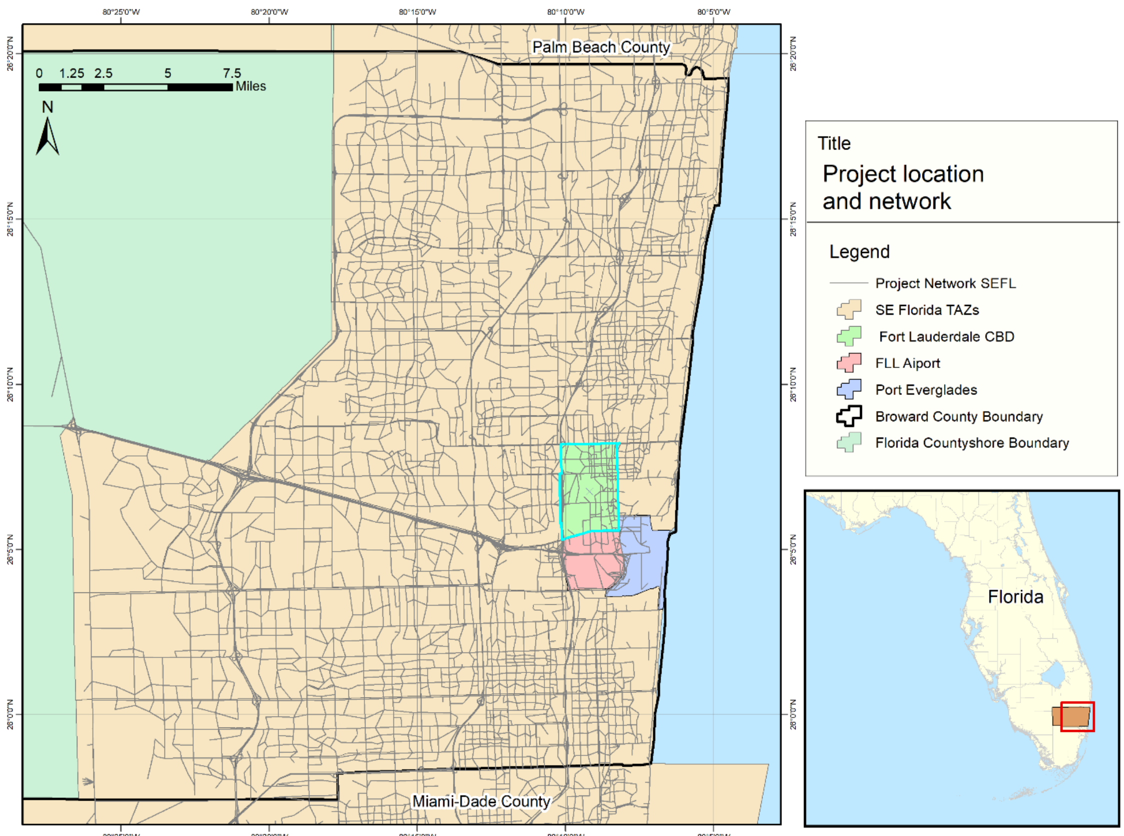


Figure 3. 1. Project location and network.

By the project specification, data must include the network, geometry, network supply elements, passenger and freight demand, and other crucial information. The stakeholders involved in this task were the Broward Metropolitan Planning Organization (Broward MPO) and the Florida Department of Transportation (FDOT).

The main network geometry is a subset of the Southeast Florida Regional Planning Model Version 8 (SERPM 8). This is an activity-based model that has become the state of the practice in travel demand forecasting in the largest U.S. metropolitan areas. This type of model is preferred in such areas because it is grounded in an explainable modeling framework that simulates how discrete travel decisions are made, as opposed to being only a mathematical construct reflecting aggregate regional characteristics of travel. The behavioral grounding and disaggregate nature of the activity-based modeling framework allows a variety of additional questions to be tested and for additional detail to be available to decision-makers working with the model output.

This dataset can comprise information for parts of the day or for the entire day. Data from the loaded network with daily values was selected. Important information from this dataset for the toolbox are the georeferenced network geometry, road characteristics, capacity, and free flow speed.

3.1 DEMAND DATABASE

Personal and commercial demand was estimated using the assigned flows provided by Broward MPO and SE Florida through a well-known Origin Destination Matrix Estimation (ODME) procedure. The TransCAD software (https://www.caliper.com/) was used to implement the ODME procedure. The OD achieved for two different travel district system, car and truck trips based on the zip code. There are 1653 origins-destinations for Broward County demand estimation. As will be discussed, in this project we utilized the most common objective used y MPOs, US-DOTs, 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).

4. METHODOLOGIES FOR RANKING CRITICAL AND VULNERABLE LINKS AND PATHS

In this chapter we present the mathematical formulation and explanation of the developed and implemented methodologies for identifying the critical links and routes in the roadway network that can assist decision makers in identifying and ranking vulnerable and critical links and routes of the roadway network. The presented methodologies will help decision makers with formulating an optimal investment plan to maximize network resilience against attacks on the network. Given the complexity of the problem, two methods have been applied for identifying the critical individual links, path, and the most critical combination of critical links:

First approach by considering topological and demand/supply characteristics of the network, rank the links and paths based on their criticality (Three hybrid measures developed by Takhtfiroozeh and Golias (1)). The hybrid analysis is able to rank links and paths in a real size network with very low computational complexity and high accuracy.

Second approach by using game theory framework and considering the worst-case scenario, identify the most critical combination of critical links in a roadway network with focusing on both day-to-day and major disruptions (Modifying game theory framework presented by Higgs and Golias (2) using hybrid measures presented by Takhtfiroozeh and Golias (1)).

The heuristic algorithm 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). Next, the nomenclature and formula for each methodology will be explained.

4.1 HYBRID MEASURES BASED ANALYSIS

Three hybrid measures (1) have been used in this project for ranking links and routes under passenger, truck, and combination demand data. These measures are variant of the link Betweenness Centrality (BC) introduced by Freeman (70). For a link, the value of BC expresses the frequency the link falls on the shortest paths connecting pairs of nodes Equation 1. Links with high betweenness centrality values represent a bridge-like connector between different parts of a network, a failure of which will affect the communication between multiple pairs of nodes through the shortest path.

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

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

For calculating the shortest paths in a network, and to no longer treat links as binary interactions, weights can be used thus adding another dimension of heterogeneity to the network beyond the topological effects. An edge-weighted graph is a pair of *(G,w)*, where *G=(V,E)* is a graph with a set of Vertices *(V)* and a set of Edges *(E)*, and *w:E⟶R* is a weight function, often referred to as the “cost” of the edge. Therefore, the three hybrid measures rank links and paths by considering two fundamental network factors in analyzing link and path criticality, I) centrality and II) traffic characteristics. Next, a brief description of the hybrid measures is presented follow by their nomenclature, and formula in Table (4.1).

4.1.1 Link Hybrid Measures:

1) Flow Weighted BC ($\boldsymbol{BC}^*$)

Based on the social efficiency perspective, roads with more demand serve more people and thus generate higher social and economic benefits, hence, need to be considered more significant. BC^* by considering social efficiency in its calculation, rank links based on their centrality and link's flow. So, if a link has more demand and is simultaneously more central, it will be recognized as more important the others. BC^* is calculating based on the product of the BC and link’s flow.

2) Flow Weighted Free Flow Travel Time BC ($T_{ff}BC^*$)

The UE principle assumes that users will always choose the shortest path from their origin to their destinations, irrespective of the type of the link (e.g., highway, arterial, collector etc.). To capture the UE principle in an uncongested network, Free Flow Travel Time (FFTT) was considered in this $T_{ff}BC^*$ as an edge weight when computing the shortest path used in the calculations of BC. $T_{ff}BC^*$ consider social both efficiency effect and uncongested conditions in identifying critical links.

3) Flow Weighted Congested Travel Time BC (T_cBC^*)

Congested travel times calculated using BPR function (which are a function of FFTT, link utilization i.e., volume to capacity ratios, and class e.g., collector, arterial, etc.) are better indicators of shortest paths under congested conditions. Congested travel time was considered in this T_cBC^* as an edge weight when computing the shortest path used in the calculations of BC. T_cBC^* consider social both efficiency effect and congested conditions in identifying critical links.

Table 4. 1. Proposed Hybrid Ranking Measures by Takhtfiroozeh et al. (1)

Hybrid Measure's Name and Abbreviation	Link Weight for BC Estimation	Formulation	Description
Flow Weighted BC ***(BC*)***	Flow (F_a)	$BC^*{}_a = F_a * BC_a$	BC_a = Betweenness Centrality of link *a* F_a=Flow of link *a*
Flow Weighted Free Flow Travel Time BC (***T_{FF}BC****)	Free Flow Travel Time (T_a^{FF}) and Flow (F_a)	$T_{FF}BC_a{}^* = F_a * (w_a BC_a)$ $w_a = T_a^{FF}$	$T_a^{FF} = \frac{L_a}{FFS_a}$ FFS_a=Free Flow Speed of link *a* L_a=Length of link *a*
Flow Weighted Congested Travel Time BC (***T_CBC****)	Congested Travel Time (T_a^C) and Flow (F_a)	$T_cBC_a{}^* = F_a * (w_a BC_a)$ $w_a = T_a^C$	$T_a^C = T_a^{FF}\left[1 + \alpha(\frac{F_a}{C_a})^\beta\right]$ C_a=Capacity of link *a* α & β =Model parameters

4.1.2 Identifying Critical Routes:

In order to identify and rank routes in a network based on their criticality, first all the possible routes between all the origins and destinations achieved by utilizing the Slope-Based Path Shift Propensity Algorithm (SPSA) (71). Then, the criticality of each path calculated by multiplying the demand value (passenger, freight, and combined) for the OD of the path into summation of the each of the three hybrid measures value for all of the links on that path. So, all the possible existing routes in the network ranked based on three different hybrid measures and for three different demand data.

4.2 HEURISTIC ALGORITHM

In this sub-section we present the methodology developed based on game theory framework to help decision makers with formulating an optimal investment plan to maximize network resilience against attacks on the network. In order to recognizing the most critical combination of critical links in a roadway network, a subcase of the optimization model and a solution algorithm developed by Higgs et al. 2017 (2) has been used. The solution algorithm has been modified by considering the worst-case disruption scenario by considering topology characteristics and focusing on both day-to-day and major disruptions. A worst-case scenario is identifying the most critical sets of links with respect to a specific performance criterion, and it is modeled as a game between three players.

The upper level (designer) are public entities responsible for the maintenance and operation of the network and optimization of the benefit of the users. The second level (Attacker) can be defined as anything (or anyone) that can have a negative impact on network performance, which will be divided into two main groups: intelligent and unintelligent. The upper-level player (designer) minimizes the objective within the constraints of the total number of links that can be defended. The second level player (attacker) maximizes its objective function (which in this project is considered the same as the defender's). Since both first and second level objective function are the same, we use a minmax reformulation to reduce the problem from a three level to a bilevel optimization problem. The inner level is road users which their behavior and their routing decision in a congested network modeled based on User Equilibrium (UE) assignment model based on the first Wardrop principle (1952) (72). Based on the assumption in Wardrop's first principle, travelers always choose the path with the least travel time, which is calculated through the Bureau of Public Roads (BPR) function. These equilibrium constraints can guarantee that no user can improve their travel time by unilaterally changing routes.

The proposed mathematical formulation assumes multiple objectives for both the decision maker and the attacker 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.

4.2.1 Nomenclature

Set	**Description**
A	Set of links
N	Set of nodes
R	Set of origins
S	Set of destinations
K_{rs}	Set of paths between origin r and destination s

Parameters

Cr_a	Capacity reduction (percentage) of link $a \in$ A (if attacked)
C_a	Link $a \in A$ capacity

Variables

x_a	Traffic flow on link $a \in$ A
y_a	Binary decision to either do nothing (0) or attack link $a \in$ A
z_a	Binary decision to either do nothing (0) or protect link $a \in$ A
$F(x, y, z)$	Defender and Attacker objective function (total network cost)
B^d	Number of links that can be attacked
B^p	Number of links that can be protected
$t_a(x, y, z)$	Link travel time function (BPR function)
q_{rs}	The demand for travel from origin $r \in R$ to destination $s \in S$
F_k^{rs}	The traffic volume for path $k \in Krs$ between origin $r \in R$ to destination $s \in \ S$

δ_a^{krs} The binary path incidence for link $a \in$ A if it belongs to path $k \in Krs$ between origin $r \in R$ to destination $s \in S$ (1) or not (0)

4.2.2 Mathematical Model:

$$\min_{x,y,z}\max\{F(x,y,z)\} \quad \text{(Equation 2)}$$

s.t.

$$\sum_a y_a \leq B^d \quad \text{(Equation 3)}$$

$$\sum_a z_a \leq B^p \quad \text{(Equation 4)}$$

$$\min_x \sum_a \int_0^{x_a} t_a\,(x,y,z)dx \quad \text{(Equation 5)}$$

s.t.

$$\sum_k f_k^{rs} = q_{rs} \quad \forall\, r\; R \; and \;\; s \in S \quad \text{(Equation 6)}$$

$$f_k^{rs} \geq 0 \qquad \forall\, k \in k_{rs}, r \in R, s \in S \quad \text{(Equation 7)}$$

$$x_a = \sum_{k,r,s} \delta_a^{krs} f_k^{rs} \quad \forall\, a \in A \quad \text{(Equation 8)}$$

The equations (2) through equation (4) represent the upper level of the problem (i.e., designer). The first sets of constraints (Eqs. 3 and 4) limit the number of links which can be attacked and protected to a fixed number, while the remaining sets of constraints (Eqs. 5 through 8) formulate the inner level of the problem as the form of classical user equilibrium (i.e., model the behavior of the network users).

4.2.3 Solution Algorithm:

The network interdiction problem is classified as NP-hard problems and there is no exact solution for that. The proposed algorithm in this paper, is a customize version of Greedy Search Algorithm to find the local optimum solution in each stage. In every iteration of the algorithm, a link or a subset of the links is selected based on the three hybrid measures (i.e., $BC^*,\ T_{ff}BC^*, and\ T_cBC^*$) to be attacked. These three hybrid measures proposed by Takhtfiroozeh et al. (2021) rank links not only by their centrality value, but also consider traffic equilibrium inputs and output in calculating the BC of a link. Therefore, links with higher hybrid measures value (i.e., the more critical links to the network) are more likely to be attacked by the adversary and this can a be representer for the intelligent attacker. The links that are selected to be attacked will have their capacity reduced (by a predetermined percentage) and the total cost of the new network is estimated using a shortest path assignment as opposed to a user equilibrium. The algorithm stops when a predetermined number of iterations (that depends on the network size and computing power) is reached. In this project, three different capacity reductions of 100%, 80% and 60% for any link that was compromised and three cases of different number of links that could be compromised i.e., 10, 20, and 30 links.

5. CRITICAL LINKS AND ROUTES IDENTIFICATION

In this section, we present a sample of the results (Figures 5.1 through 5…) obtained from presented methodologies (hybrid measures and game theory framework) to showcase their capabilities in identifying critical links and routes. The rest of the figures, ArcGIS toolbox and MATLAB codes for generating more figures can be downloaded from "most probably a dropbox link".

In this project, Broward County located in the state of Florida was used as a case study for the numerical examples. The tested network consists of 16459 links, 1653 pairs of ODs, and 7548 connectors.

5.1 INDIVIDUAL CRITICAL LINK

Figures 5.1 through 5.9 present the top 5%, 10%, 15%, and 20% important links identified by each one of the three hybrid measures. The critical links recognized for three different demand data, i.e., truck, passenger, and combined demand. In these figures, the road classification of the identified critical links showed by using two different colors. The top critical links which are arterial are shown by red color, and the critical links which are non-arterial, have been shown by green. As seen in these figures, the majority of the identified critical links are arterial links. These links carry more flow than non-arterial links, so disrupting them have a more negative cost effect on the network. Also, these figures show that central links (i.e., links that belong to a higher number of shortest paths between ODs) are more critical than the others. So, if a link has more demand and is simultaneously more central, it is a more critical link than the others. On the other hand, attacks concentrated around origins and destinations with a high amount of demand in a way that would effectively isolate that origin or destination (i.e., a bridge).

Besides centrality and social efficiency, $T_{ff}BC^{*},\ and\ T_{c}BC^{*}$ consider travel time shortest path (uncongested and congested situations) in their calculation to find the most important links in the network. Based on $T_{FF}BC^*$ and $T_{C}BC^*$ (Figures 5.4 through 5.9), links which are more central as compared to the others, and simultaneously have higher demand and more travel time required to commute on them (for both congested and non-congested situations), are more important than the other links.

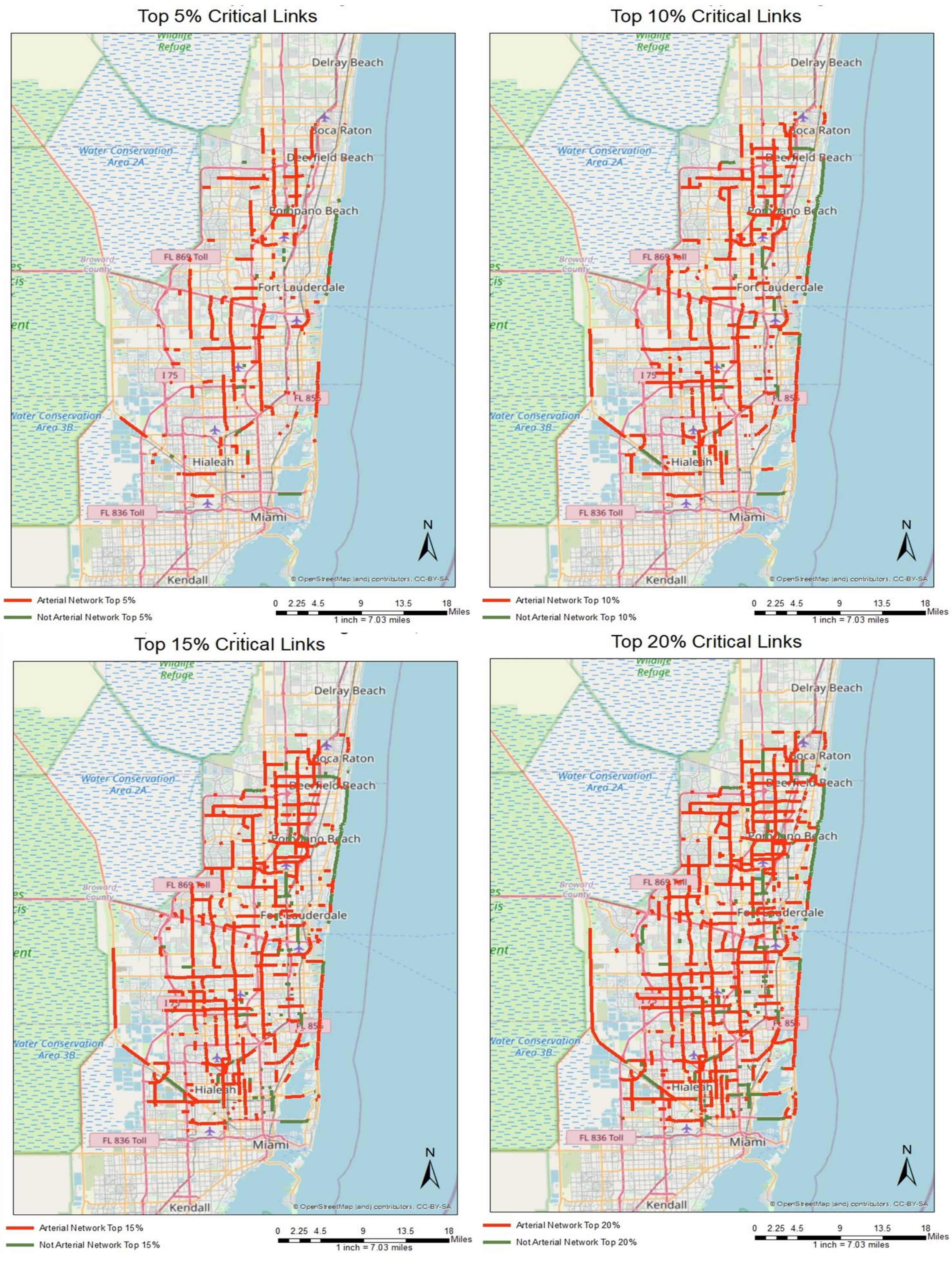


Figure 5. 1 Critical links identified by the BC^{*} hybrid measure (Passenger Demand Only)

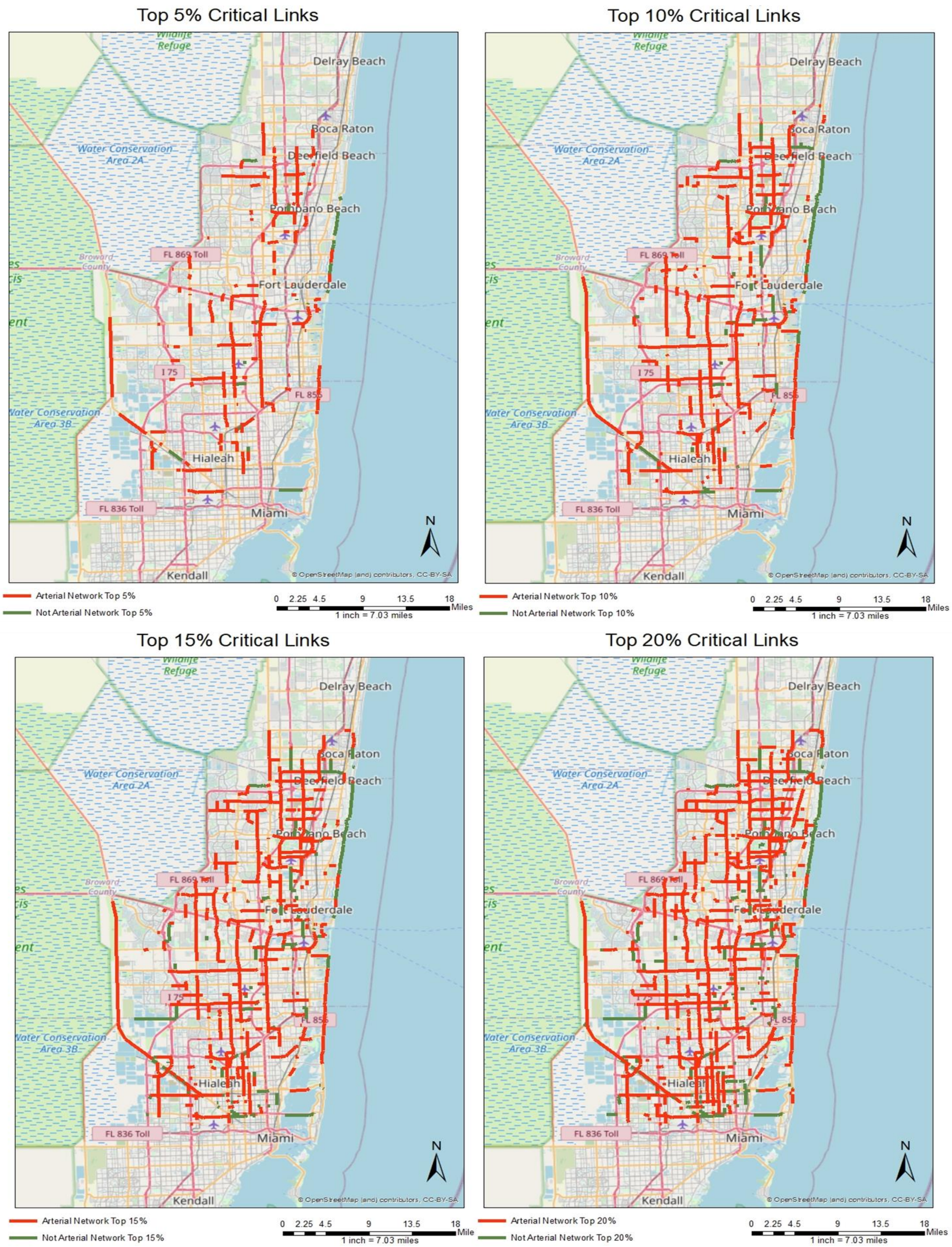


Figure 5. 2 Critical links identified by BC^* hybrid measure (Truck Demand Only)

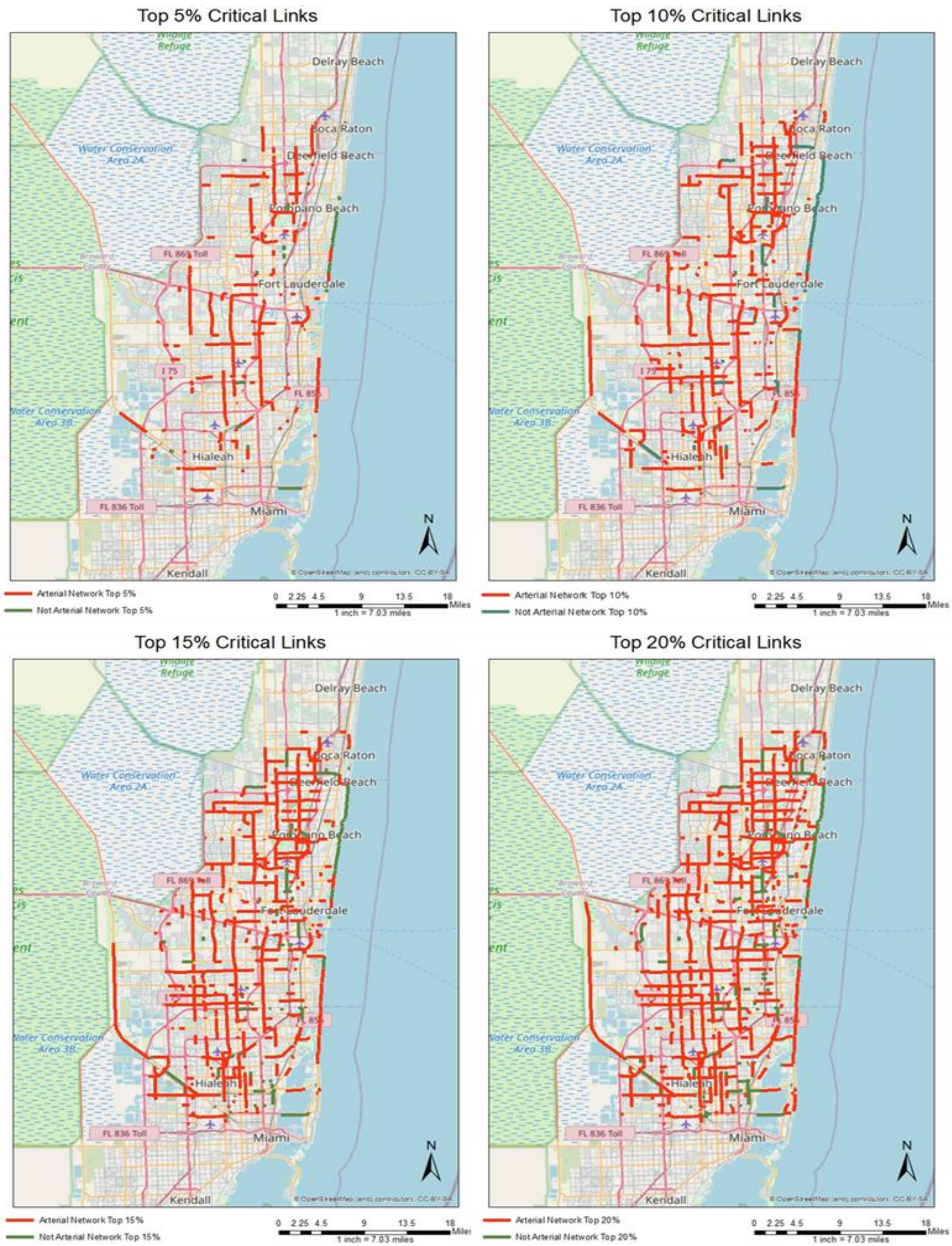


Figure 5. 3 Critical links identified by BC^{*} hybrid measure (Combined Demand)

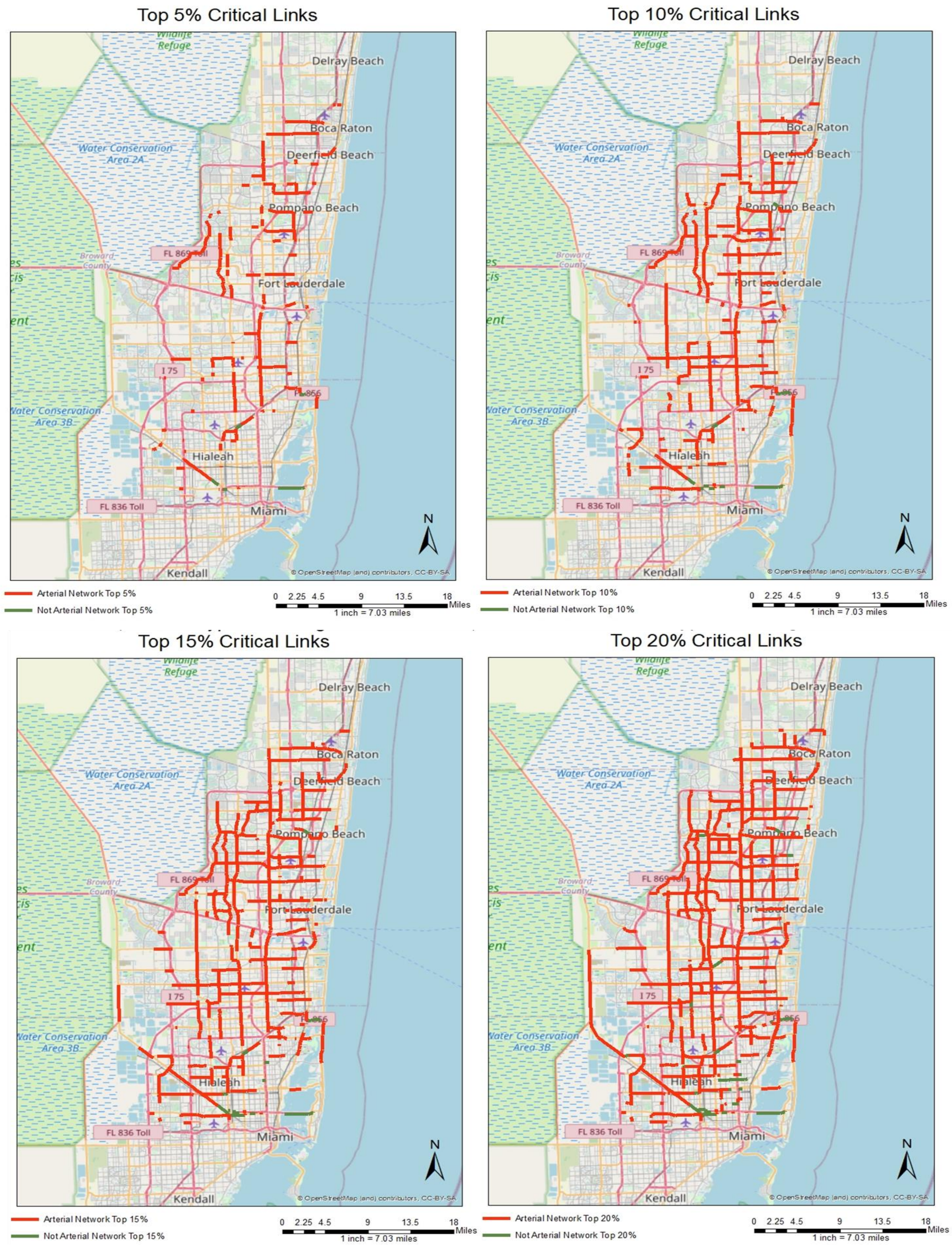


Figure 5. 4 Critical links identified by $T_{ff}BC^{*}$ hybrid measure (Passenger Demand Only)

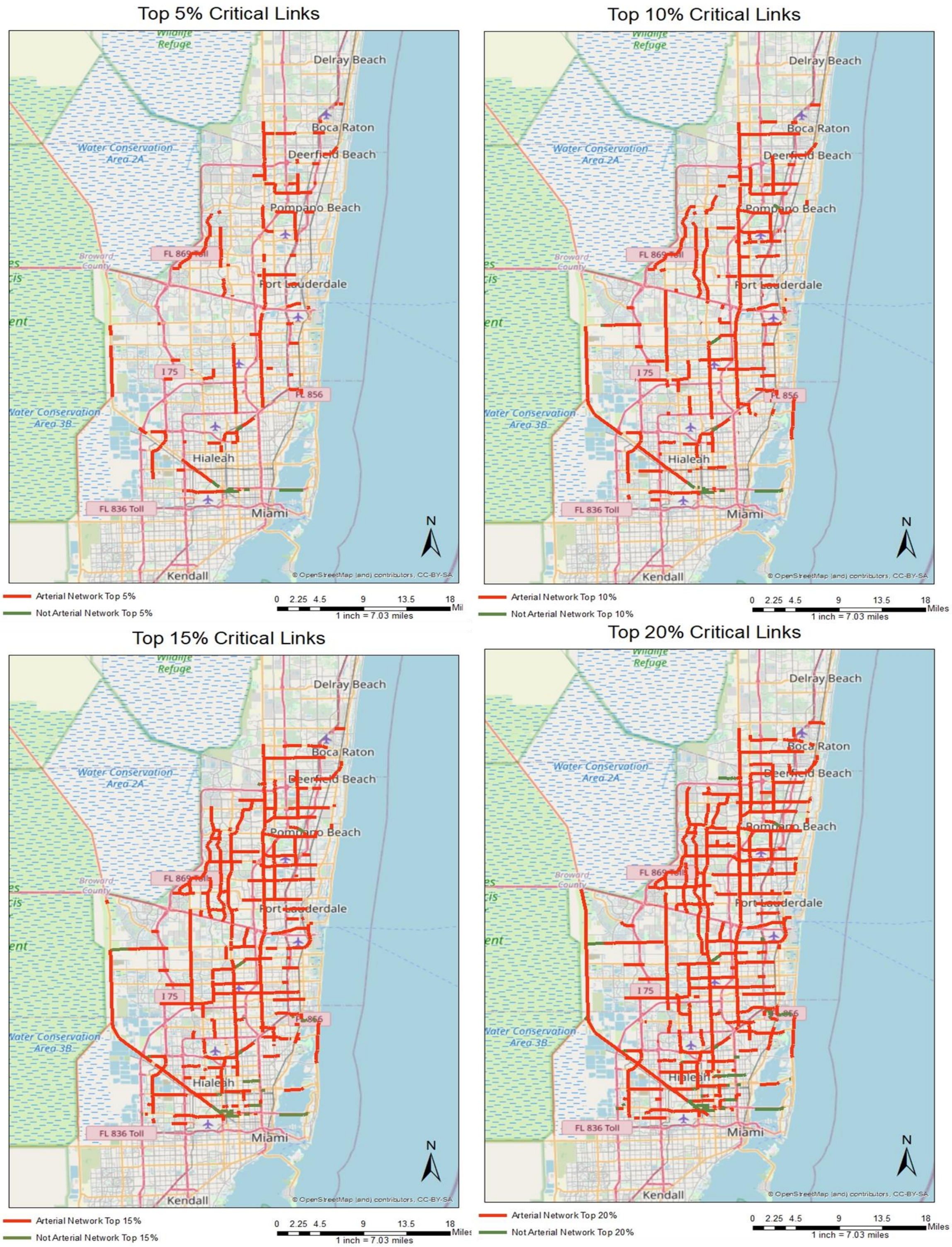


Figure 5. 5 Critical links identified by $T_{ff}BC^{*}$ hybrid measure (Truck Demand Only)

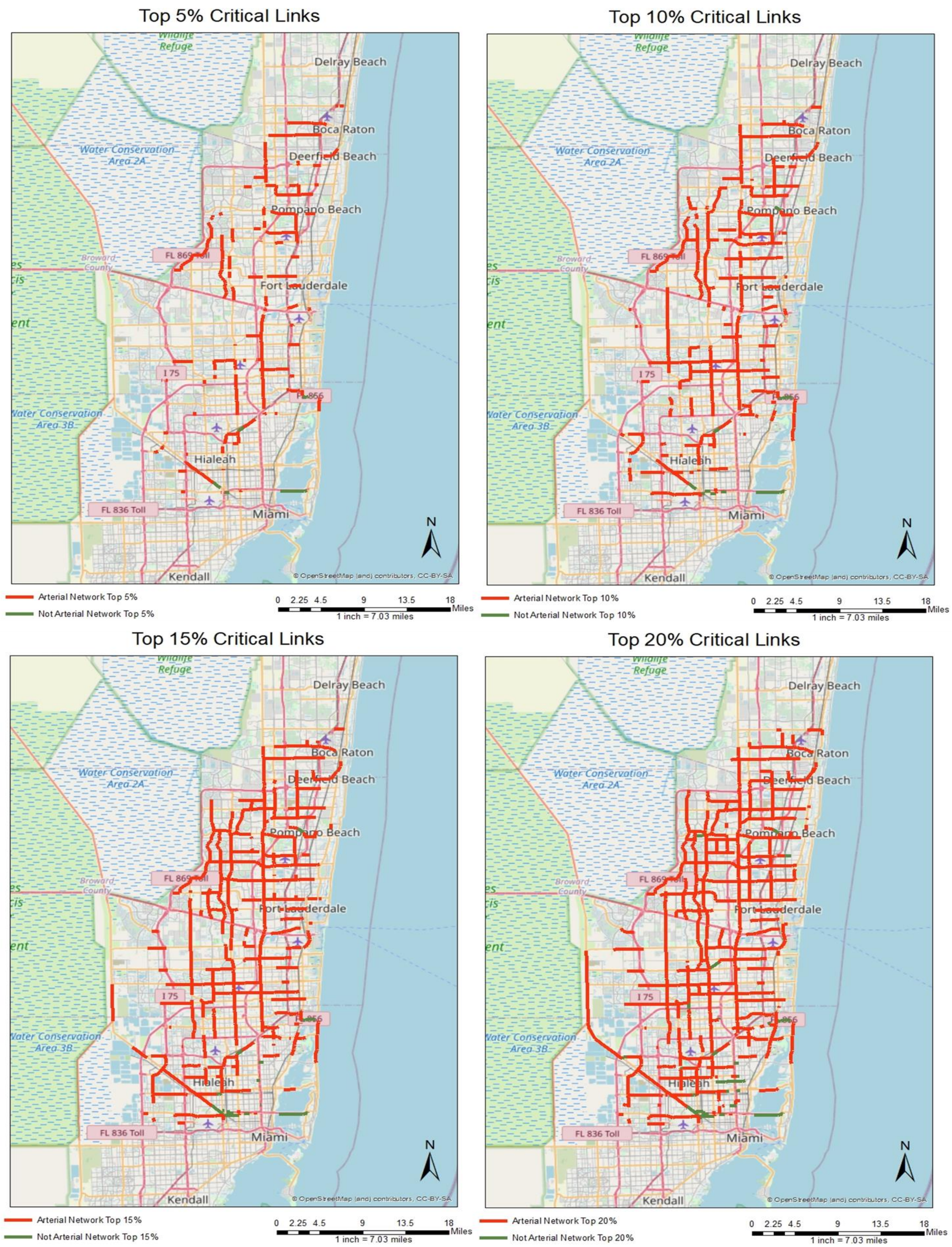


Figure 5. 6 Critical links identified by $T_{ff}BC^{*}$ hybrid measure (Combined Demand)

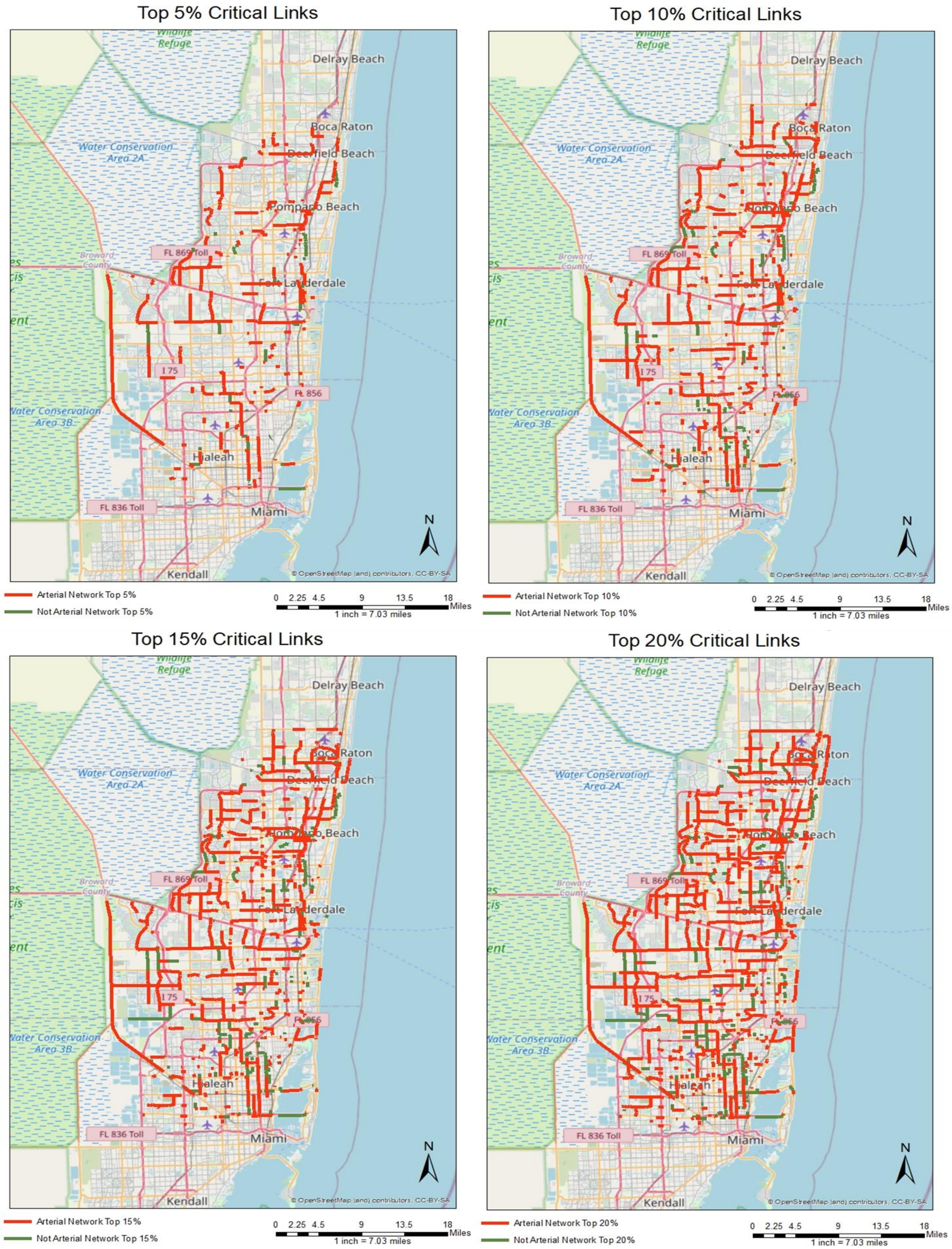


Figure 5. 7 Critical links identified by T_cBC^* hybrid (Passenger Demand Only)

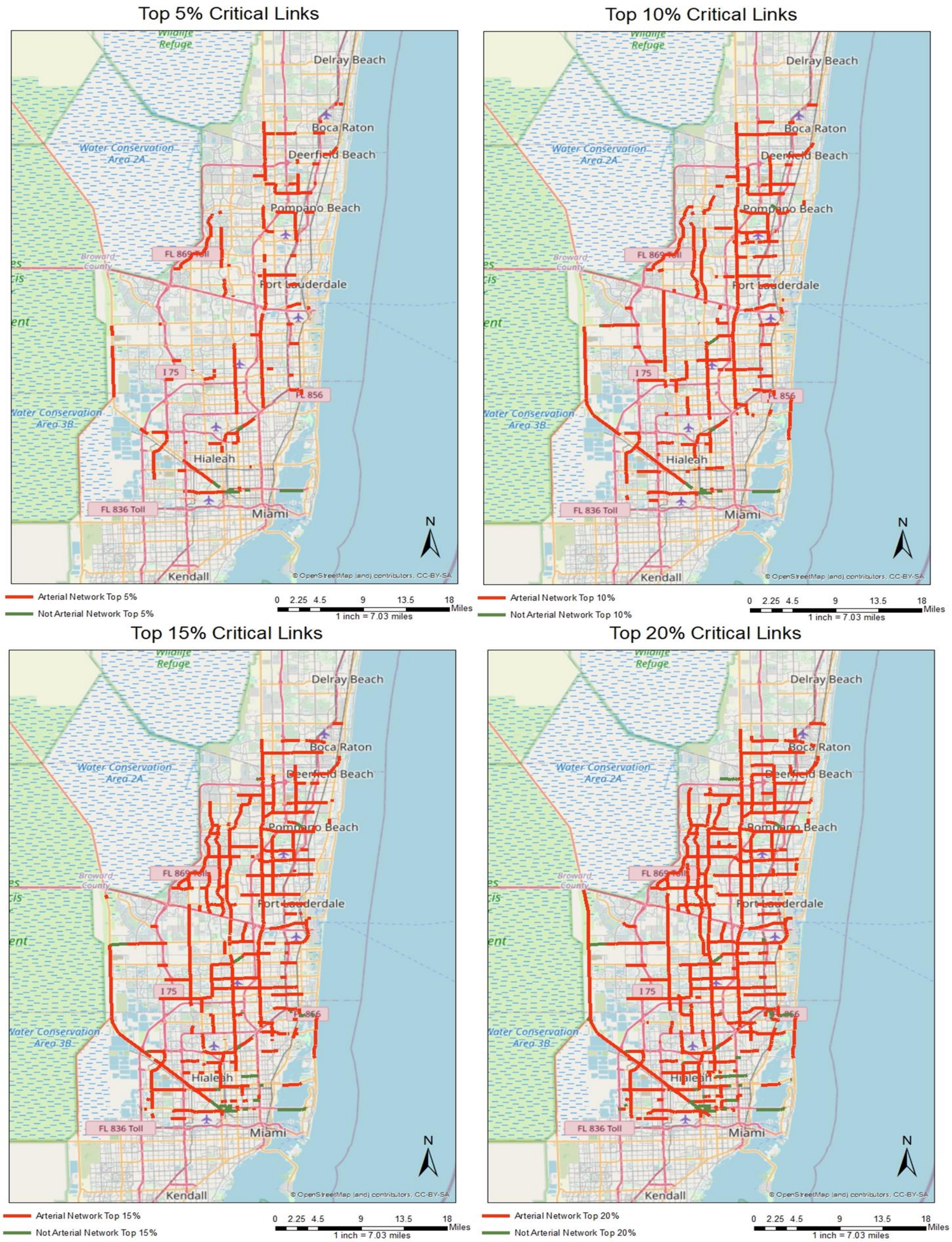


Figure 5. 8 Critical links identified by T_cBC^* hybrid (Truck Demand Only)

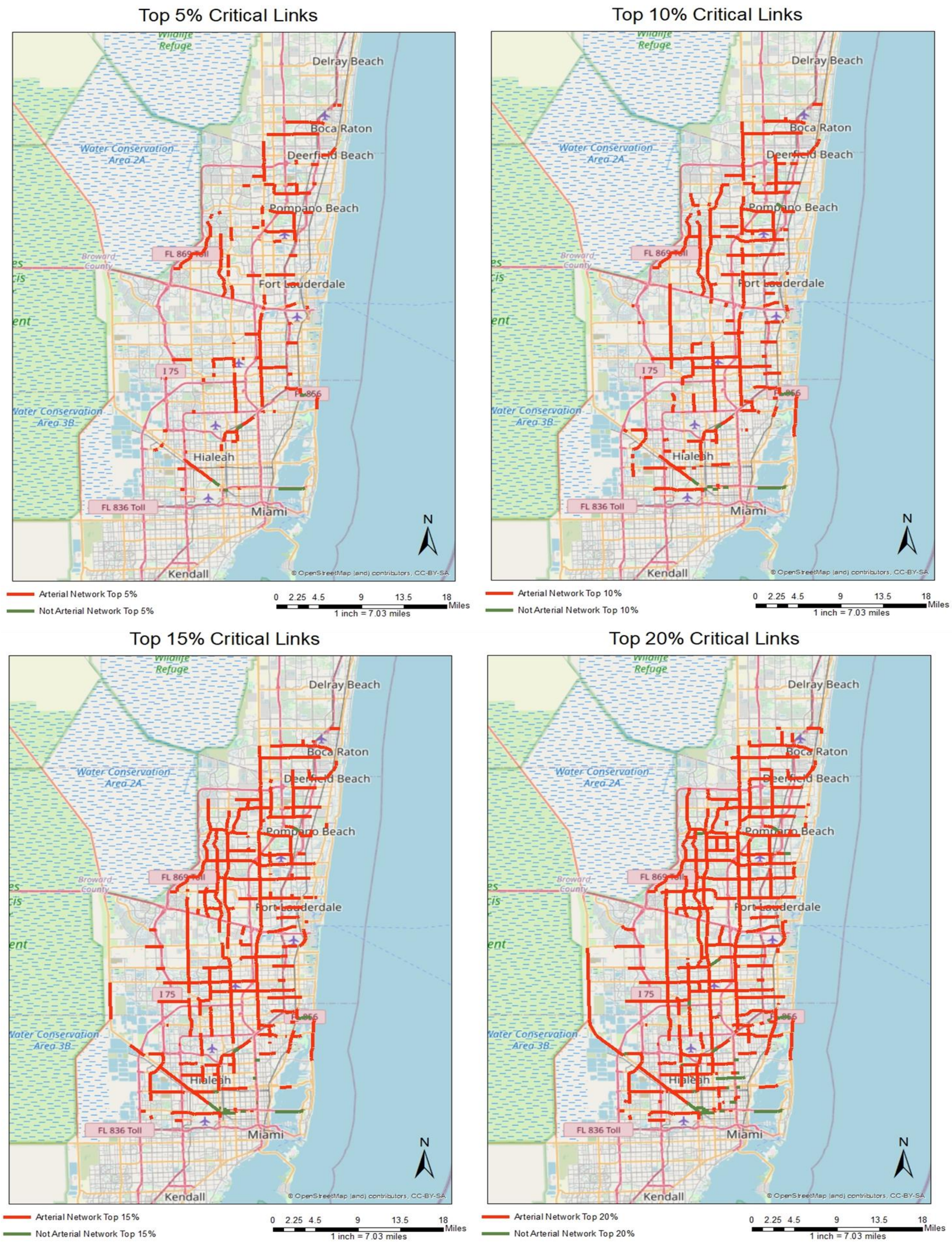


Figure 5. 9 Critical links identified by T_cBC^* hybrid (Combined Demand)

5.2 COMMON CRITICAL LINK

In this section more analysis to show the common critical links identified by the three hybrid measures for three different truck, passenger, and combined loaded networks have been presented in Figures 5.10 to 5.12. These figures showed the top 5%, 10%, 15%, and 20% important links which are commonly recognized as critical links by BC^*, $T_{ff}BC^*$, and T_cBC^* hybrid measures. Since each of these three measures consider different cost for weighting the network, this analysis helps to have a better insight of the presented results in the subsection 5.1.

As discussed in Chapter 4 of this report, BC^* considering centrality and social efficiency for finding the critical links, it means as much as a link is more central and carry more demand, it is more important. $T_{ff}BC^*$ not only considers centrality and social efficiency in its calculation but also it considers the effect of the uncongested situation (by weighting the graph by link's free flow travel time as the link's cost in shortest path calculation) in finding the critical links. T_cBC^* evaluate the network in the congested situation. This measure recognizes a link more critical than the others if it is more central and simultaneously it carries more demand, and more travel time is needed to commute on that in the loaded network than the others.

Critical links showed in Figures 5.10 to 5.12 are the links that not only appear more often in the shortest paths connecting ODs than the others (i.e., more central) but also, they have more demand, more free flow travel time, and need more real travel time is needed to commute on them. As it can be seen, these three hybrid measures have more commonality for truck demand loaded network which is the main objective of this project.

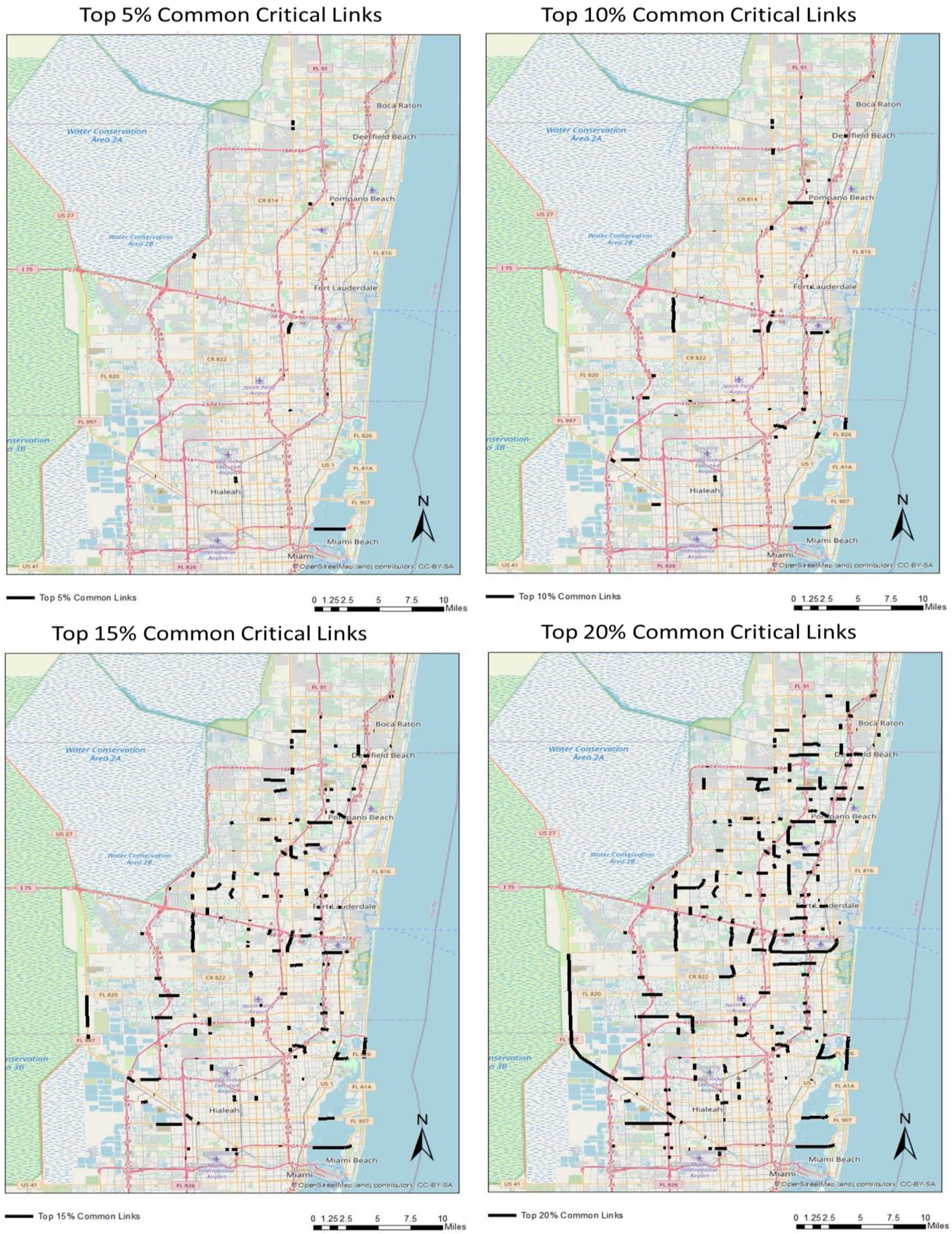


Figure 5. 10 Common critical links identified by $BC^{*}, T_{ff}BC^{*}, and\ T_{c}BC^{*}$ hybrid measures (Passenger Demand Only)

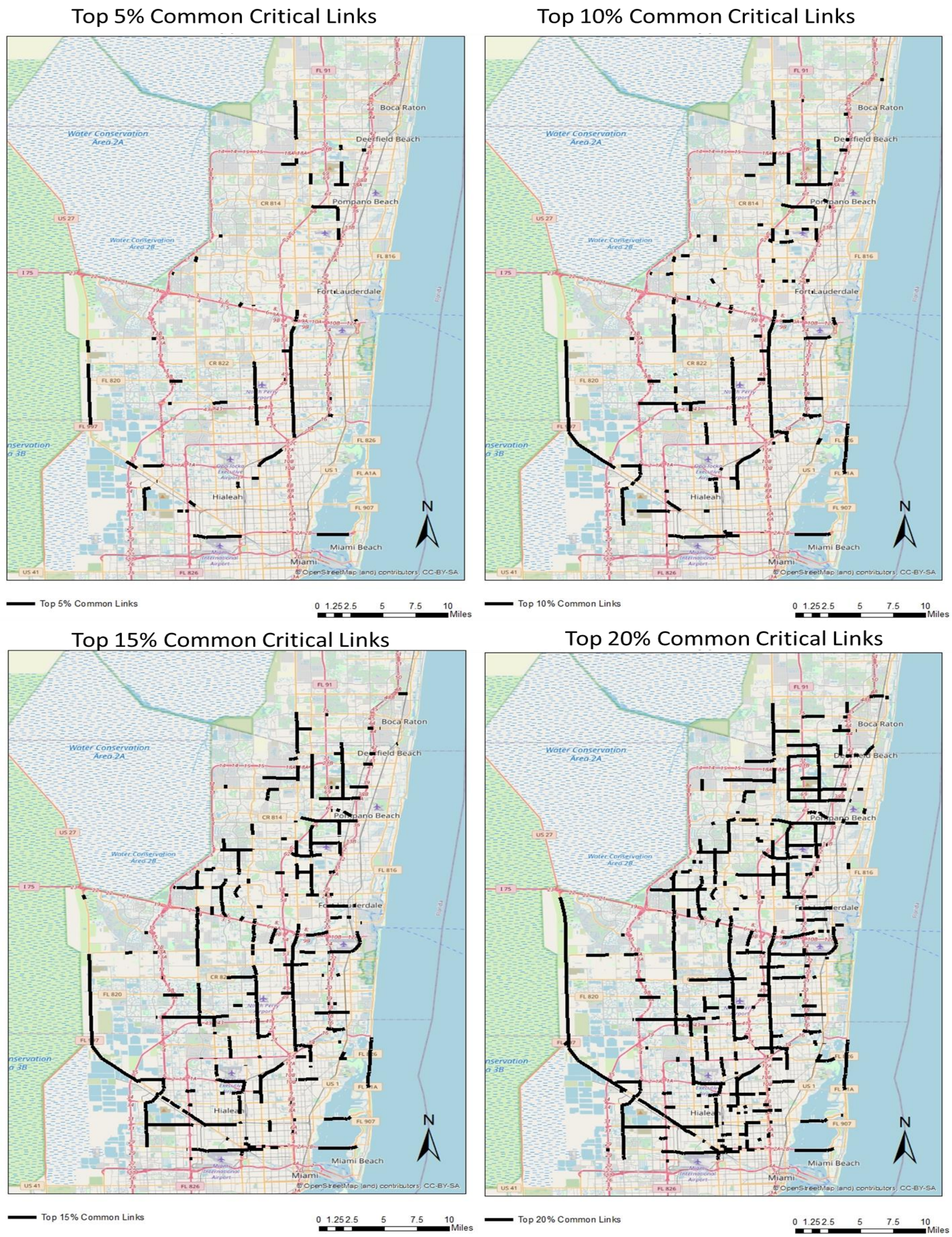


Figure 5. 11 Common critical links identified by $BC^{*}, T_{ff}BC^{*}, and\ T_{c}BC^{*}$ hybrid measures (Truck Demand Only)

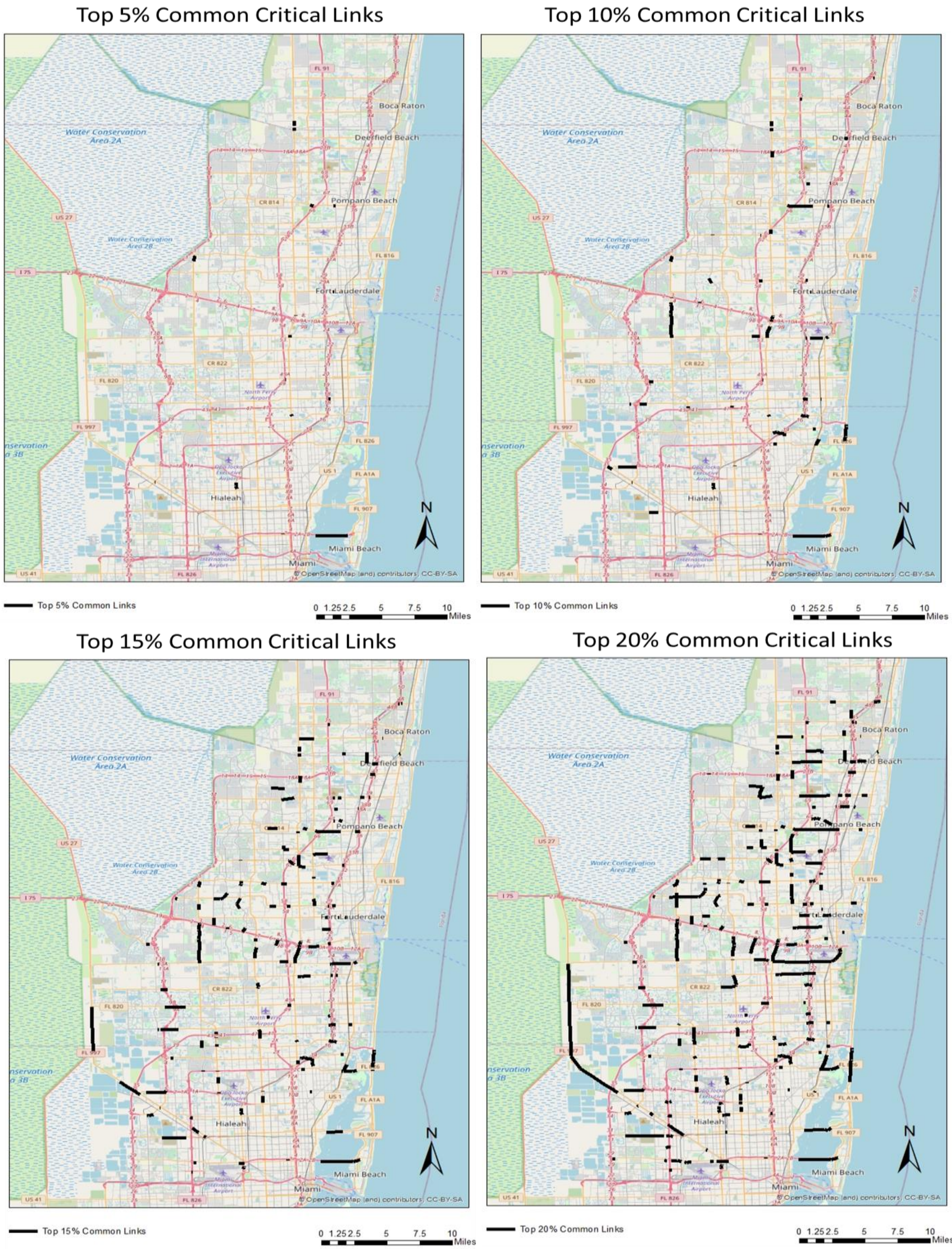


Figure 5. 12 Common critical links identified by $BC^{*}, T_{ff}BC^{*}, and\ T_{c}BC^{*}$ hybrid measures (Combined Demand)

5.3 CRITICAL SETS OF LINKS

For each defined scenario in section 4.2.3 (three different capacity reductions of 100%, 80% and 60% for any link that was compromised based on three different links selection (i.e., $BC^*,\ T_{ff}BC^*,$ $and\ T_cBC^*$ and three cases of different number of links that could be compromised i.e., 10, 20, and 30 links) by using the developed heuristic algorithm, 10,000 different critical sets of links are recognized. These sets of links are ranked based on the effect that they will have on increasing the travel cost when they were attacked. In other words, a subset of links is more important than others, when attacking those links leads to the greatest increase in travel time across the network.

In this subsection to show a sample of the results, the first, second, and third sets of 30 critical links under different capacity reductions (i.e., 100%, 80%, and 60%) are shown in figures 5.13 through 5.15. MATLAB Codes to visualize the results and generating more figures are saved in the (dropbox link) folder. Also, the manual of the ArcGIS toolbox which prepared based on the proposed game-theory framework is in the Appendix at the end of this report.

As Figures 5.13 to 5.15 indicate, the most critical subset of links will be changed based on the attack efficiency (partial closure or full closure of the link). The results showed that based on the severity of the disruption scenario (day-to-day or major disruption), different links could be identified as critical in the roadway network. Even considering different capacity reductions (60% and 80%) in partial closure scenarios will lead to different critical sets of links as well (comparing Figure 5.13 and 5.14).

Comparing these figures by results presented in subsection 5.1, reveals that the most critical sets of links that attacking them are led to the most negative effect on the total travel cost of the system, are not simply the combination of the most single-link failure. Identifying the critical sets of links are highly dependent on the attacker inelegancy, link attack selection, and the defined disruption scenario in terms of partial or full link closure.

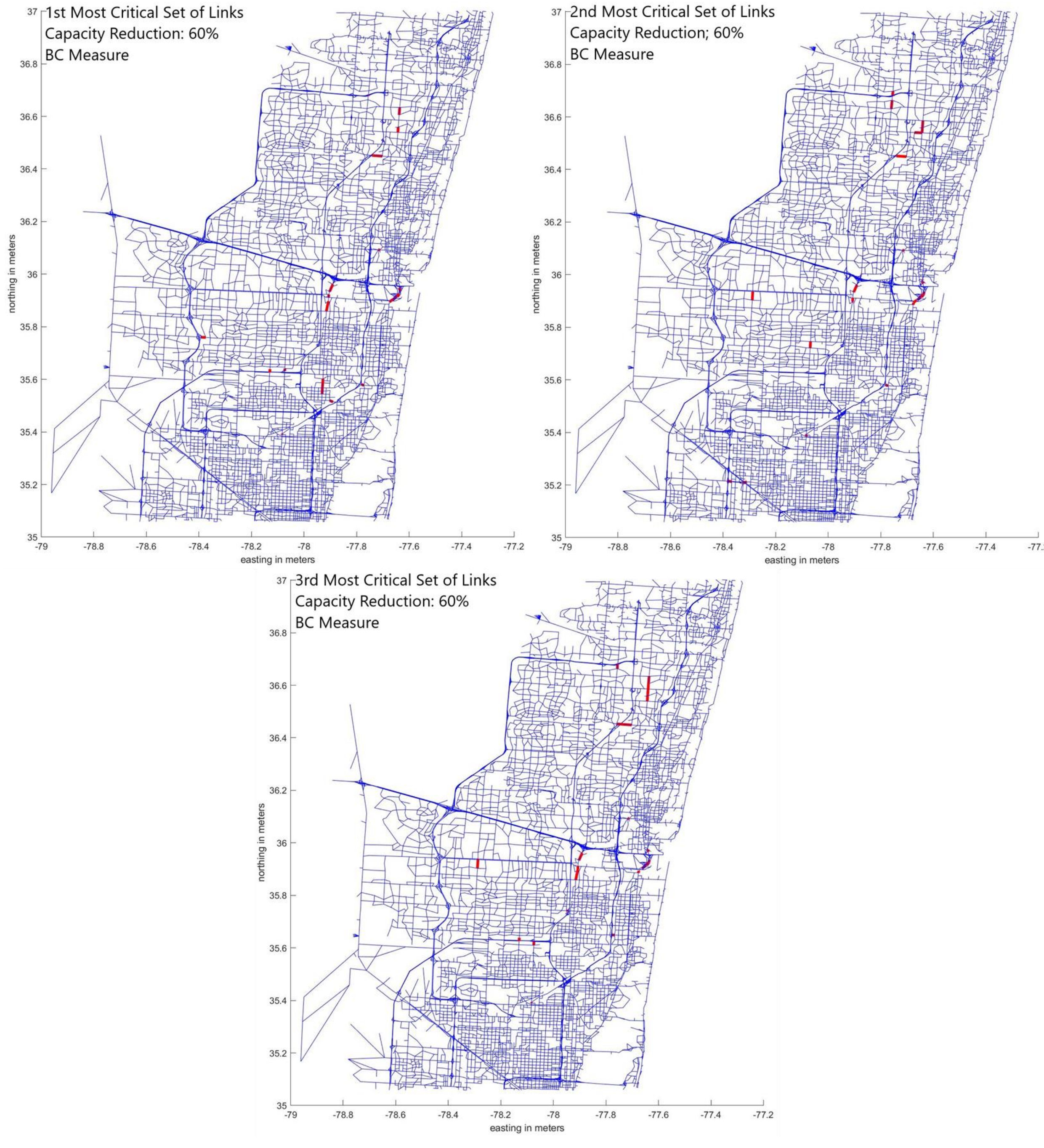


Figure 5. 13 1st, 2nd, and 3rd 30 critical links identified by game theory framework, under different capacity reductions of 60%.

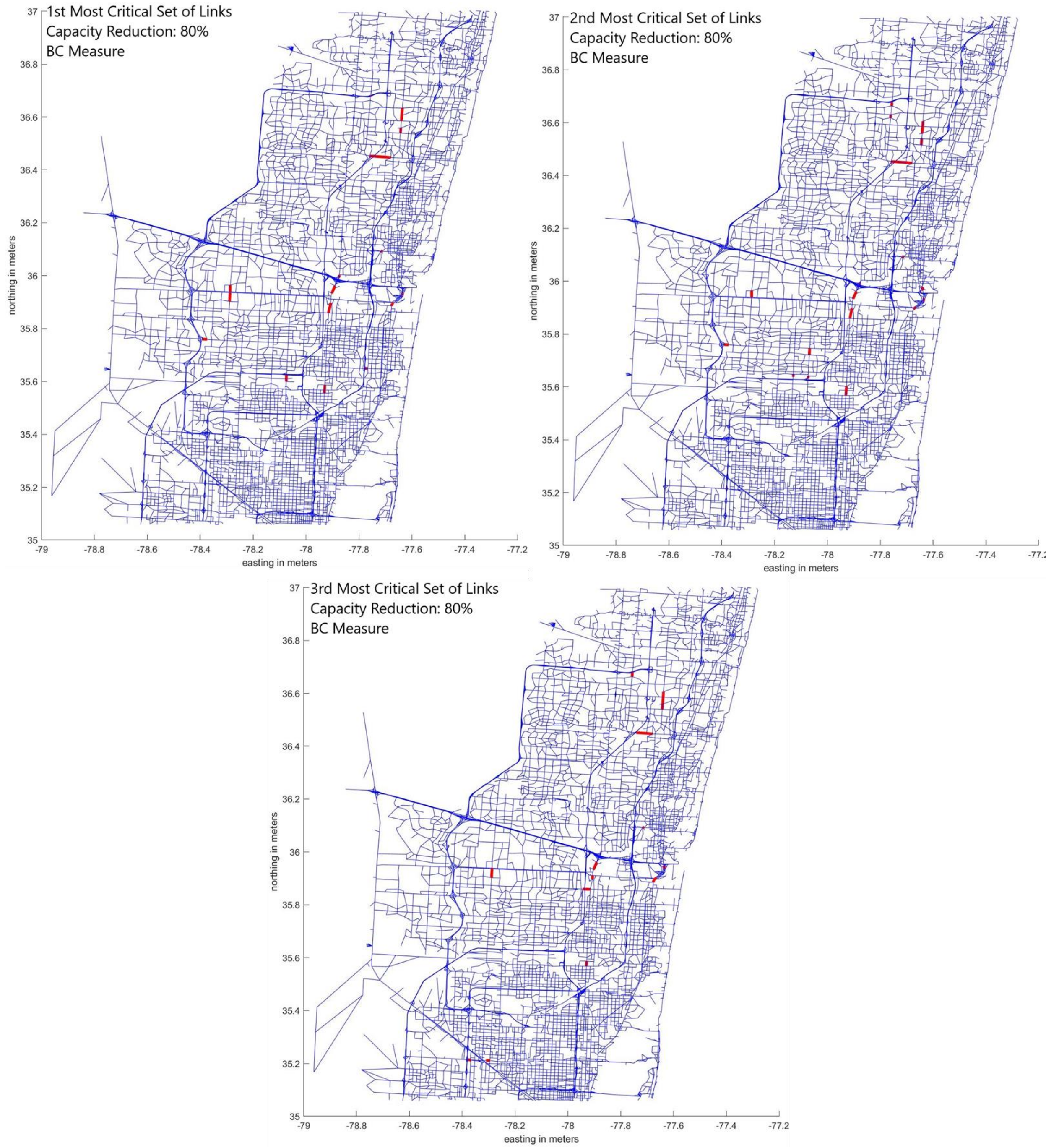


Figure 5. 14 1st, 2nd, and 3rd 30 critical links identified by game theory framework, under different capacity reductions of 80%.

Figure 5. 15 1st, 2nd, and 3rd 30 critical links identified by game theory framework, under different capacity reductions of 100%.

5.4 LINKS ATTACK PROBABILITY

In this subsection, we present a sample of results on the probability of attack for each link based on the BC^* link selection measure for three different numbers of links per set (10, 20, and 30 links) under different capacity reductions (i.e., 100%, 80%, and 60%) in figures 5.16 through 5.18. MATLAB Codes to visualize the results and generating more figures for other two links selection measures (i.e., $T_{ff}BC^*$and T_cBC^* are presented in Appendix and saved in the (dropbox link) folder.

The probability can be considered as a measure of a links' criticality and is estimated as a sum of the number of times a link is selected by the heuristic in critical sets of links (for all 10,000 sets). Comparing figures presented in subsection 5.3 and Figures 5.16 through 5.18 in this subsection, reveals that the links recognized by the developed heuristic algorithm as the most critical ones are the links that have the highest attack probability. Also, as it can be seen as much the number of links in each set increases (compare Figures 5.16 with 5.18), we will have the attack probability for a greater number of links. In this research for reducing the computational time, 30 was the greatest number of links in each set considered in the analysis. Based on the Broward county network size and its number of links (24007 links), obviously considering more links per set (like 200 or 400 links per set) will give more debatable and useful results for planning and investing.

Figure 5. 16 Link's attack probability for 10 links per set under three different capacity reduction (60%, 80%, and 100%), Link attack selection: BC^*

Figure 5. 17 Link's attack probability for 20 links per set under three different capacity reduction (60%, 80%, and 100%), Link attack selection: BC^*

Figure 5. 18 Link's attack probability for 30 links per set under three different capacity reduction (60%, 80%, and 100%), Link attack selection: BC^{*}

5.5 CRITICAL ROUTES

In this project, hybrid measures were used to find the most critical routes started from each origin. As it is explained in Chapter 4 of this report, the criticality of each specific route calculated by multiplying the demand value (passenger and truck) for the OD of the path into the summation of each of the three hybrid measures value for all the links on that path. Based on this explanation, all the existing routes in the network are ranked based on three measures for two different demand data.

After ranking all the routes based on their criticality value, the results prepared for the first 10 most critical routes started from each origin. It means that we will end up with 16530 critical routes recognized by each criticality hybrid measure. In this subsection, we present a sample of the results as a representative outcome and the MATLAB code for generating more maps based on the presented results is provided in Appendix B. Also, for making more options available for future analysis, (like identifying 20, 30,…) most critical routes started from each origin) a folder contains 1653 texts files which represent all the possible shortest paths started from each origin is saved in the (dropbox link) with the name of "All_Paths".

Figure 5.19 and 5.20 presented a presentative result of using BC^* to identify the first 10 critical routes for 4 different origins for both truck and passenger demand. Comparing Figure 5.19 and Figure 5.20 shows that critical routes for the same origin depends on which demand data was chosen for investigating the critical routes (freight or passenger) can be completely different.

Figure 5. 19 The first 10 critical freight routes starting from specific origin, identified by BC^*

Figure 5. 20 The first 10 critical passenger routes starting from specific origin, identified by BC^{*}

6. CONCLUSIONS AND FUTURE RESEARCH

In this project, two modeling frameworks, a solution algorithm, and a GIS-based toolbox that can assist decision-makers in identifying and ranking vulnerable and critical links and routes of a transportation network for both passengers and freight were developed and implements in Broward County, FL. Two different approaches were used to consider different network attributes and different disruption scenarios in identifying the vulnerable and critical links and routes. The first approach, by considering both topological and demand/supply characteristics of the network identified the most critical single links and routes in the network. The second approach by utilizing the game theory framework and bi-level formulation identified the most critical sets of links in a roadway network with focusing on both day-to-day and major disruptions. Despite most of the vulnerability approaches which require multiple traffic assignments to assess the vulnerability of the network, the developed methodologies in this project rely on running only one traffic assignment in their calculation. So, the presented methodologies in this project without any computational burden are easily applicable to evaluate the vulnerability of any scale of the roadway networks.

The numerical experiments that were performed showed that the transportation network is extremely vulnerable to attacks. The results showed that the links which are more central as compared to the others, and simultaneously have higher demand and more travel time require to commute on them (for both congested and non-congested situations), are critical links. On the other hand, attacks concentrated around origins and destinations with a high amount of demand in a way that would effectively isolate that origin or destination (i.e., a bridge).

Also, the presented outcomes indicate that the most identified critical sets of links that attacking them are led to the most negative effect on the total travel cost of the system, are not simply the combination of the most single-link failure. Identifying the critical sets of links are highly dependent on the attacker’s inelegancy, link attack selection, and the defined disruption scenario in terms of partial or full link closure.

6.1 PERSPECTIVE FOR FUTURE RESEARCH

The proposed method relied on a static user equilibrium which cannot capture the effects of link interaction and uncertainty of demand in the traffic assignment. Future research could focus on implementing dynamic traffic assignment and/or variable demand. Also, future research can focus on proposing new hybrid measures (by either modifying existing topological measures or combining the hybrid ones proposed in this research).

The research directions for future studies may also focus on the expansion of the hierarchical three-level game proposed in this research by introducing a combination of sets of links with the 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. In this project, the objective functions of both the defender and the attacker were assumed to be equal to the total travel time of all users. Other improvement that could be implemented include considering different objective functions for defender and attacker or even considering multiple attackers with different sets of objectives.

REFERENCES

1. Takhtfiroozeh, H; Golias, MM; Mishra S. Topological-based measures with flow Attributes to identify critical links in a transportation network. Transp Res Rec J Transp Res Board. 2021;(March):0–2.

2. Higgs B, Golias MM, Mishra S. Multi-level multi-objective vulnerability assessment of transportation networks. Transp Res Board, Washingt DC. 2017.

3. Lock JB, Gelling MJ. The Tasman Bridge disaster-before and after. Aust Road Res. 1976;6(2).

4. Taylor M. Vulnerability analysis for transportation networks. Elsevier; 2017.

5. Rupi F, Angelini S, Bernardi S, Danesi A, Rossi G. Ranking links in a road transport network: A practical method for the calculation of link importance. Transp Res Procedia. 2015;5:221–32.

6. Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal. 1981;1(1):11–27.

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

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

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

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

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

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

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

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

p. 206.

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

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

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

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

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

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

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

22. Jenelius E, Mattsson L-G. Road network vulnerability analysis of area-covering disruptions: A grid-based approach with case study. Transp Res part A policy Pract. 2012;46(5):746–60.

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

24. Knoop VL, Snelder M, van Zuylen HJ, Hoogendoorn SP. Link-level vulnerability indicators for real-world networks. Transp Res Part A Policy Pract. 2012;46(5):843–54.

25. Zhang M, Lomax T. Estimating congestion index at the link level with TransCAD GIS. In: Plan, Build, and Manage Transportation Infrastructure in China. 2008. p. 7–17.

26. Luping Y, Dalin Q. Vulnerability analysis of road networks. J Transp Syst Eng Inf Technol. 2012;12(1):105–10.

27. Roads USB of P. Traffic assignment manual for application with a large, high speed computer. Vol. 2. US Department of Commerce, Bureau of Public Roads, Office of Planning, Urban …; 1964.

28. Pratt RH, Lomax TJ. Performance measures for multimodal transportation systems. Transp Res Rec. 1996;1518(1):85–93.

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

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

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

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

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

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

35. Chen BY, Lam WHK, Sumalee A, Li Q, Li Z-C. Vulnerability analysis for large-scale and congested road networks with demand uncertainty. Transp Res Part A Policy Pract. 2012;46(3):501–16.

36. Cats O, Jenelius E. Planning for the unexpected: the value of reserve capacity for public transport network robustness. Transp Res Part A Policy Pract. 2015;81:47–61.

37. Dehghanisanij M, Flintsch GW, McNeil S. Vulnerability analysis of degrading roadway networks. In: 92nd Annual Meeting of the Transportation Research Board, Washington, DC. 2013.

38. Tampere CMJ, Stada J, Immers B, Peetermans E, Organe K. Methodology for identifying vulnerable sections in a national road network. Transp Res Rec. 2007;2012(1):1–10.

39. Alderson DL, Brown GG, Carlyle WM, Wood RK. Solving defender-attacker-defender models for infrastructure defense. Naval Postgraduate School Monterey CA Dept Of Operations Research; 2011.

40. Nagurney A, Qiang Q. 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. 2007.

41. Miller-Hooks E, Zhang X, Faturechi R. Measuring and maximizing resilience of freight

transportation networks. Comput Oper Res. 2012;39(7):1633–43.

42. Zhang L, Wen Y, Huang Z, Jin M. Framework of calculating the measures of resilience (MOR) for intermodal transportation systems. Mississippi. Dept. of Transportation; 2010.

43. Zhu S, Levinson D, Liu HX, Harder K. The traffic and behavioral effects of the I-35W Mississippi River bridge collapse. Transp Res part A policy Pract. 2010;44(10):771–84.

44. Volpe JA. Effect of catastrophic events on transportation system comparative analysis. 2004.

45. Mattsson L-G, Jenelius E. Vulnerability and resilience of transport systems–A discussion of recent research. Transp Res Part A Policy Pract. 2015;81:16–34.

46. Sohn J. Evaluating the significance of highway network links under the flood damage: An accessibility approach. Transp Res Part A Policy Pract. 2006 Jul;40(6):491–506.

47. Demšar U, Špatenková O, Virrantaus K. Identifying critical locations in a spatial network with graph theory. Trans GIS. 2008;12(1):61–82.

48. Duan Y, Lu F. Robustness of city road networks at different granularities. Phys A Stat Mech its Appl. 2014 Oct 1;411:21–34.

49. Latora V, Marchiori M. Efficient behavior of small-world networks. Phys Rev Lett. 2001;87(19):198701.

50. Porta S, Crucitti P, Latora V. The network analysis of urban streets: A dual approach. Phys A Stat Mech its Appl. 2006;369(2):853–66.

51. Taylor MAP, Sekhar SVC, D'Este GM. Application of accessibility based methods for vulnerability analysis of strategic road networks. Networks Spat Econ. 2006;6(3):267–91.

52. Furno A, El Faouzi N-E, Sharma R, Cammarota V, Zimeo E. A graph-based framework for real-time vulnerability assessment of road networks. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE; 2018. p. 234–41.

53. Kim TJ, Ham H, Boyce DE. Economic impacts of transportation network changes: Implementation of a combined transportation network and input-output model. Pap Reg Sci. 2002 Apr;81(2):223–46.

54. Tatano H, Tsuchiya S. A framework for economic loss estimation due to seismic transportation network disruption: a spatial computable general equilibrium approach. Nat Hazards. 2008 Feb;44(2):253–65.

55. Bono F, Gutiérrez E. A network-based analysis of the impact of structural damage on urban accessibility following a disaster: the case of the seismically damaged Port Au Prince and

Carrefour urban road networks. J Transp Geogr. 2011;19(6):1443–55.

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

57. Almotahari A, Yazici MA. A link criticality index embedded in the convex combinations solution of user equilibrium traffic assignment. Transp Res Part A Policy Pract. 2019 Aug 1;126:67–82.

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

59. Lownes NE, Wang Q, Ibrahim S, Ammar RA, Rajasekaran S, Sharma D. Many-to-many game-theoretic approach for the measurement of transportation network vulnerability. Transp Res Rec. 2011;2263(1):1–8.

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

61. Wang DZW, Liu H, Szeto WY, Chow AHF. Identification of critical combination of vulnerable links in transportation networks–a global optimisation approach. Transp A Transp Sci. 2016;12(4):346–65.

62. Candelieri A, Galuzzi BG, Giordani I, Archetti F. Vulnerability of public transportation networks against directed attacks and cascading failures. Public Transp. 2019;11(1):27–49.

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

64. Taylor MAP. Critical transport infrastructure in Urban areas: impacts of traffic incidents assessed using accessibility-based network vulnerability analysis. Growth Change. 2008;39(4):593–616.

65. Nagurney A, Qiang Q. A Transportation Network Efficiency Measure that Captures Flows, Behavior, and Costs with Applications to Network Component Importance Identification and Vulnerability.

66. El-Rashidy RA, Grant-Muller SM. An assessment method for highway network vulnerability. J Transp Geogr. 2014;34:34–43.

67. Cantillo V, Macea LF, Jaller M. Assessing vulnerability of transportation networks for disaster response operations. Networks Spat Econ. 2019;19(1):243–73.

68. Gauthier P, Furno A, El Faouzi NE. Road network resilience: how to identify critical links

subject to day-to-day disruptions. Transp Res Rec. 2018;2672(1):54–65.

69. Li F, Jia H, Luo Q, Li Y, Yang L. Identification of critical links in a large-scale road network considering the traffic flow betweenness index. PLoS One. 2020;15(4):1–23. http://dx.doi.org/10.1371/journal.pone.0227474

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

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

72. Sheffi Y. Urban Transportation Networks: Equilibrium analysis with mathematical programming methods (New Jersey: J. Prentice Hall, England Cliffs). 1985;

APPENDIX A: GIS TOOLBOX USER MANUAL

Vulnerability Software User Manual

Developed Tools

Required File

- **Vulnerability Tools.pyt**
- **SPSA_v5.exe**

NOTE:

the format that developed toolbox can read the OD demand file is in a way that each row should determine the demand from one origin to one destination. Since the testbed network in this project (i.e. Broward County) has 1653 OD pairs, we will end up with an OD demand table with 1653*1653*=2,732,400 rows, which cannot creatable and readable by both Excel and ArcGIS. As a result, Memphis Network chose by the research team as the alternative network to show the capability of the developed vulnerability ArcGIS toolbox and preparing the user manual for explaining the necessary steps to run it based on that.

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 **Vulnerability Tools** toolbox and lunch Net Conversion Tool (see FIGURE A. 1)

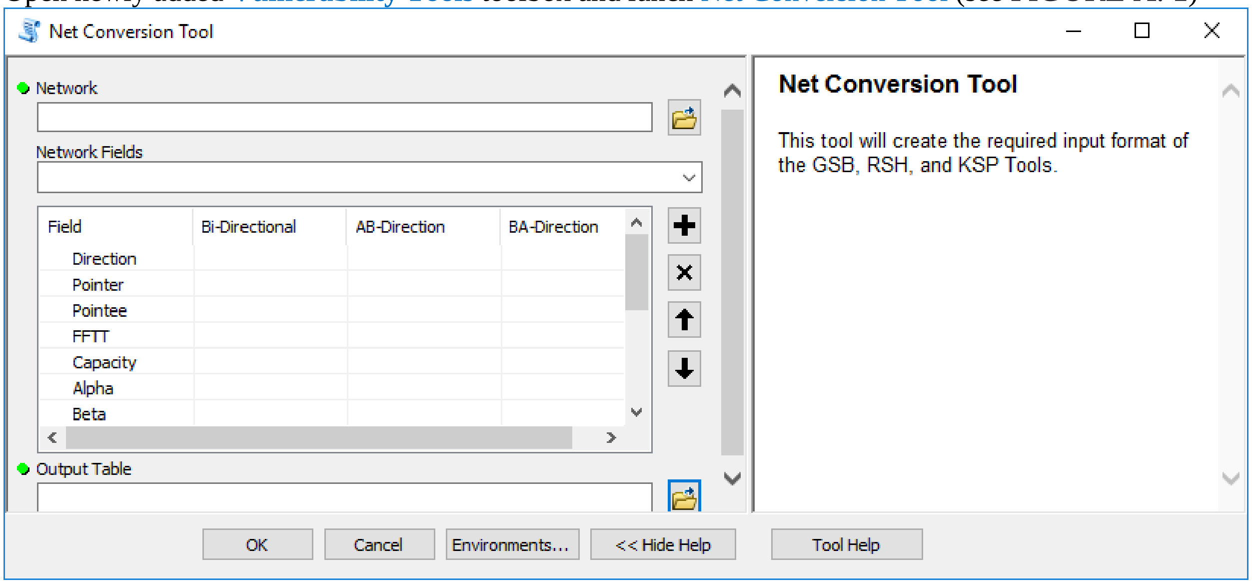


Figure A. 2 Net Conversion Tool

STEP 2

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

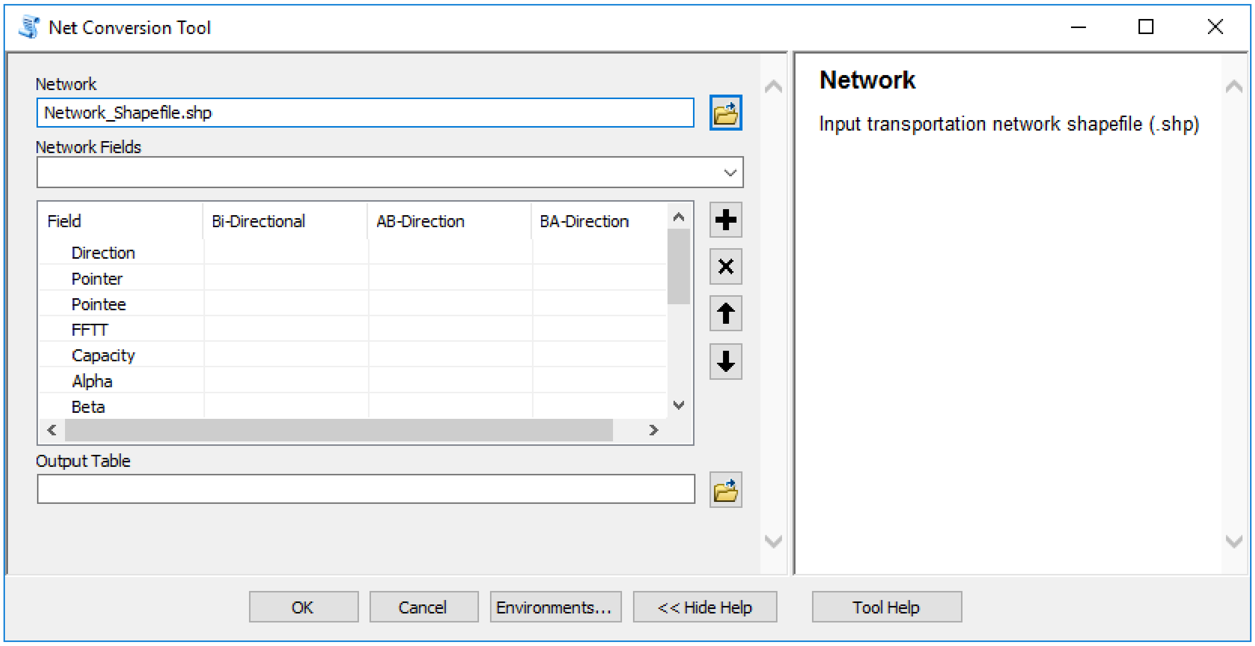


Figure A. 3 Input Transportation Network Shapefile (.shp)

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.)

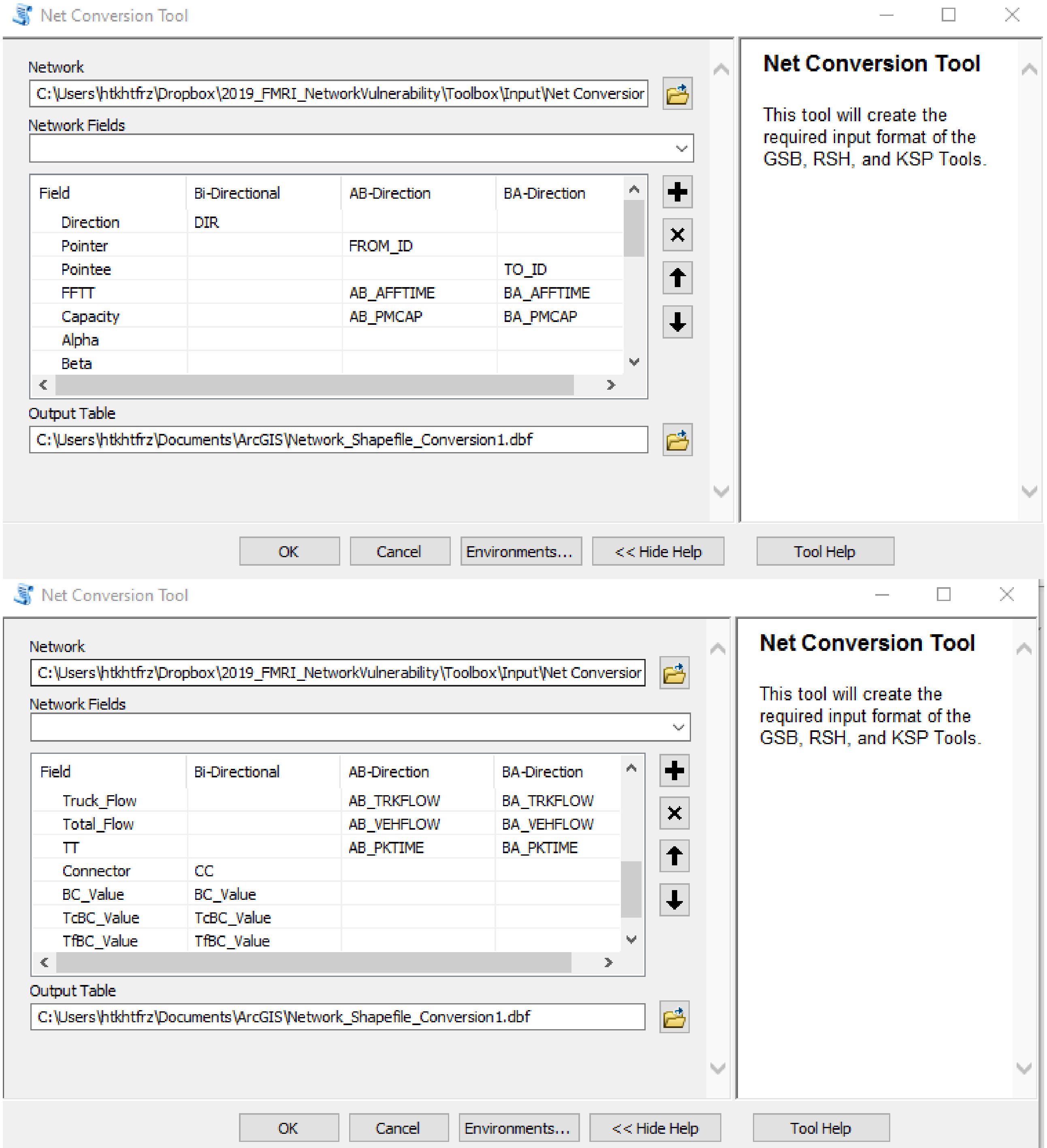


Figure A. 4 Select the corresponding Input Network Attribute Fields

STEP 4

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

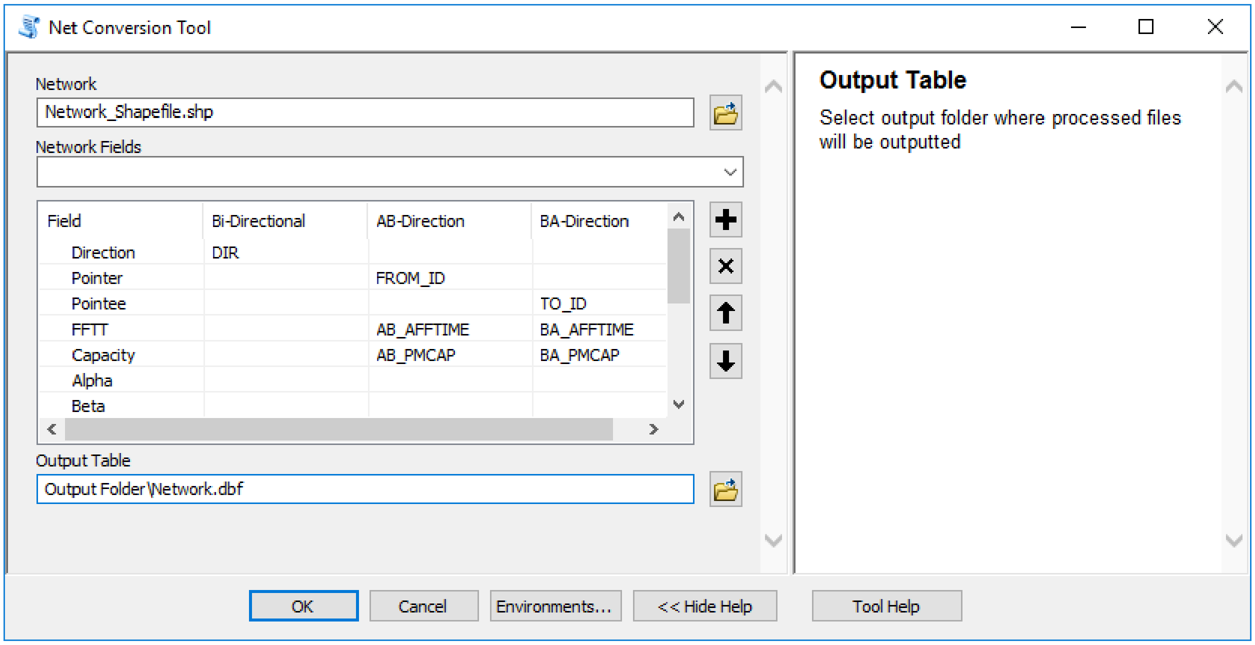


Figure A. 5 Input Path to Output Table

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.

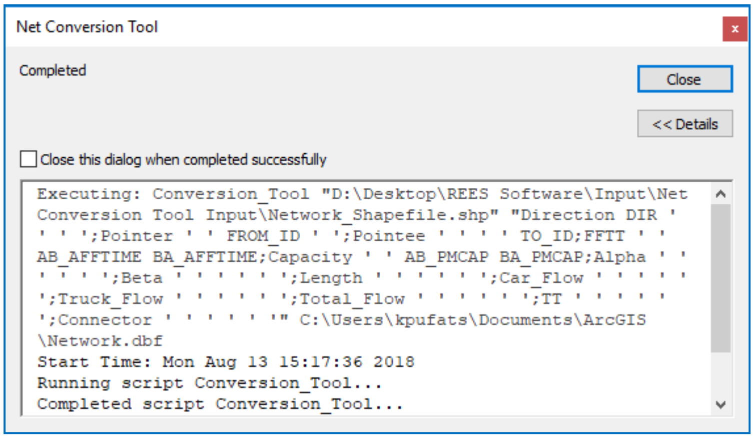
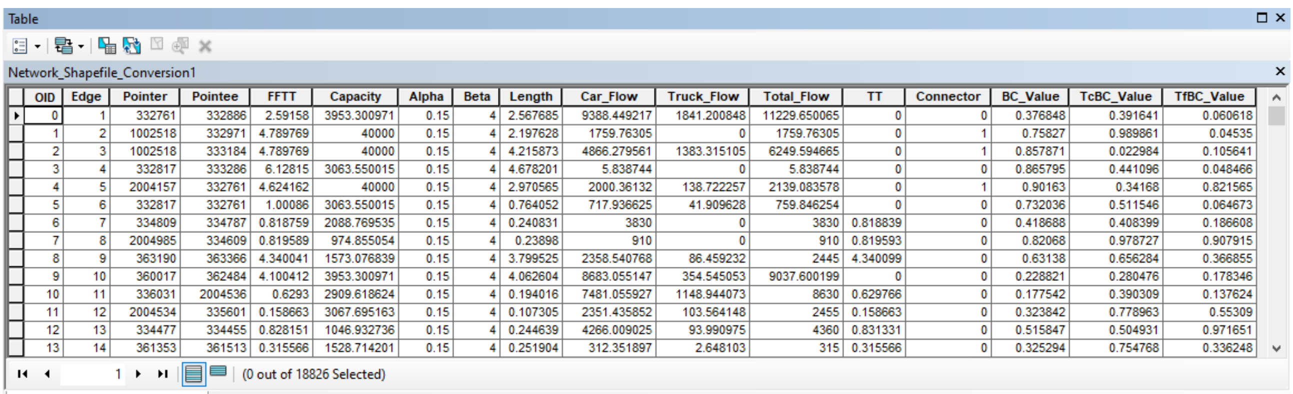


Figure A. 6 Application Performance Task Window



Table

Network_Shapefile_Conversion1

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector	BC_Value	TcBC_Value	TfBC_Value
0	1	332761	332886	2.59158	3953.300971	0.15	4	2.567685	9388.449217	1841.200848	11229.650065	0	0	0.376848	0.391641	0.060618
1	2	1002518	332971	4.789769	40000	0.15	4	2.197628	1759.76305	0	1759.76305	0	1	0.75827	0.989861	0.04535
2	3	1002518	333184	4.789769	40000	0.15	4	4.215873	4866.279561	1383.315105	6249.594665	0	1	0.857871	0.022984	0.105641
3	4	332817	333286	6.12815	3063.550015	0.15	4	4.678201	5.838744	0	5.838744	0	0	0.865795	0.441096	0.048466
4	5	2004157	332761	4.624162	40000	0.15	4	2.970565	2000.36132	138.722257	2139.083578	0	1	0.90163	0.34168	0.821565
5	6	332817	332761	1.00086	3063.550015	0.15	4	0.764052	717.936625	41.909628	759.846254	0	0	0.732036	0.511546	0.064673
6	7	334809	334787	0.818759	2088.769535	0.15	4	0.240831	3830	0	3830	0.818839	0	0.418688	0.408399	0.186608
7	8	2004985	334609	0.819589	974.855054	0.15	4	0.23898	910	0	910	0.819593	0	0.82068	0.978727	0.907915
8	9	363190	363366	4.340041	1573.076839	0.15	4	3.799525	2358.540768	86.459232	2445	4.340099	0	0.63138	0.656284	0.366855
9	10	360017	362484	4.100412	3953.300971	0.15	4	4.062604	8683.055147	354.545053	9037.600199	0	0	0.228821	0.280476	0.178346
10	11	336031	2004536	0.6293	2909.618624	0.15	4	0.194016	7481.055927	1148.944073	8630	0.629766	0	0.177542	0.390309	0.137624
11	12	2004534	335601	0.158663	3067.695163	0.15	4	0.107305	2351.435852	103.564148	2455	0.158663	0	0.323842	0.778963	0.55309
12	13	334477	334455	0.828151	1046.932736	0.15	4	0.244639	4266.009025	93.990975	4360	0.831331	0	0.515847	0.504931	0.971651
13	14	361353	361513	0.315566	1528.714201	0.15	4	0.251904	312.351897	2.648103	315	0.315566	0	0.325294	0.754768	0.336248

(0 out of 18826 Selected)

Figure A. 7 Output Table

The Greedy Search Based Vulnerability Tool (GSB Tool)

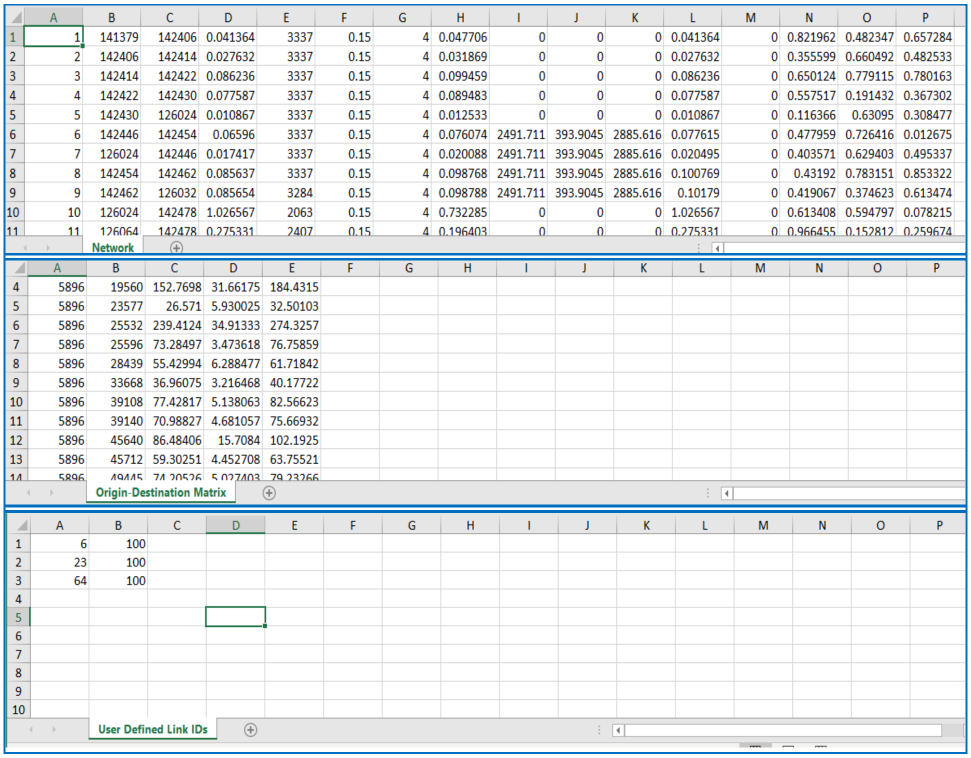
Description

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), BC_Value, TcBC_Value, TfBC_Value.
- **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	O	P
1	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0	0.821962	0.482347	0.657284
2	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0	0.355599	0.660492	0.482533
3	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0	0.650124	0.779115	0.780163
4	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0	0.557517	0.191432	0.367302
5	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0	0.116366	0.63095	0.308477
6	6	142446	142454	0.06596	3337	0.15	4	0.076074	2491.711	393.9045	2885.616	0.077615	0	0.477959	0.726416	0.012675
7	7	126024	142446	0.017417	3337	0.15	4	0.020088	2491.711	393.9045	2885.616	0.020495	0	0.403571	0.629403	0.495337
8	8	142454	142462	0.085637	3337	0.15	4	0.098768	2491.711	393.9045	2885.616	0.100769	0	0.43192	0.783151	0.853322
9	9	142462	126032	0.085654	3284	0.15	4	0.098788	2491.711	393.9045	2885.616	0.10179	0	0.419067	0.374623	0.613474
10	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	1.026567	0	0.613408	0.594797	0.078215
11	11	126064	142478	0.275331	2407	0.15	4	0.196403	0	0	0	0.275331	0	0.966455	0.152812	0.259674

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
14	5896	49445	74.20526	5.027403	79.23266

Origin-Destination Matrix

	A	B
1	6	100
2	23	100
3	64	100

User Defined Link IDs

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

Table

Network_Shapefile_Conversion1

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector	BC_Value	TcBC_Value	TfBC_Value
0	1	332761	332886	2.59158	3953.300971	0.15	4	2.567685	9388.449217	1841.200848	11229.650065	0	0	0.376848	0.391641	0.060618
1	2	1002518	332971	4.789769	40000	0.15	4	2.197628	1759.76305	0	1759.76305	0	1	0.75827	0.989861	0.04535
2	3	1002518	333184	4.789769	40000	0.15	4	4.215873	4866.279561	1383.315105	6249.594665	0	1	0.857871	0.022984	0.105641
3	4	332817	333286	6.12815	3063.550015	0.15	4	4.678201	5.838744	0	5.838744	0	0	0.865795	0.441096	0.048466
4	5	2004157	332761	4.624162	40000	0.15	4	2.970565	2000.36132	138.722257	2139.083578	0	1	0.90163	0.34168	0.821565
5	6	332817	332761	1.00086	3063.550015	0.15	4	0.764052	717.936625	41.909628	759.846254	0	0	0.732036	0.511546	0.064673
6	7	334809	334787	0.818759	2088.769535	0.15	4	0.240831	3830	0	3830	0.818839	0	0.418688	0.408399	0.186608
7	8	2004985	334609	0.819589	974.855054	0.15	4	0.23898	910	0	910	0.819593	0	0.82068	0.978727	0.907915
8	9	363190	363366	4.340041	1573.076839	0.15	4	3.799525	2358.540768	86.459232	2445	4.340099	0	0.63138	0.656284	0.366855
9	10	360017	362484	4.100412	3953.300971	0.15	4	4.062604	8683.055147	354.545053	9037.600199	0	0	0.228821	0.280476	0.178346
10	11	336031	2004536	0.6293	2909.618624	0.15	4	0.194016	7481.055927	1148.944073	8630	0.629766	0	0.177542	0.390309	0.137624
11	12	2004534	335601	0.158663	3067.695163	0.15	4	0.107305	2351.435852	103.564148	2455	0.158663	0	0.323842	0.778963	0.55309
12	13	334477	334455	0.828151	1046.932736	0.15	4	0.244639	4266.009025	93.990975	4360	0.831331	0	0.515847	0.504931	0.971651
13	14	361353	361513	0.315566	1528.714201	0.15	4	0.251904	312.351897	2.648103	315	0.315566	0	0.325294	0.754768	0.336248

1 (0 out of 18826 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. 9 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and lunch GSB Tool (see FIGURE A.9)

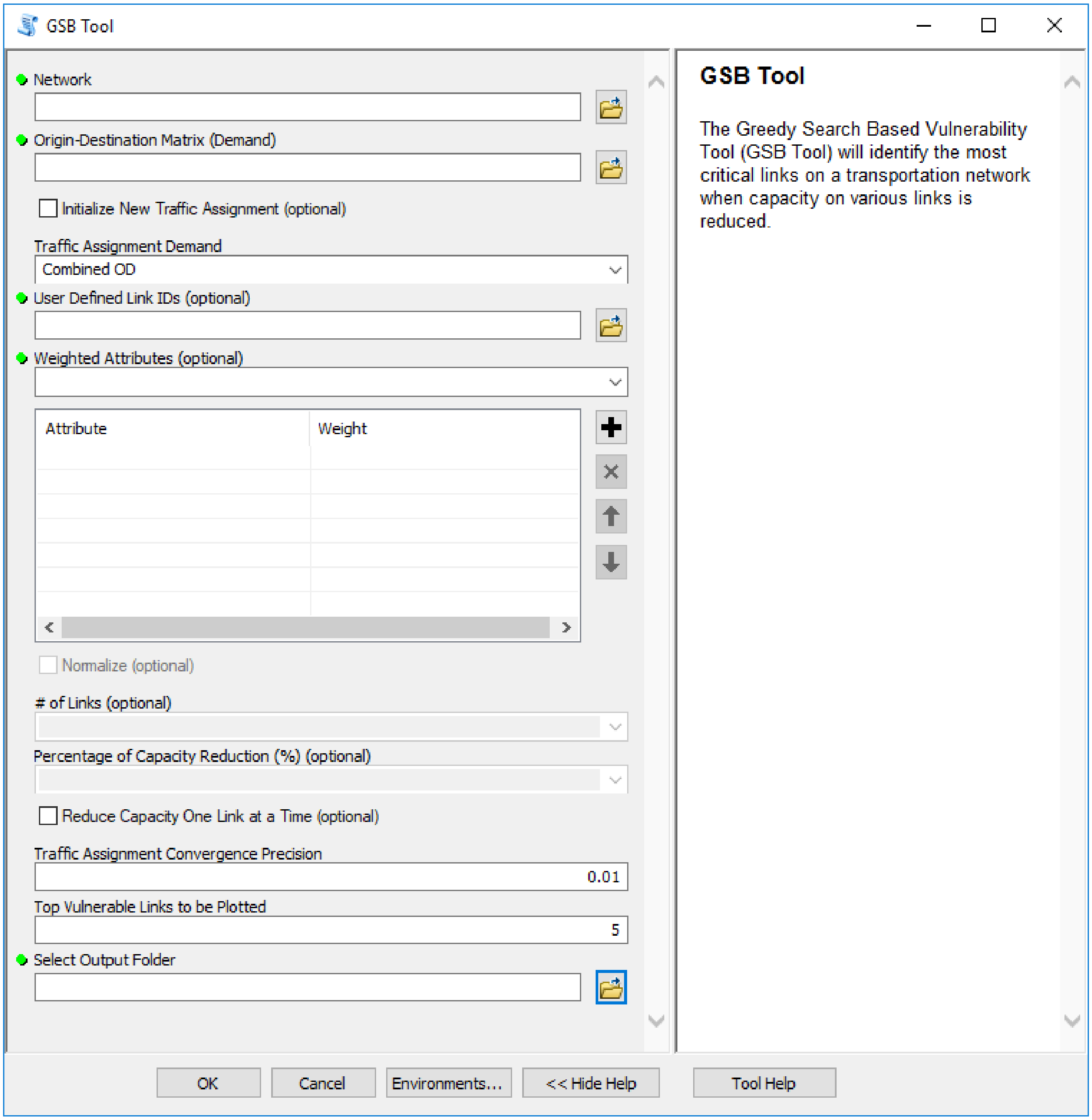


Figure A. 10 GSB Tool

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).

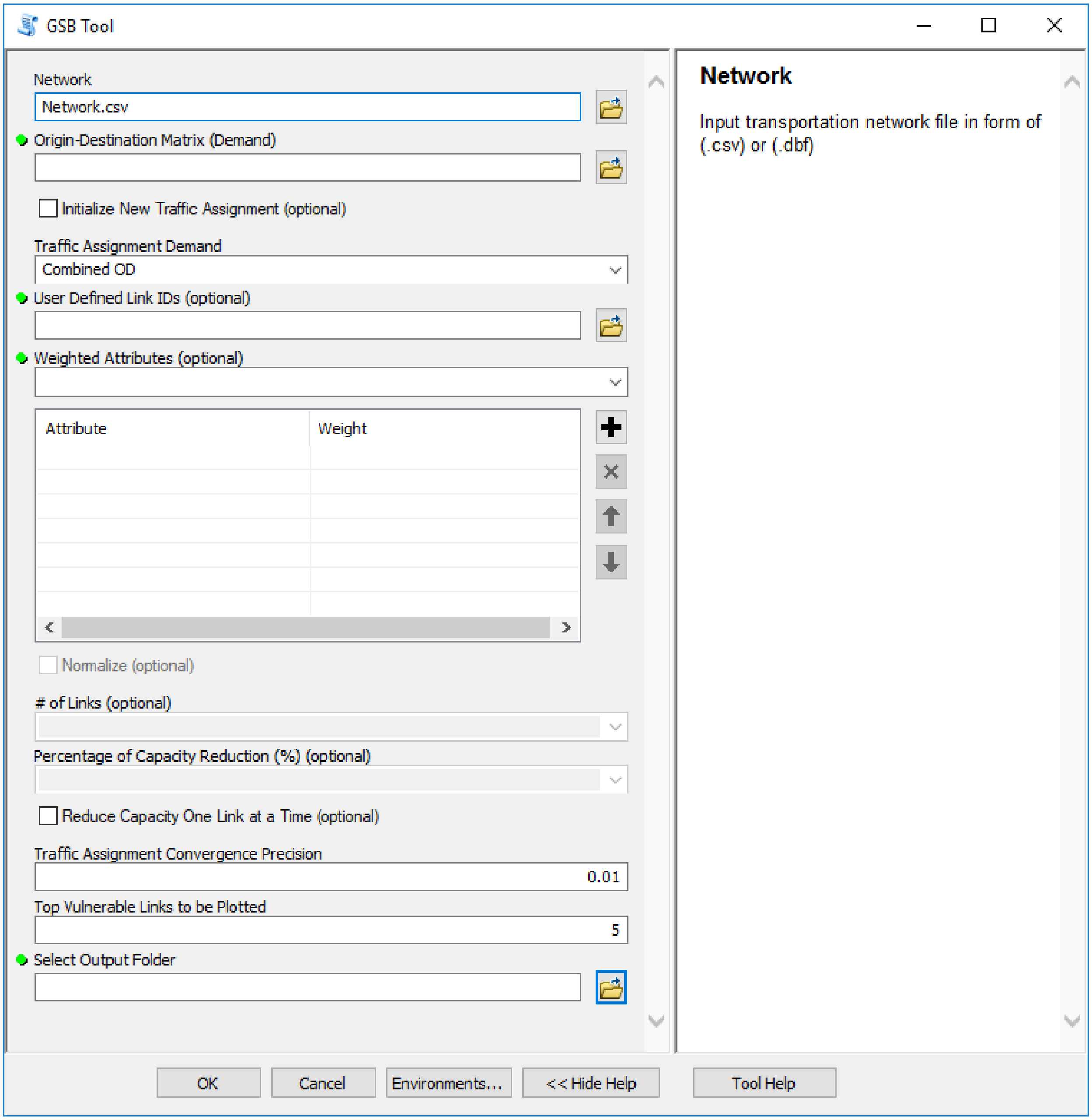


Figure A. 11 Input Network

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).

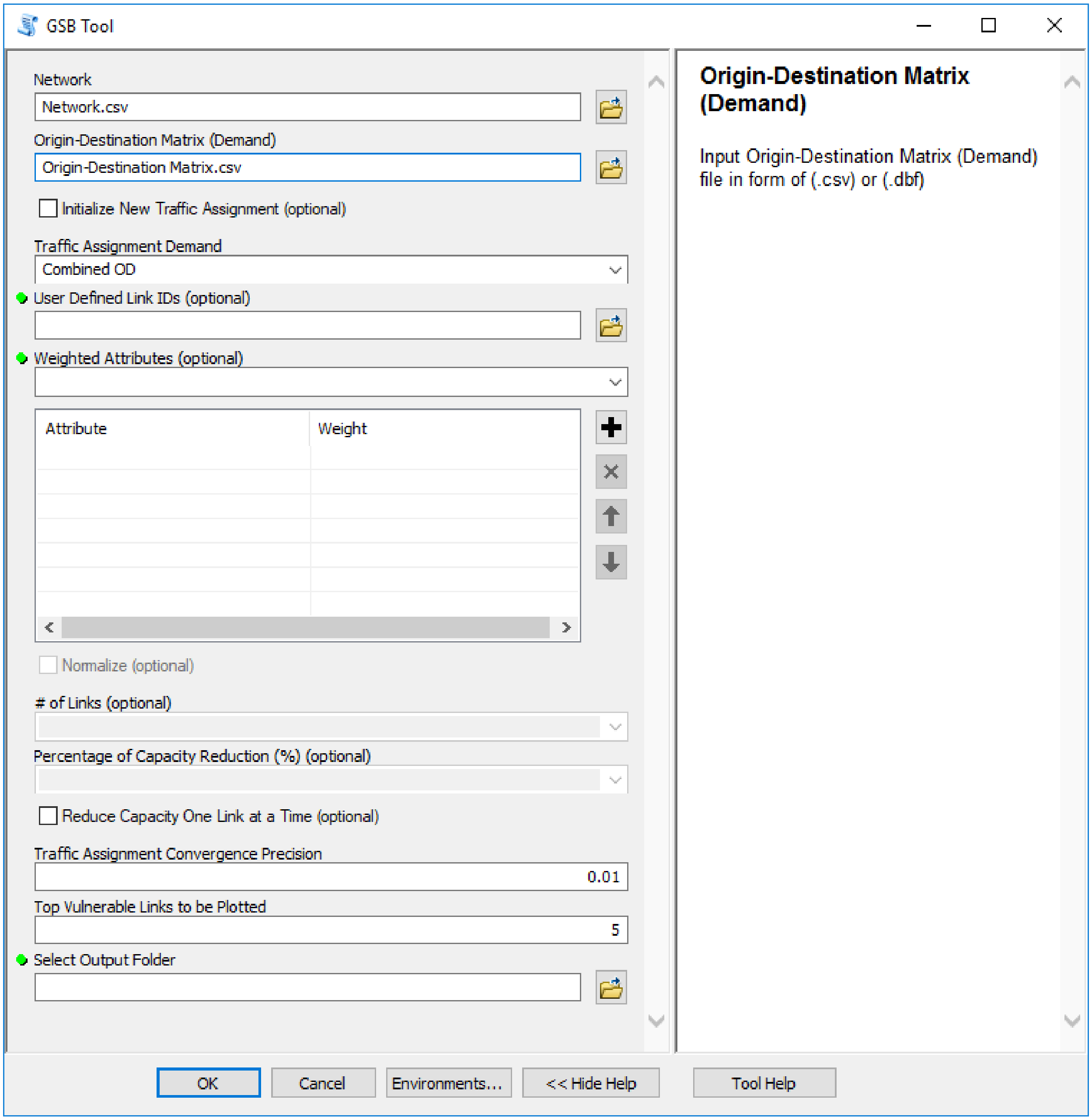


Figure A. 12 Input Origin-Destination Matrix

STEP 4

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).

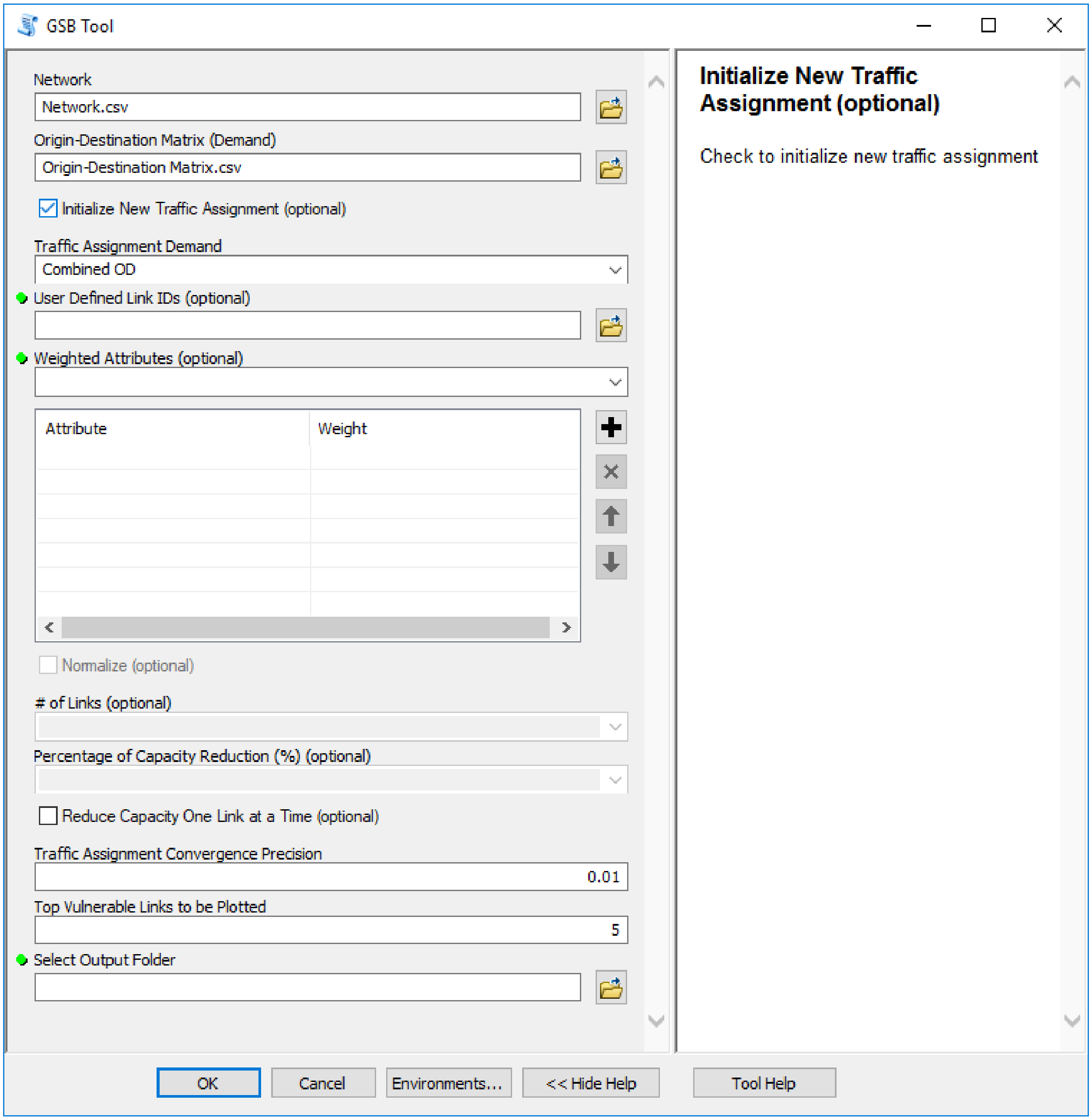


Figure A. 13 Initialize New Traffic Assignment

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.)

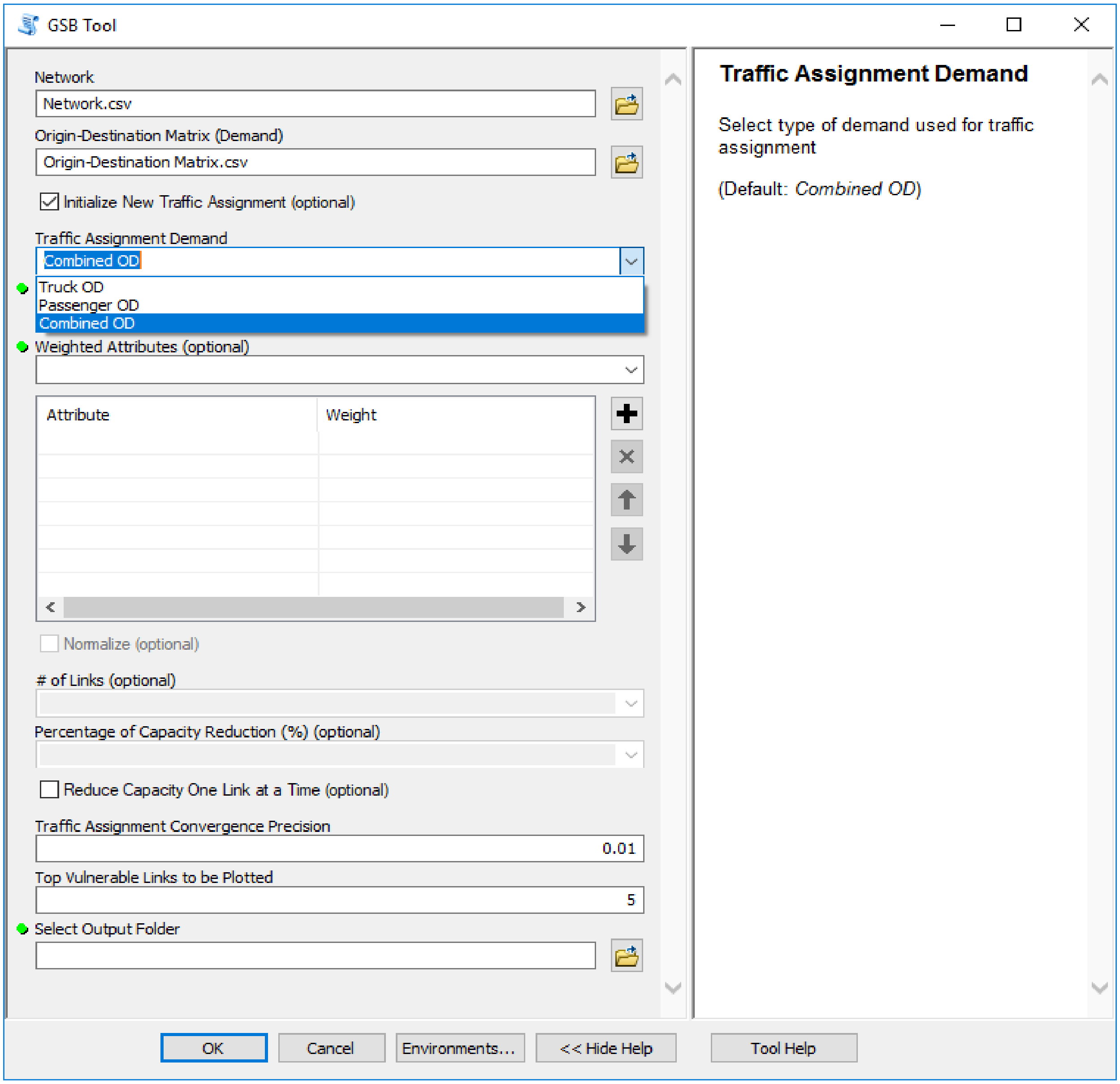


Figure A. 14 Select Type of Demand Used for Traffic Assignment

STEP 6 (Option 1)

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).

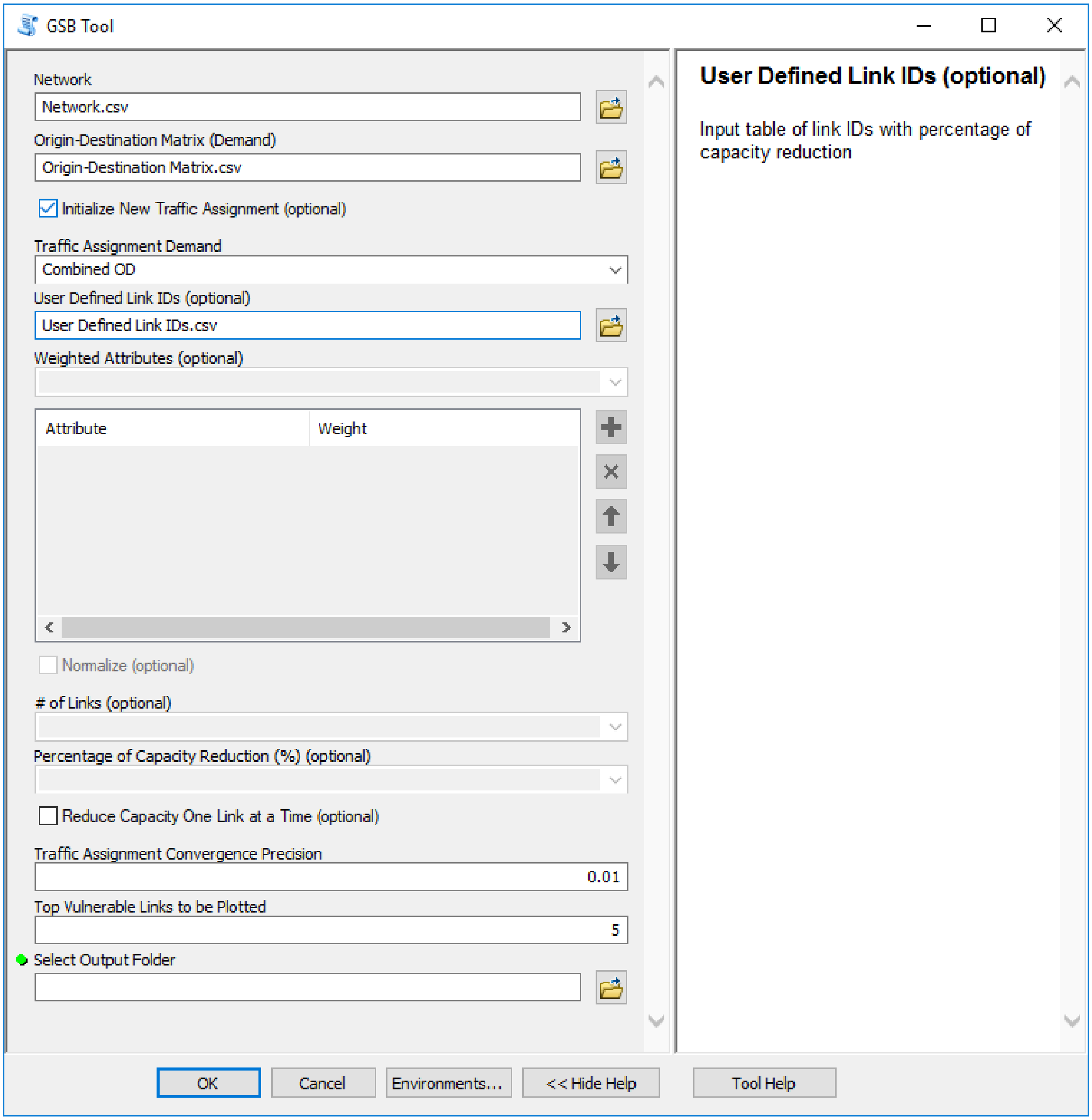


Figure A. 15 Input User Defined Link IDs

STEP 6.1 (Option2)

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

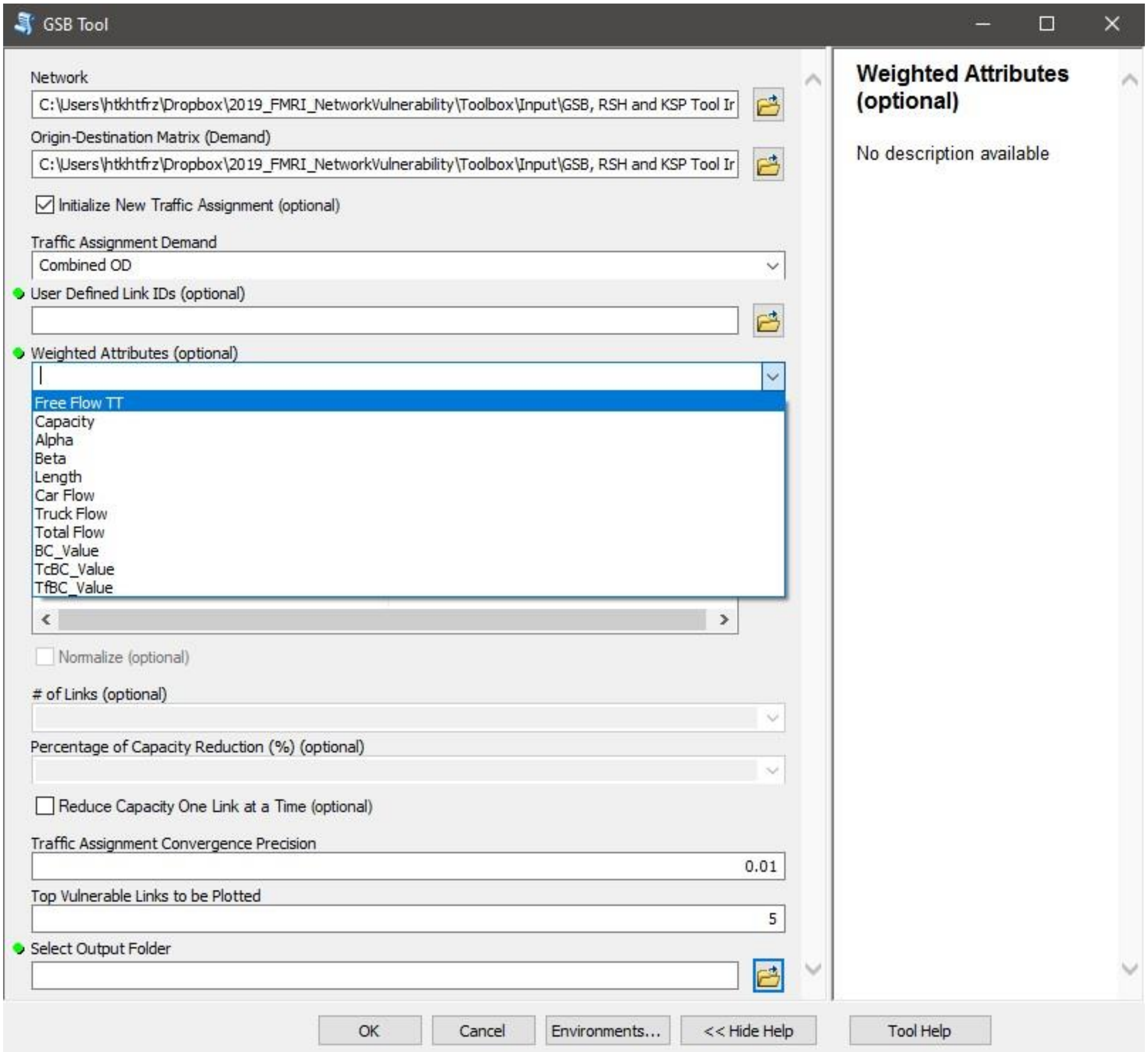


Figure A. 16 Select Attributes

STEP 6.2 (Option 2)

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

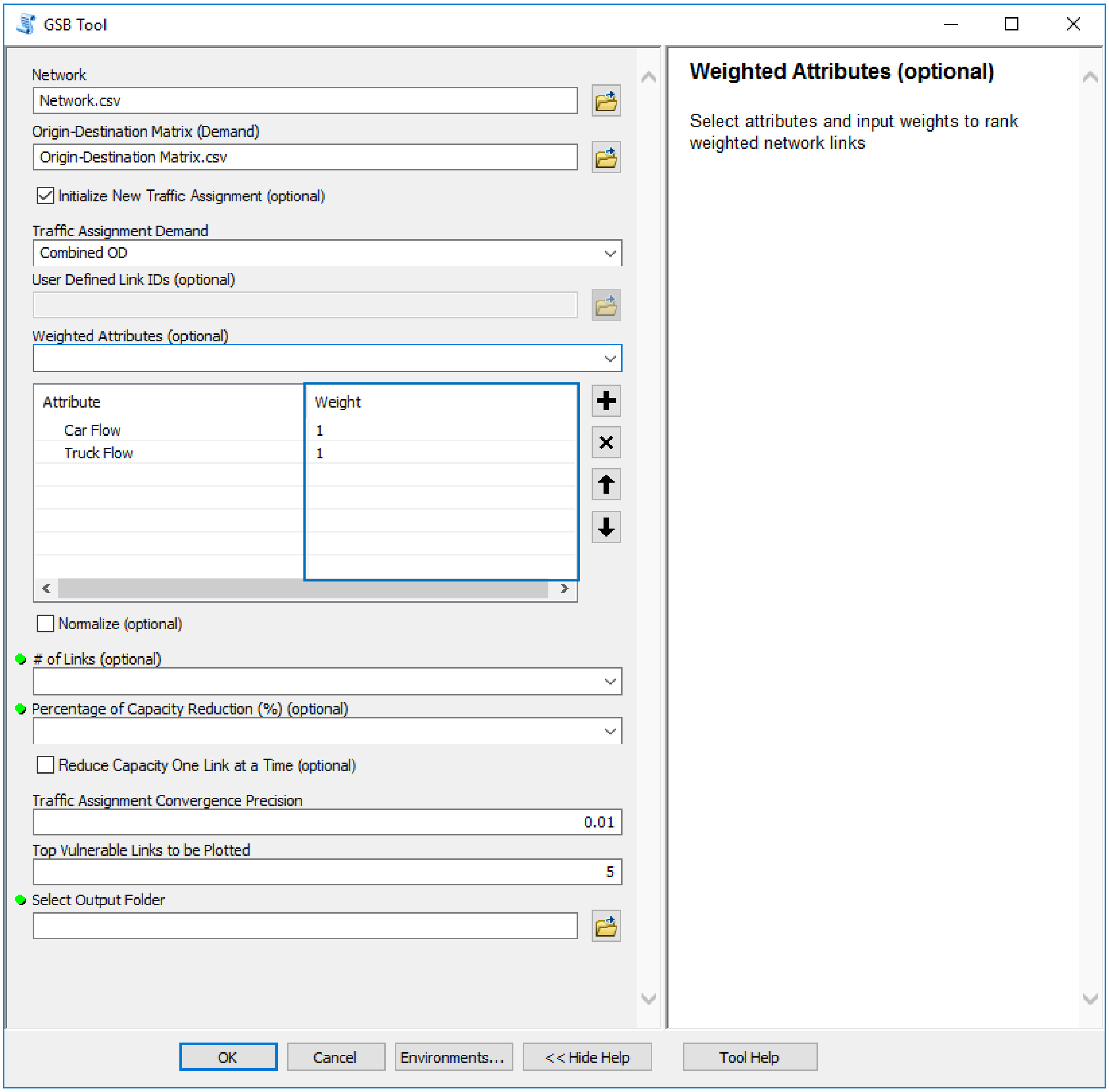


Figure A. 17 Input Weights

STEP 6.3 (Option 2) (Optional)

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

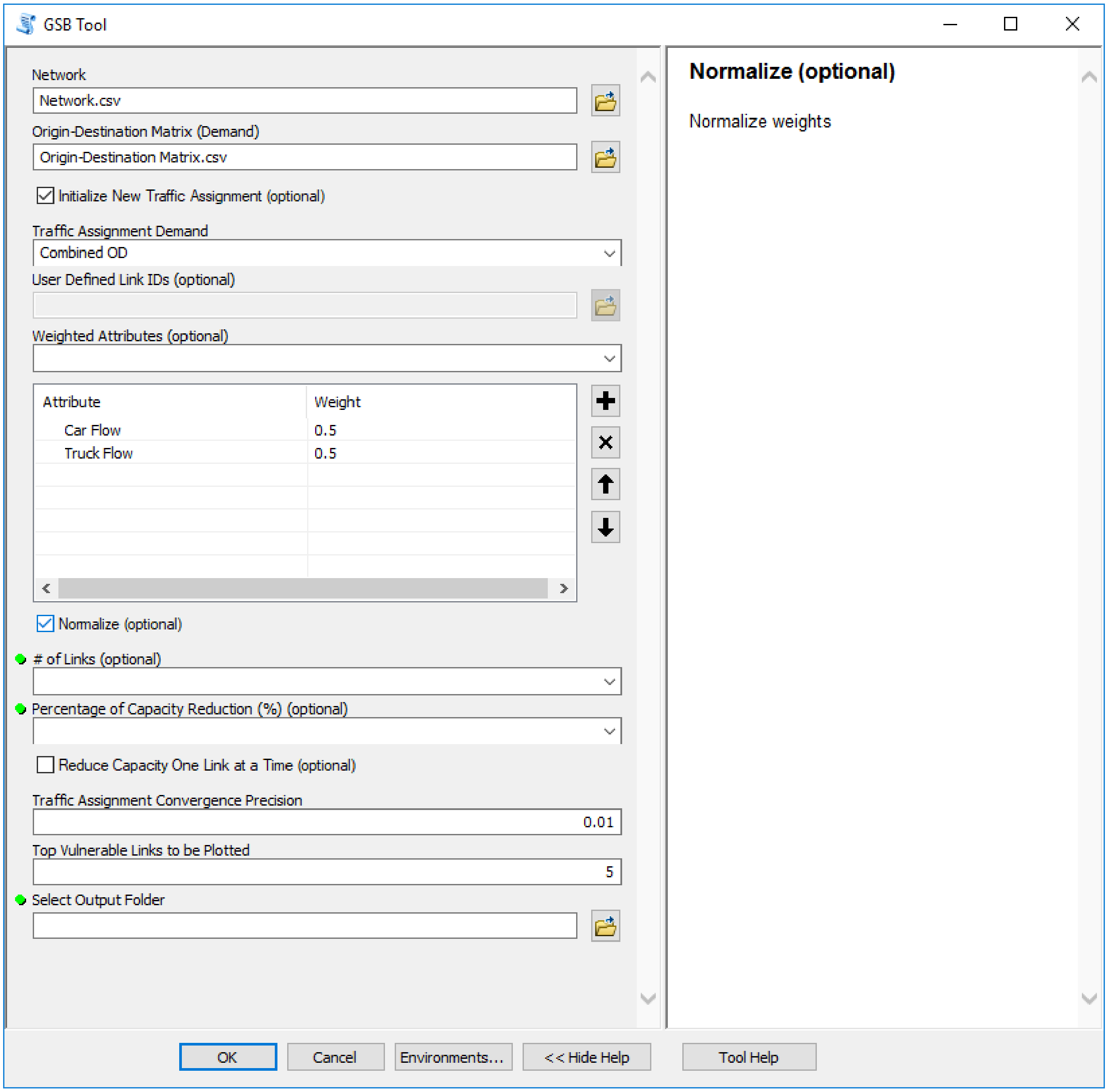


Figure A. 18 Normalize Weights

STEP 7
Select the number of top ranked links used to reduce capacity in input parameter # of Links (see FIGURE A.18).

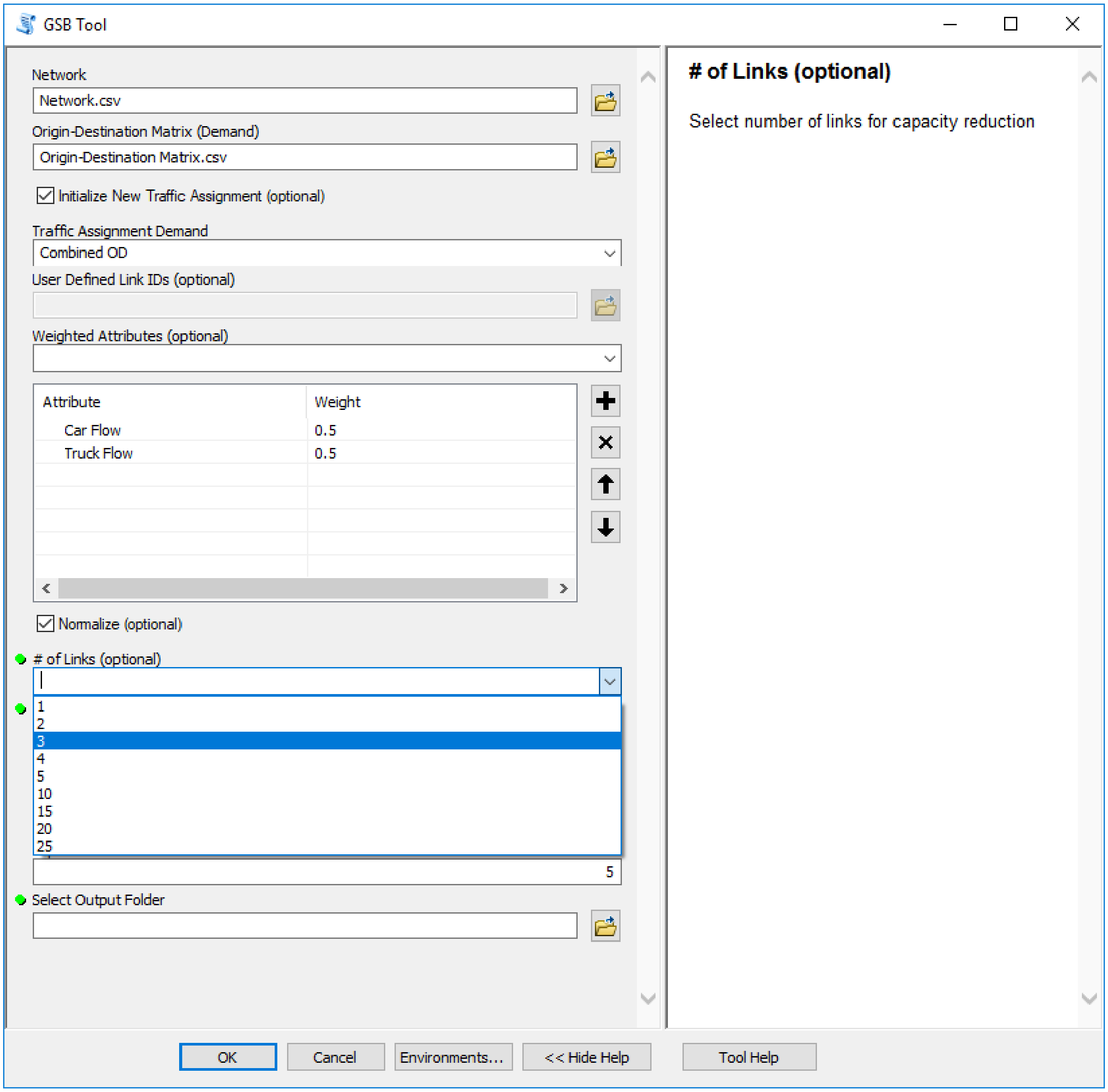


Figure A. 19 Select Number of Links

STEP 8 (Optional)
Select the percentage used to reduce capacity for the top ranked links in input parameter Percentage of Capacity Reduction (%) (see FIGURE A.19).

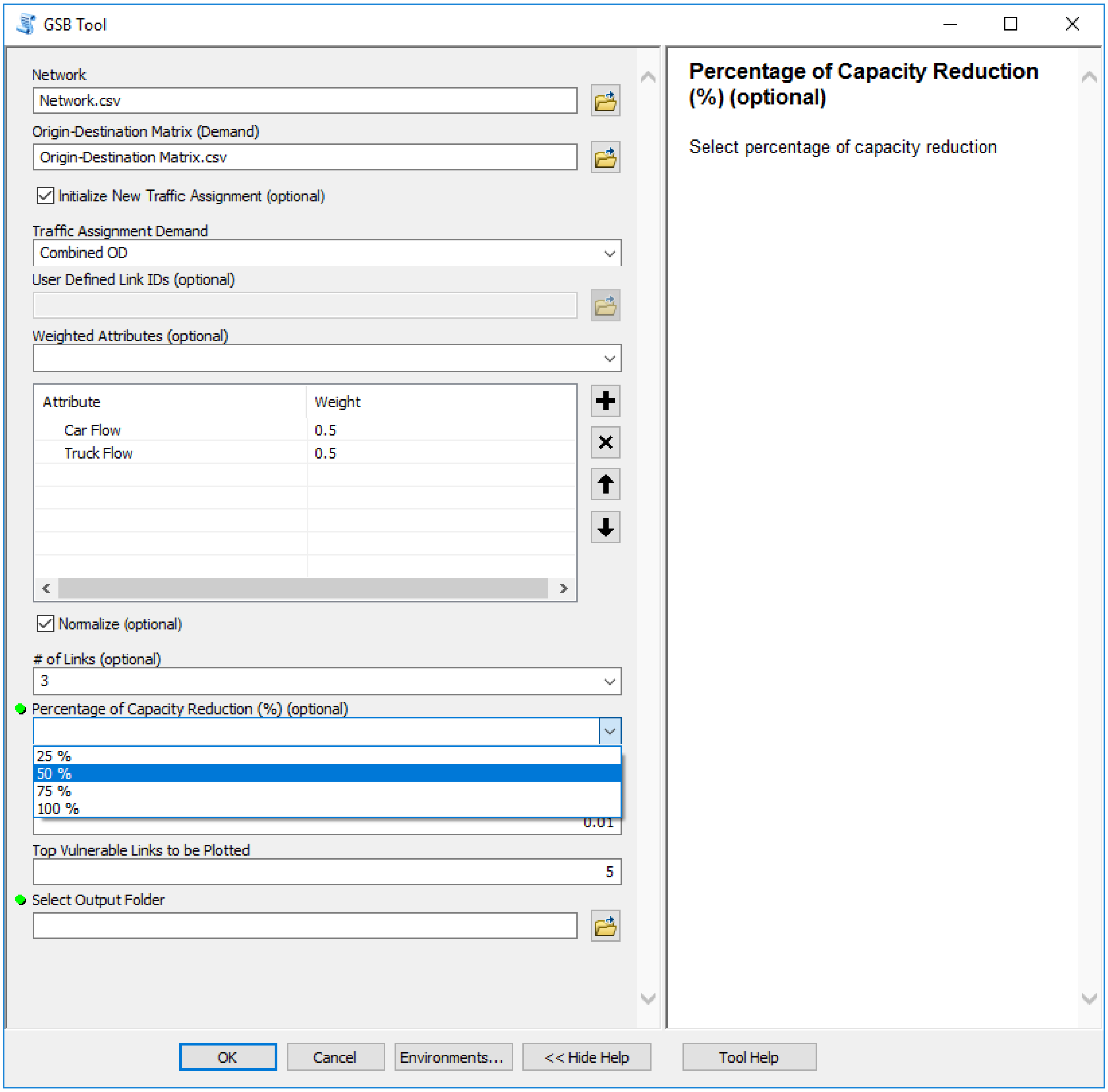


Figure A. 20 Select the Percentage of Capacity Reduction (%)

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)

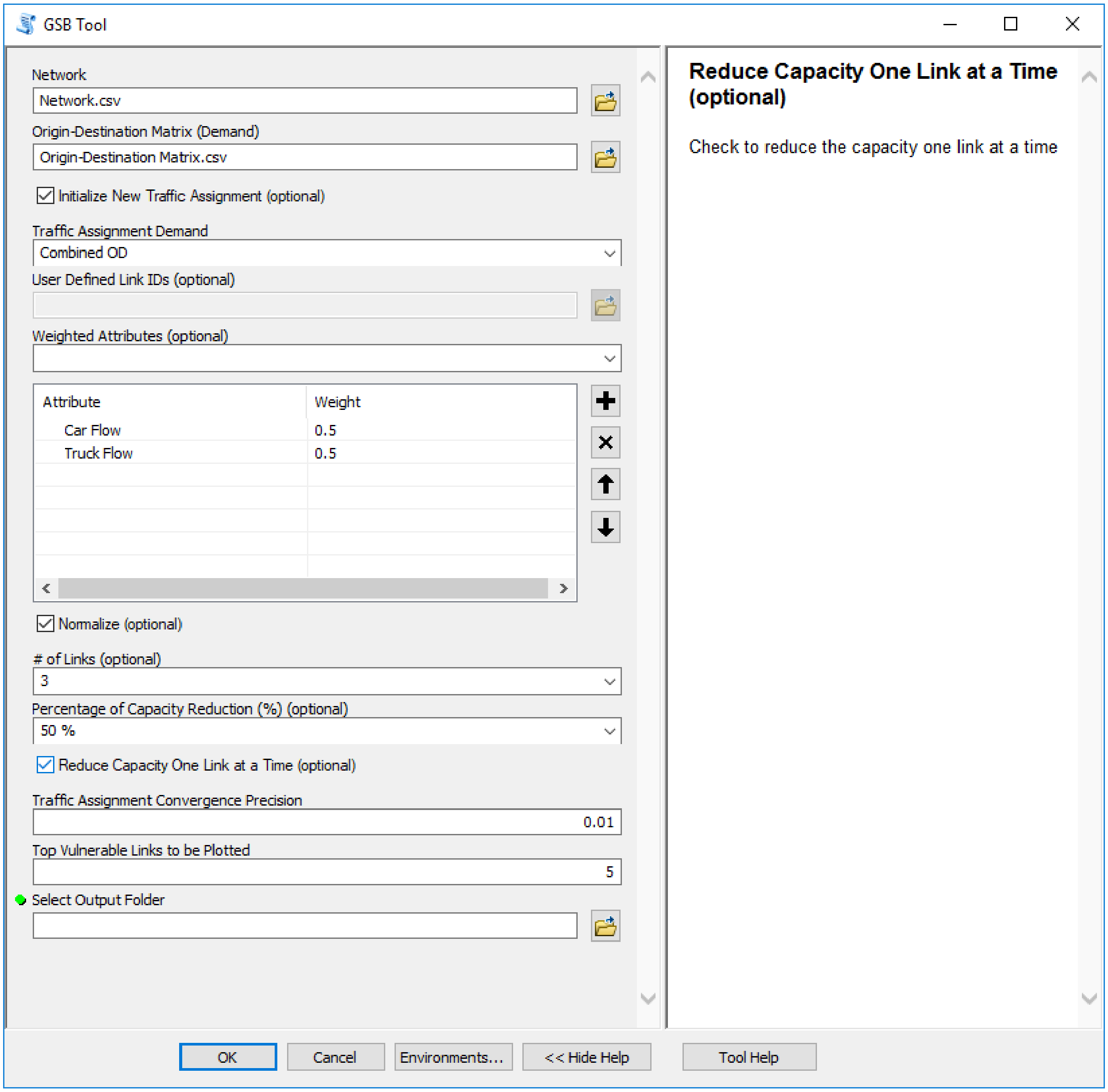


Figure A. 21 Select Reduce Capacity One Link at a Time

STEP 10

Input Traffic Assignment Convergence Precision (see A.FIGURE 21).

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

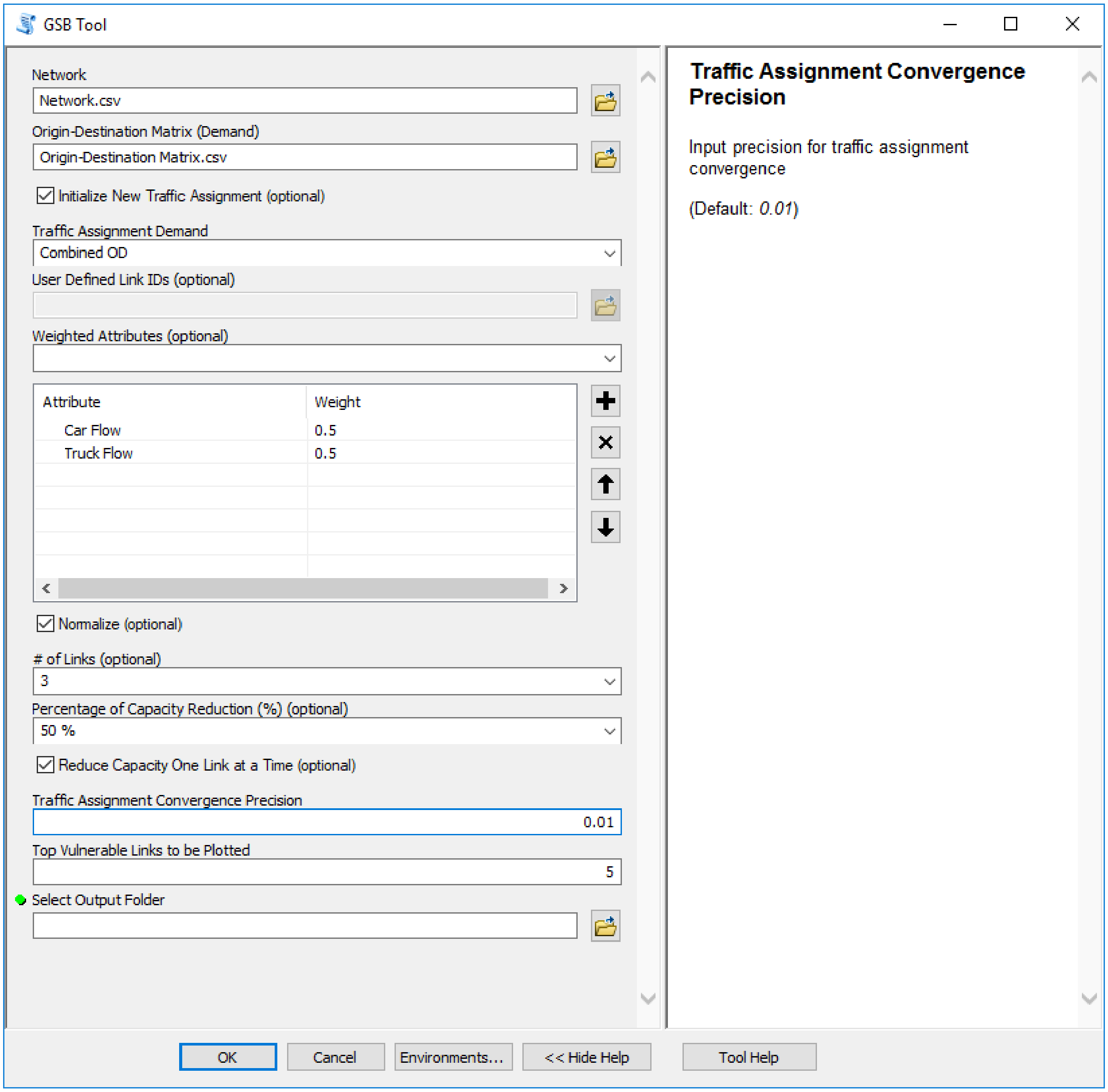


Figure A. 22 Input Traffic Assignment Convergence Precision

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.)

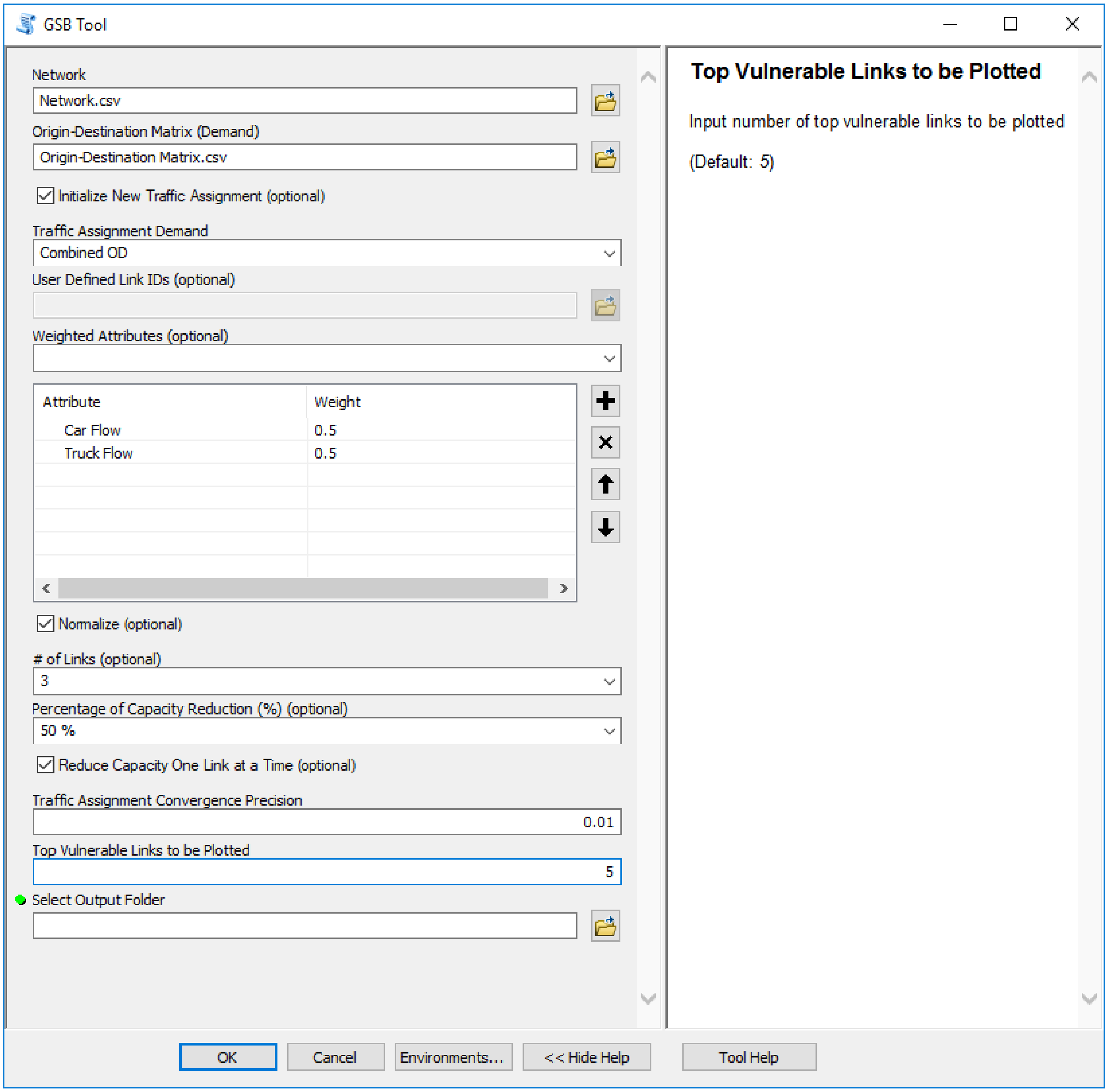


Figure A. 23 Input Top Vulnerable Links to be Plotted

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)

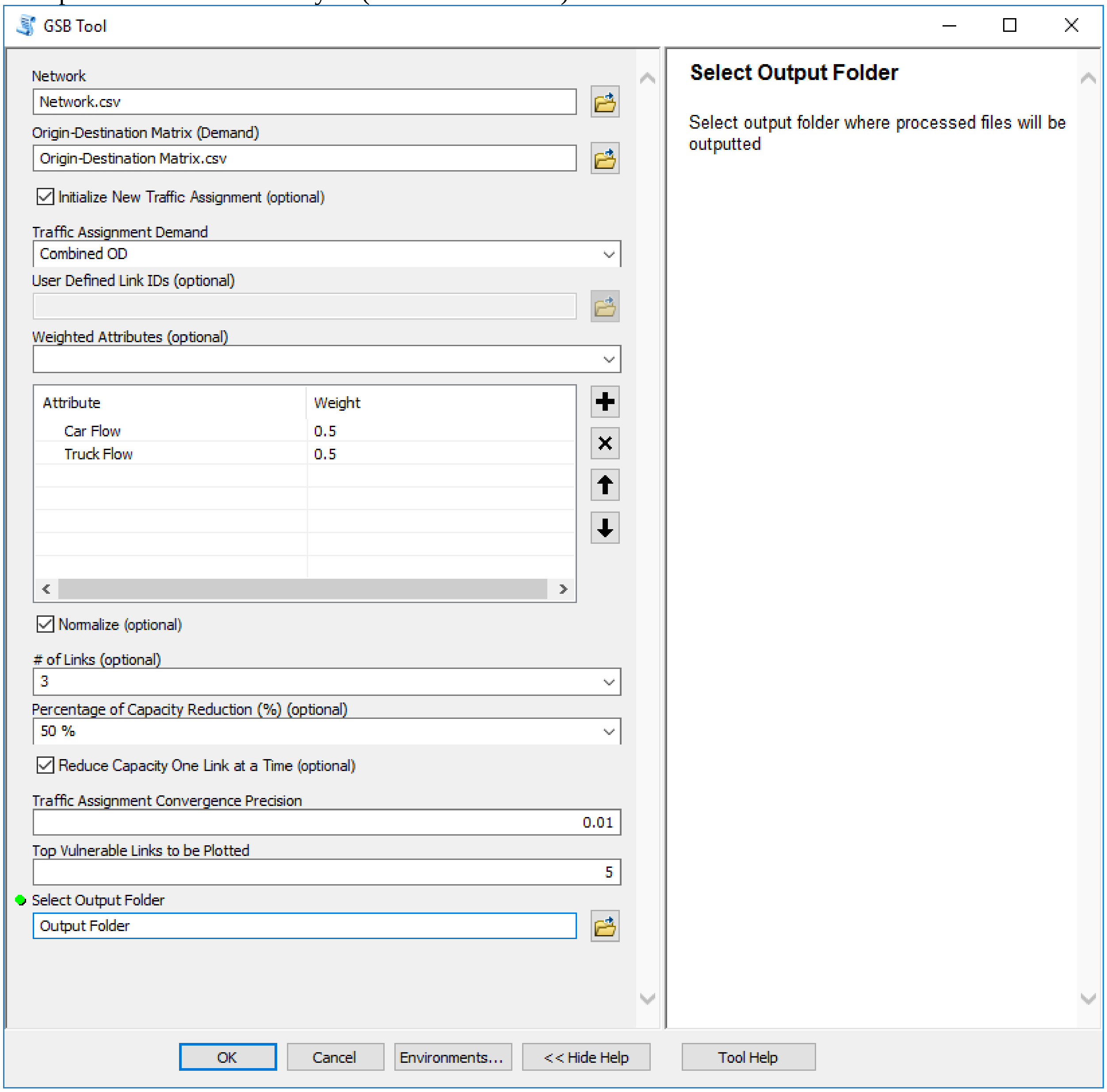


Figure A. 24 Input Output Folder

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.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.

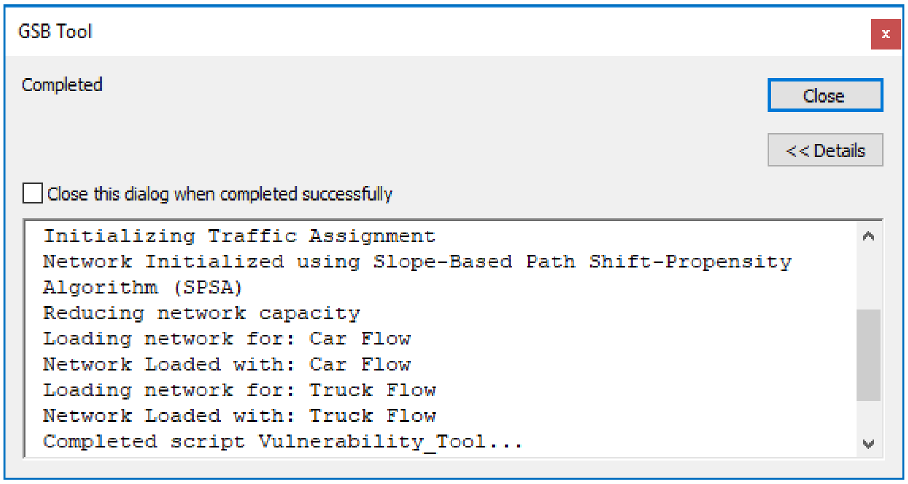


Figure A. 25 Application Performance Task Window

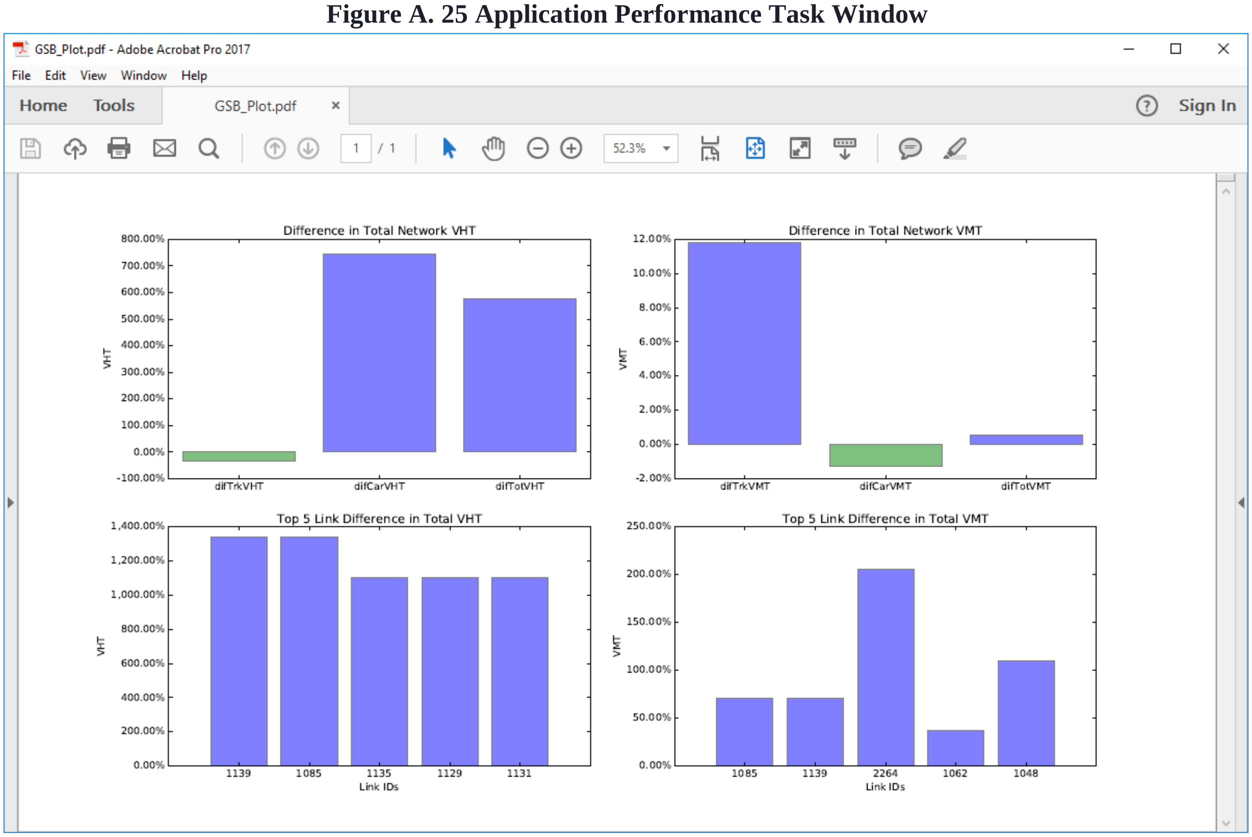


Figure A. 26 GSB Plot

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. 27 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).

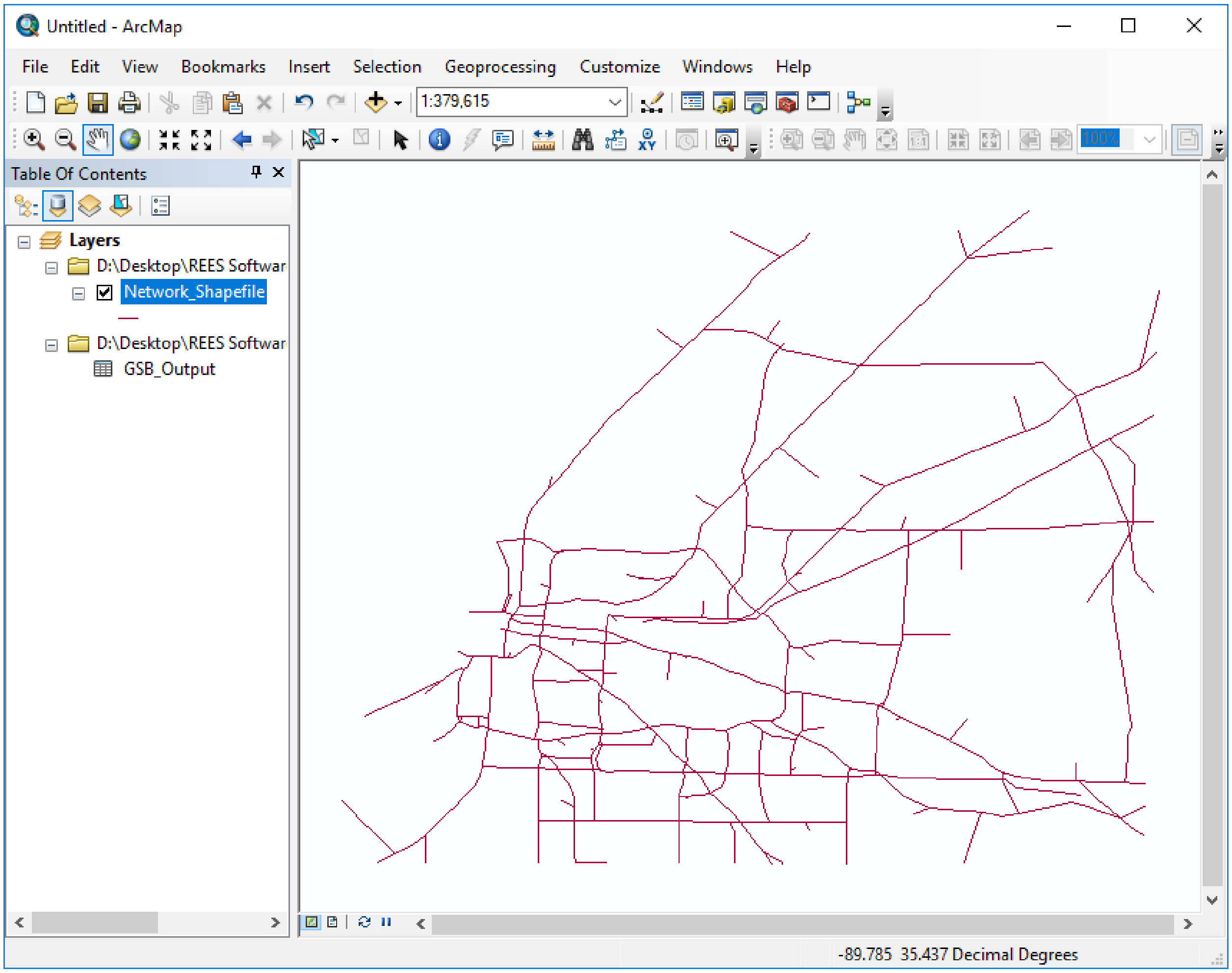
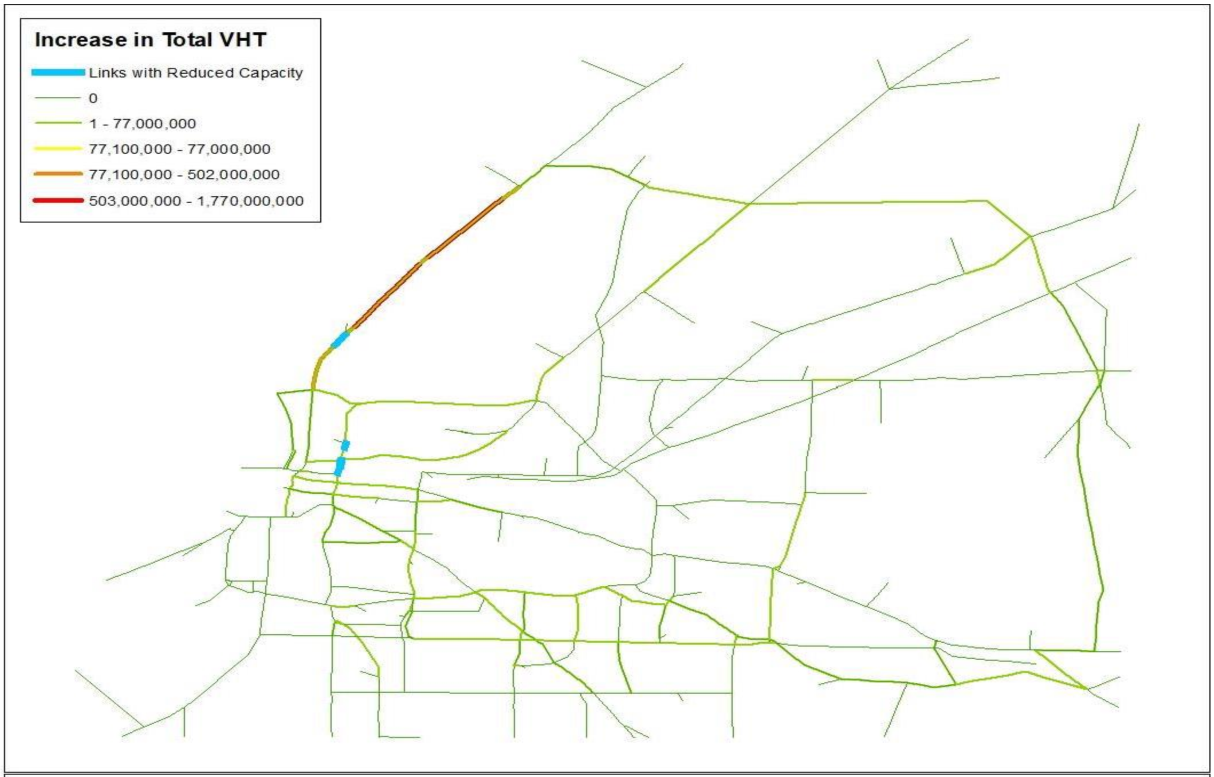


Figure A. 28 Add Network in a Form of Shapefile



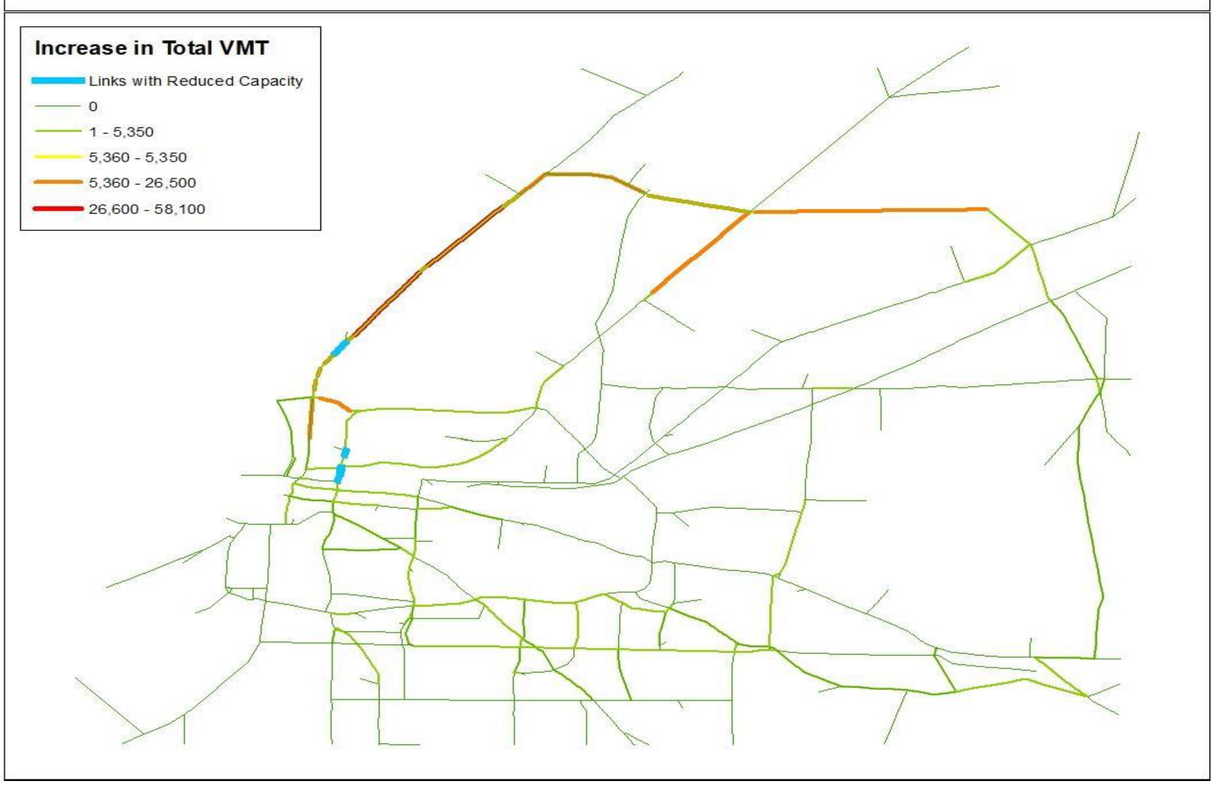


Figure A. 29 Visualize the GSB Tool Output

Table A. 1 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 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), BC_Value, TcBC_Value, TfBC_Value.
- **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.

Network

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	1	141379	142406	0.041364	3337	0.15	4	0.047706	0	0	0	0.041364	0	0.821962	0.482347	0.657284
2	2	142406	142414	0.027632	3337	0.15	4	0.031869	0	0	0	0.027632	0	0.355599	0.660492	0.482533
3	3	142414	142422	0.086236	3337	0.15	4	0.099459	0	0	0	0.086236	0	0.650124	0.779115	0.780163
4	4	142422	142430	0.077587	3337	0.15	4	0.089483	0	0	0	0.077587	0	0.557517	0.191432	0.367302
5	5	142430	126024	0.010867	3337	0.15	4	0.012533	0	0	0	0.010867	0	0.116366	0.63095	0.308477
6	6	142446	142454	0.06596	3337	0.15	4	0.076074	2491.711	393.9045	2885.616	0.077615	0	0.477959	0.726416	0.012675
7	7	126024	142446	0.017417	3337	0.15	4	0.020088	2491.711	393.9045	2885.616	0.020495	0	0.403571	0.629403	0.495337
8	8	142454	142462	0.085637	3337	0.15	4	0.098768	2491.711	393.9045	2885.616	0.100769	0	0.43192	0.783151	0.853322
9	9	142462	126032	0.085654	3284	0.15	4	0.098788	2491.711	393.9045	2885.616	0.10179	0	0.419067	0.374623	0.613474
10	10	126024	142478	1.026567	2063	0.15	4	0.732285	0	0	0	1.026567	0	0.613408	0.594797	0.078215
11	11	126064	142478	0.275331	2407	0.15	4	0.196403	0	0	0	0.275331	0	0.966455	0.152812	0.259674

Origin-Destination Matrix

	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
14	5896	49445	74.20526	5.027403	79.23266

User Defined Link IDs

	A	B
1	6	100
2	23	100
3	64	100

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

Table

Network_Shapefile_Conversion1

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector	BC_Value	TcBC_Value	TfBC_Value
0	1	332761	332886	2.59158	3953.300971	0.15	4	2.567685	9388.449217	1841.200848	11229.650065	0	0	0.376848	0.391641	0.060618
1	2	1002518	332971	4.789769	40000	0.15	4	2.197628	1759.76305	0	1759.76305	0	1	0.75827	0.989861	0.04535
2	3	1002518	333184	4.789769	40000	0.15	4	4.215873	4866.279561	1383.315105	6249.594665	0	1	0.857871	0.022984	0.105641
3	4	332817	333286	6.12815	3063.550015	0.15	4	4.678201	5.838744	0	5.838744	0	0	0.865795	0.441096	0.048466
4	5	2004157	332761	4.624162	40000	0.15	4	2.970565	2000.36132	138.722257	2139.083578	0	1	0.90163	0.34168	0.821565
5	6	332817	332761	1.00086	3063.550015	0.15	4	0.764052	717.936625	41.909628	759.846254	0	0	0.732036	0.511546	0.064673
6	7	334809	334787	0.818759	2088.769535	0.15	4	0.240831	3830	0	3830	0.818839	0	0.418688	0.408399	0.186608
7	8	2004985	334609	0.819589	974.855054	0.15	4	0.23898	910	0	910	0.819593	0	0.82068	0.978727	0.907915
8	9	363190	363366	4.340041	1573.076839	0.15	4	3.799525	2358.540768	86.459232	2445	4.340099	0	0.63138	0.656284	0.366855
9	10	360017	362484	4.100412	3953.300971	0.15	4	4.062604	8683.055147	354.545053	9037.600199	0	0	0.228821	0.280476	0.178346
10	11	336031	2004536	0.6293	2909.618624	0.15	4	0.194016	7481.055927	1148.944073	8630	0.629766	0	0.177542	0.390309	0.137624
11	12	2004534	335601	0.158663	3067.695163	0.15	4	0.107305	2351.435852	103.564148	2455	0.158663	0	0.323842	0.778963	0.55309
12	13	334477	334455	0.828151	1046.932736	0.15	4	0.244639	4266.009025	93.990975	4360	0.831331	0	0.515847	0.504931	0.971651
13	14	361353	361513	0.315566	1528.714201	0.15	4	0.251904	312.351897	2.648103	315	0.315566	0	0.325294	0.754768	0.336248

1 (0 out of 18826 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. 31 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and lunch RSH Tool (see FIGURE A.31)

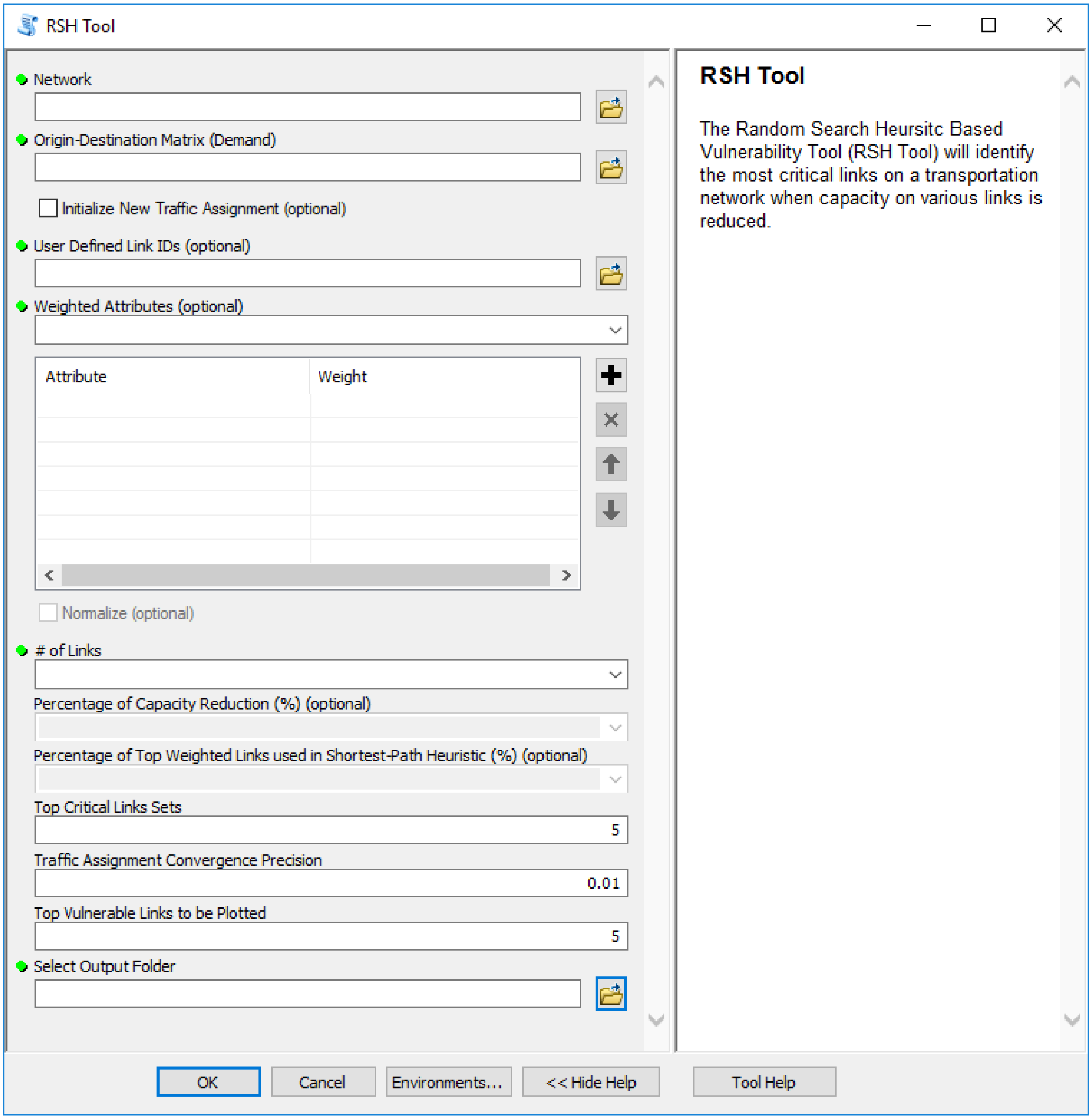


Figure A. 32 RSH Tool

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).

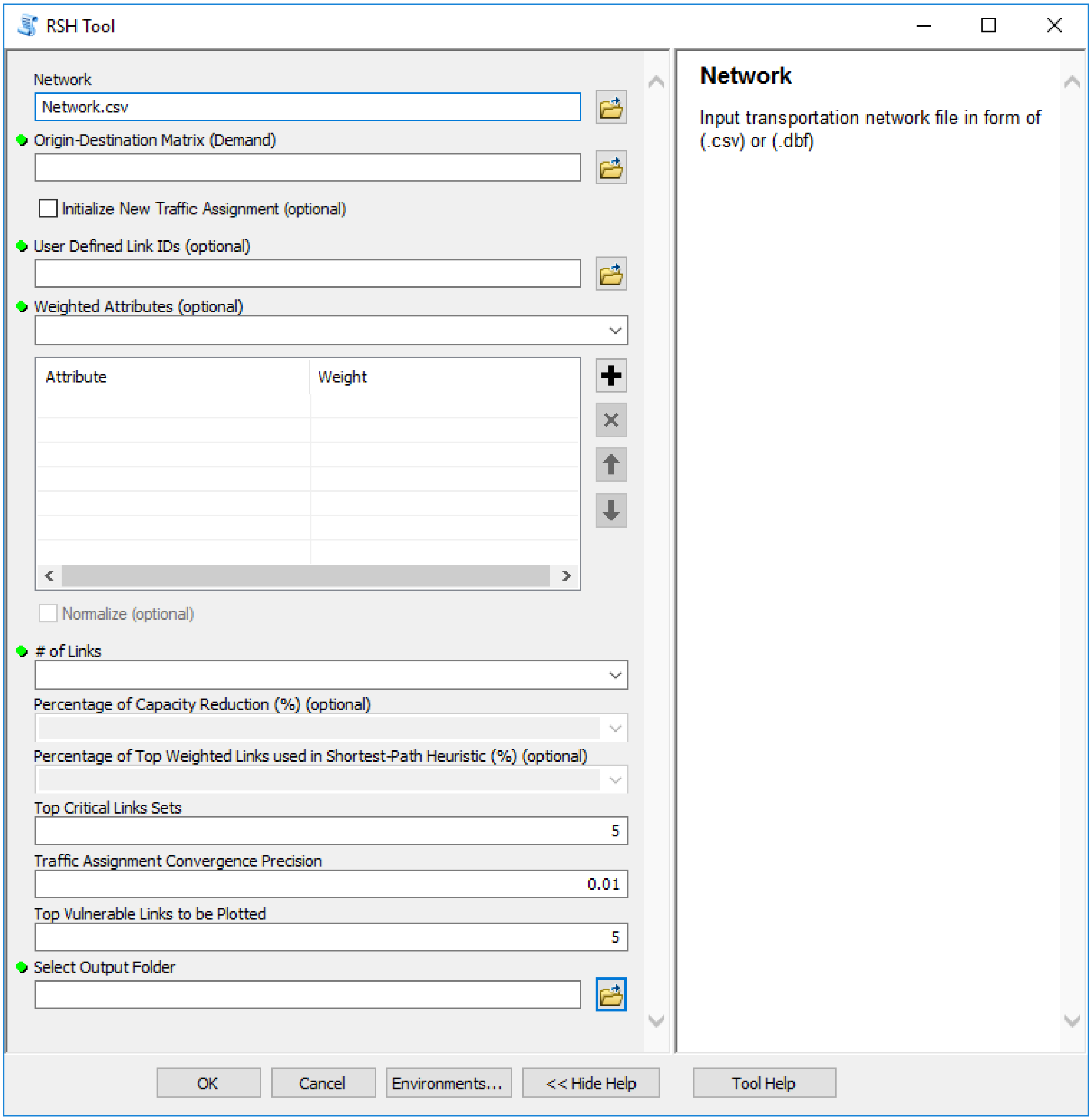


Figure A. 33 Input Network

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).

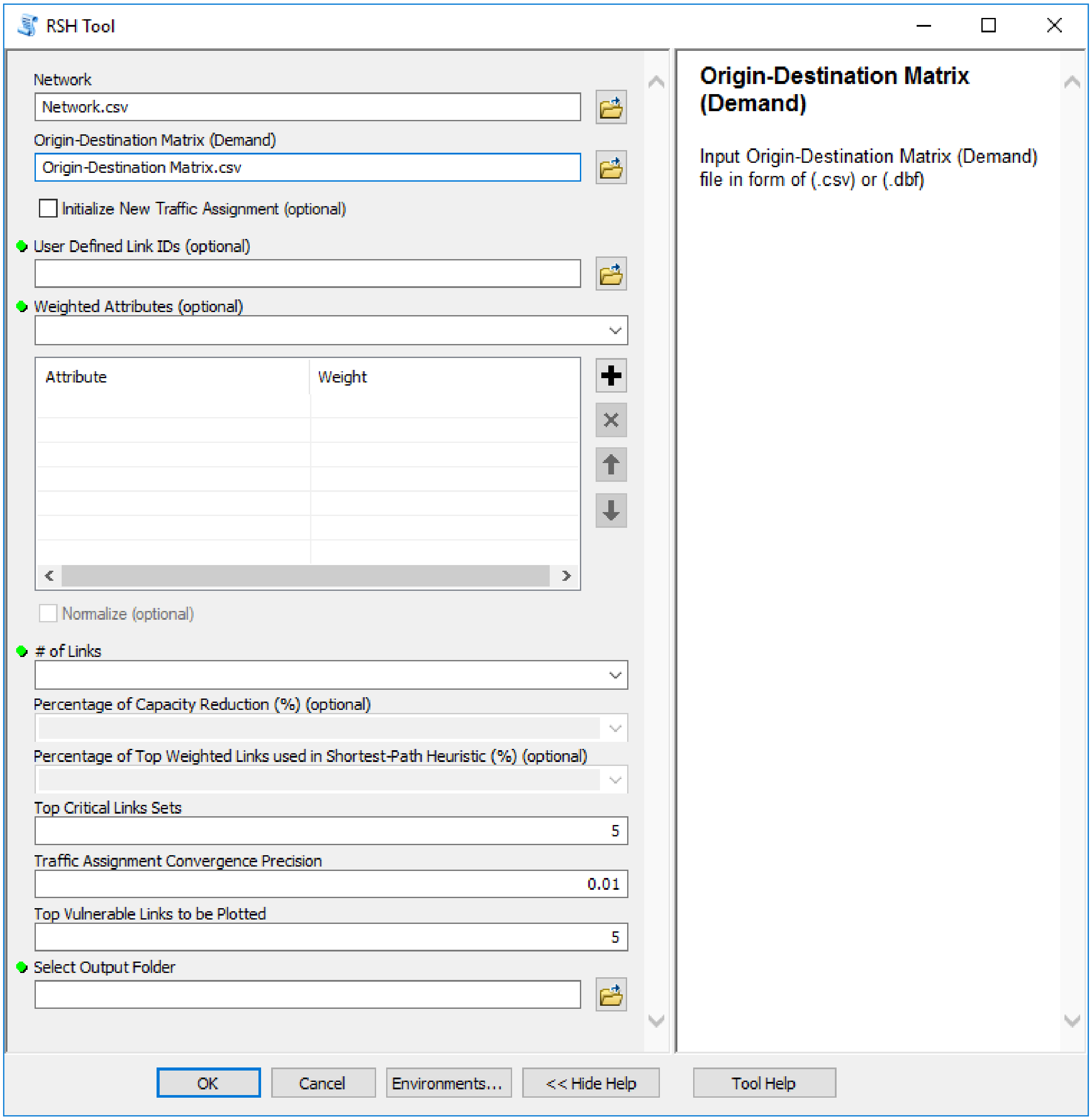


Figure A. 34 Input Origin-Destination Matrix

STEP 4 (Optional)
Select option to Initialize New Traffic Assignment if user wishes use a new traffic assignment initialized by Random Search Heuristic Based Vulnerability Tool (see FIGURE A.34).

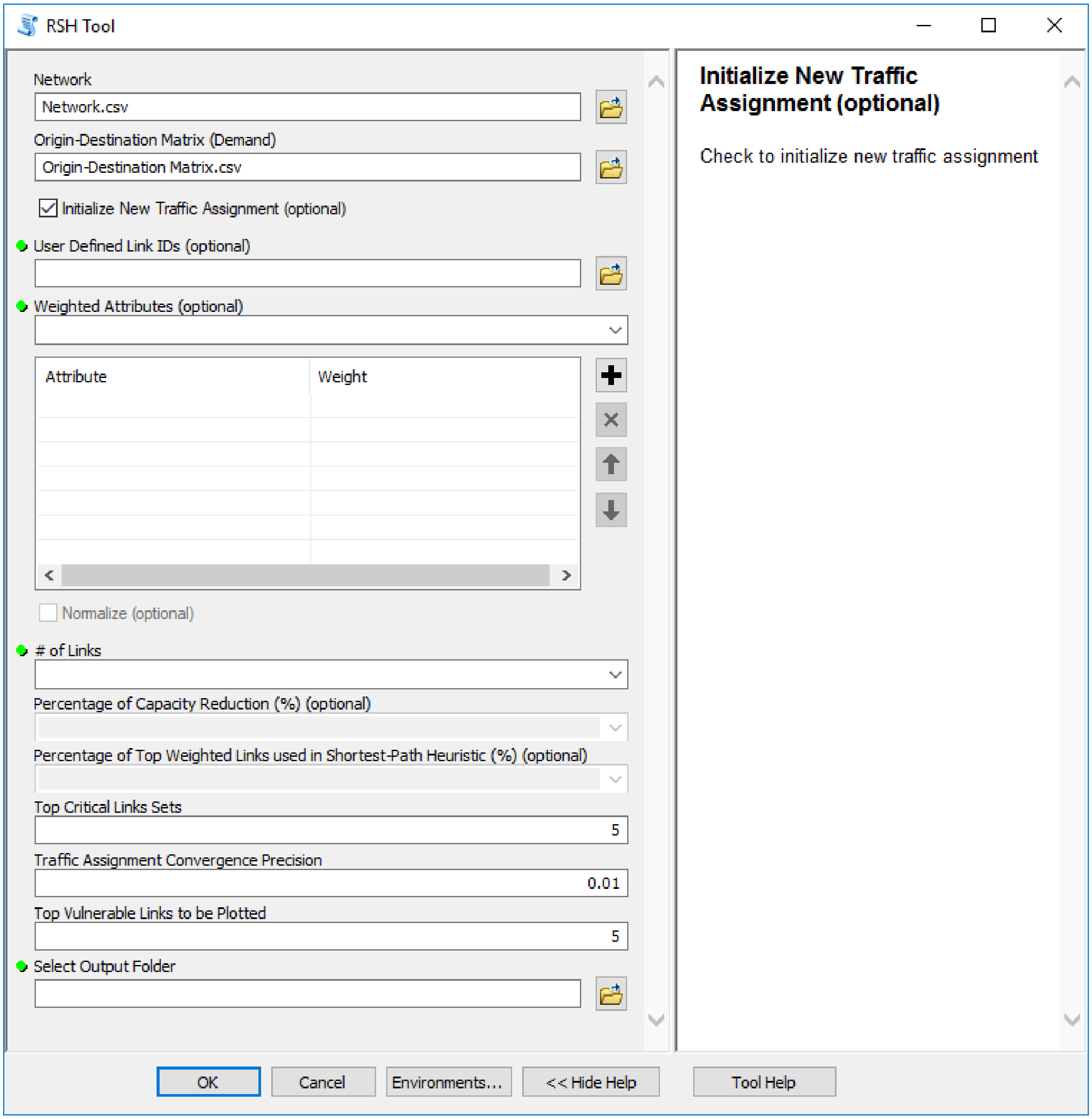


Figure A. 35 Initialize New Traffic Assignment

STEP 5 (Option 1)
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).

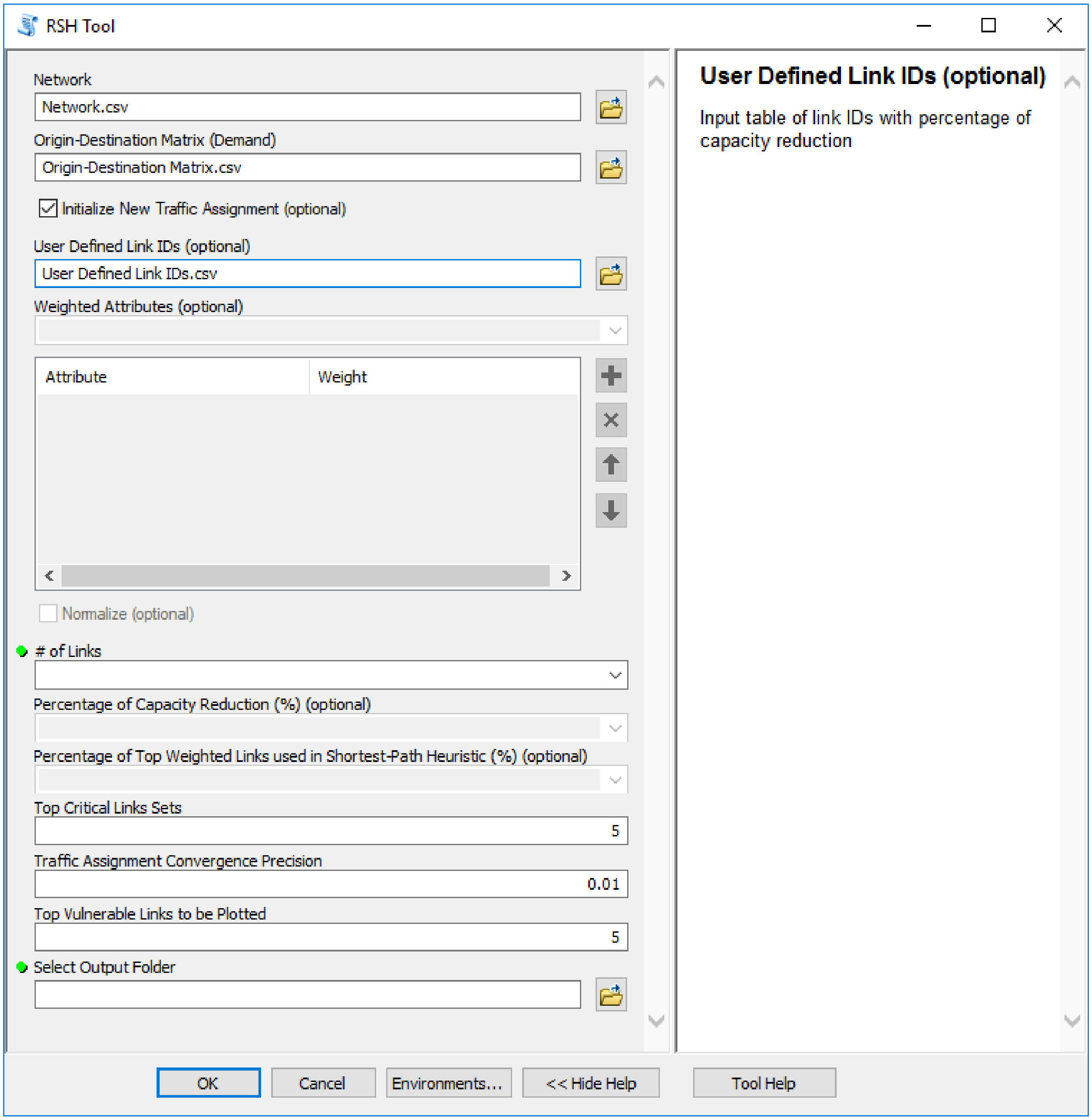


Figure A. 36 Input User Defined Link IDs

STEP 5.1 (Option 2)
Select attributes from input parameter Weighted Attributes drop down list (see FIGURE A.36).

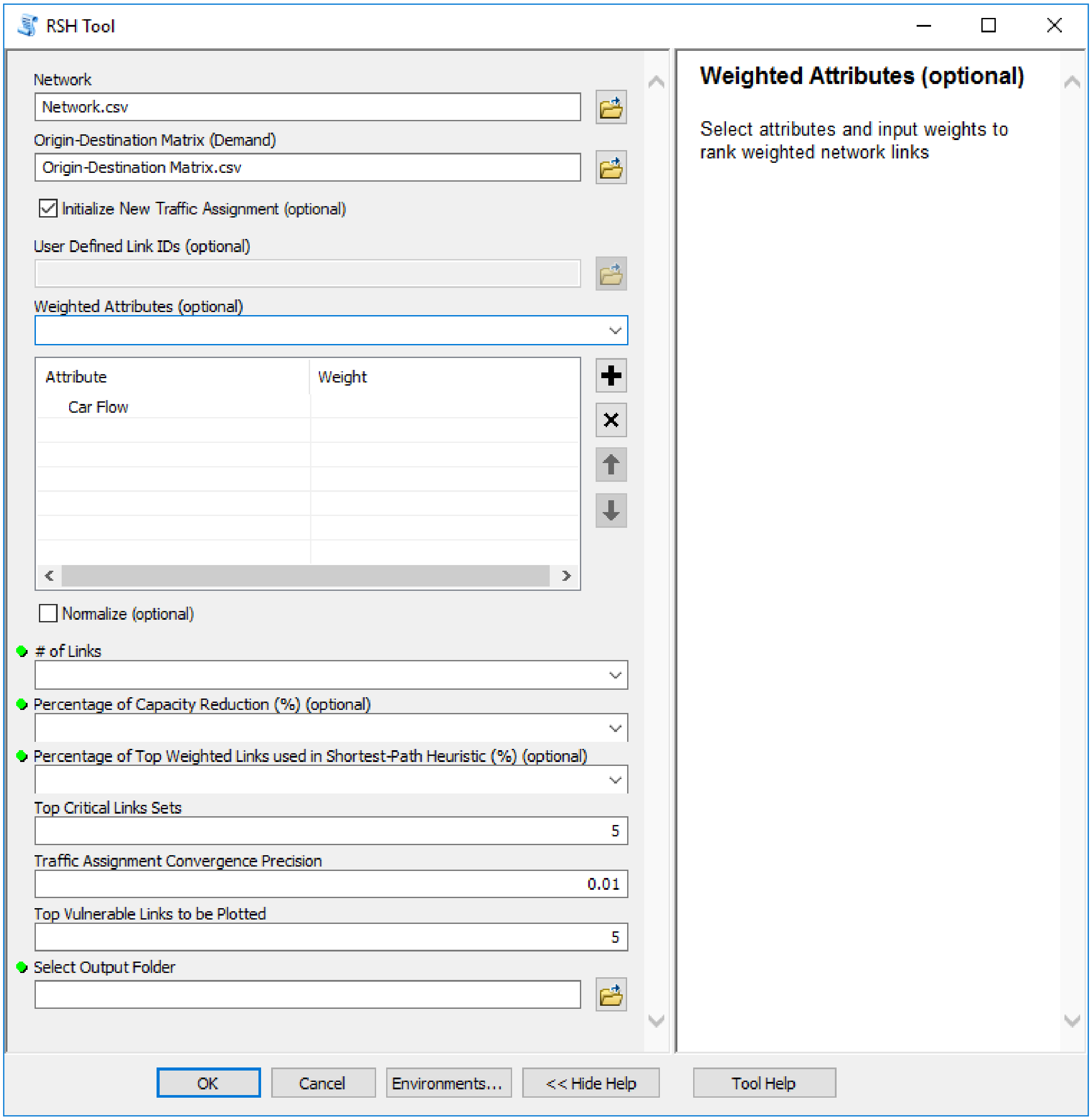


Figure A. 37 Select Attributes

STEP 5.2 (Option 2)
Input weights for selected field attributes in input parameter Weighted Attributes (see FIGURE A.37).

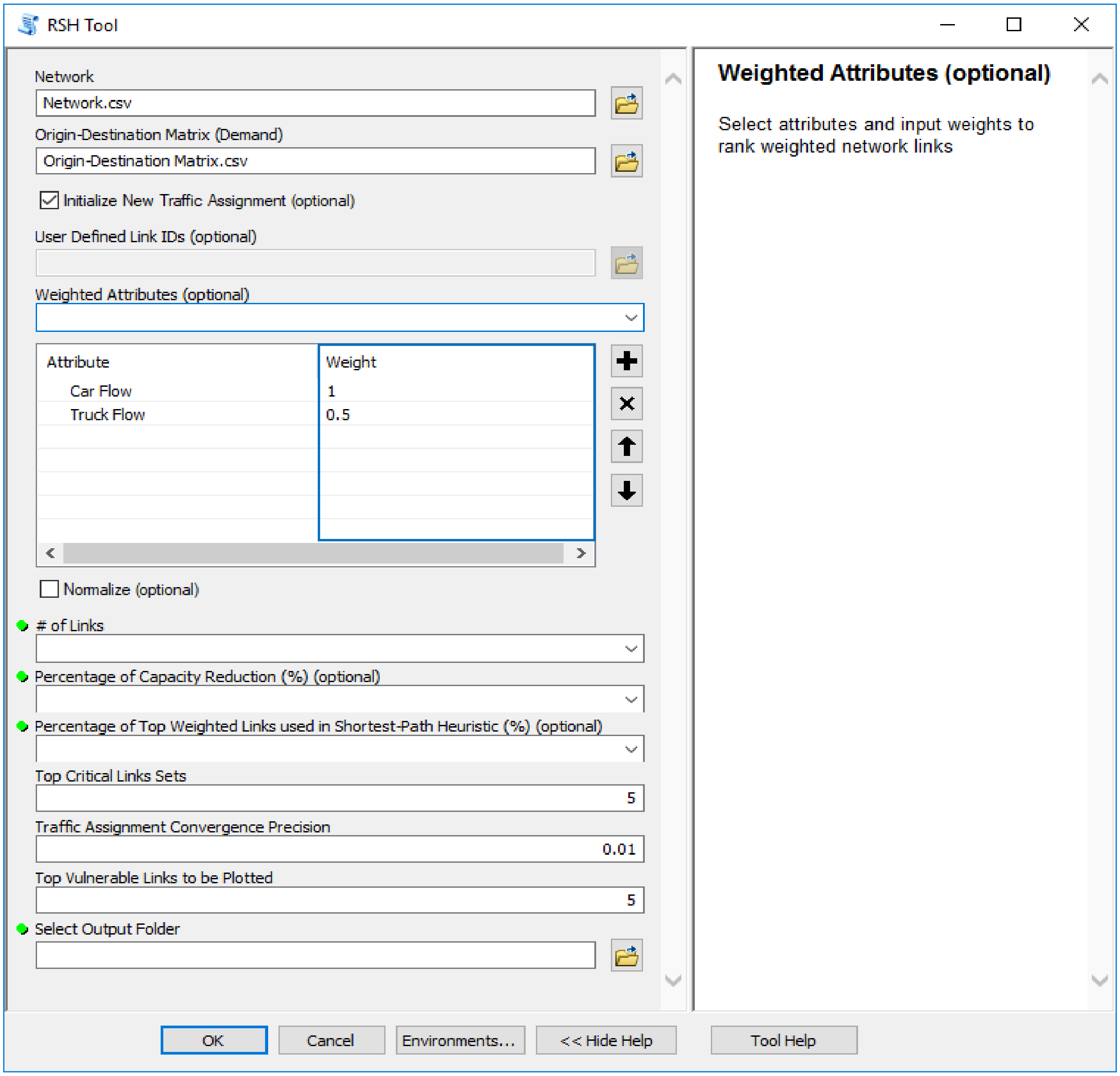


Figure A. 38 Input Weights

STEP 5.3 (Option 2) (Optional)

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

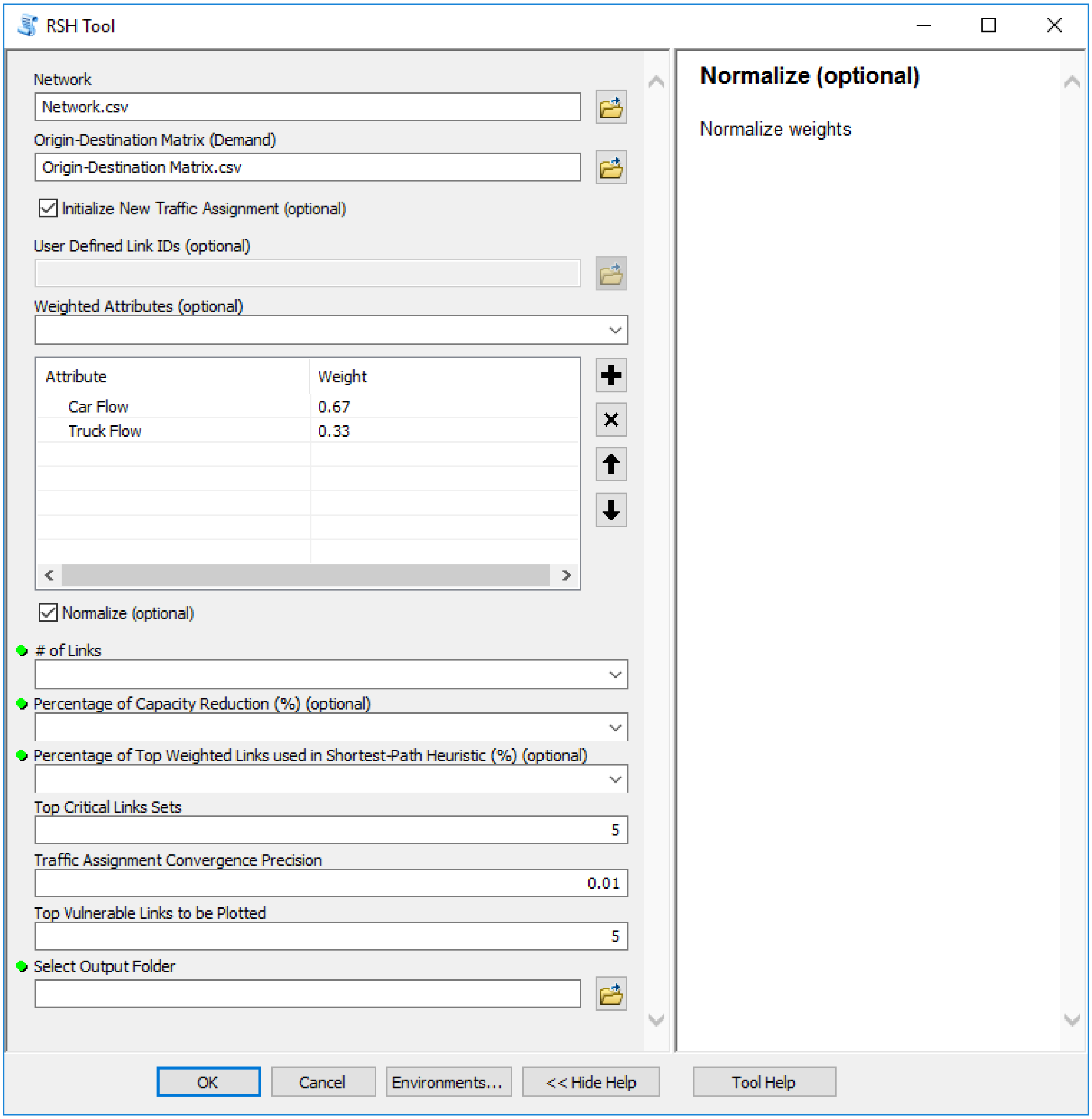


Figure A. 39 Normalize Weights

STEP 6

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

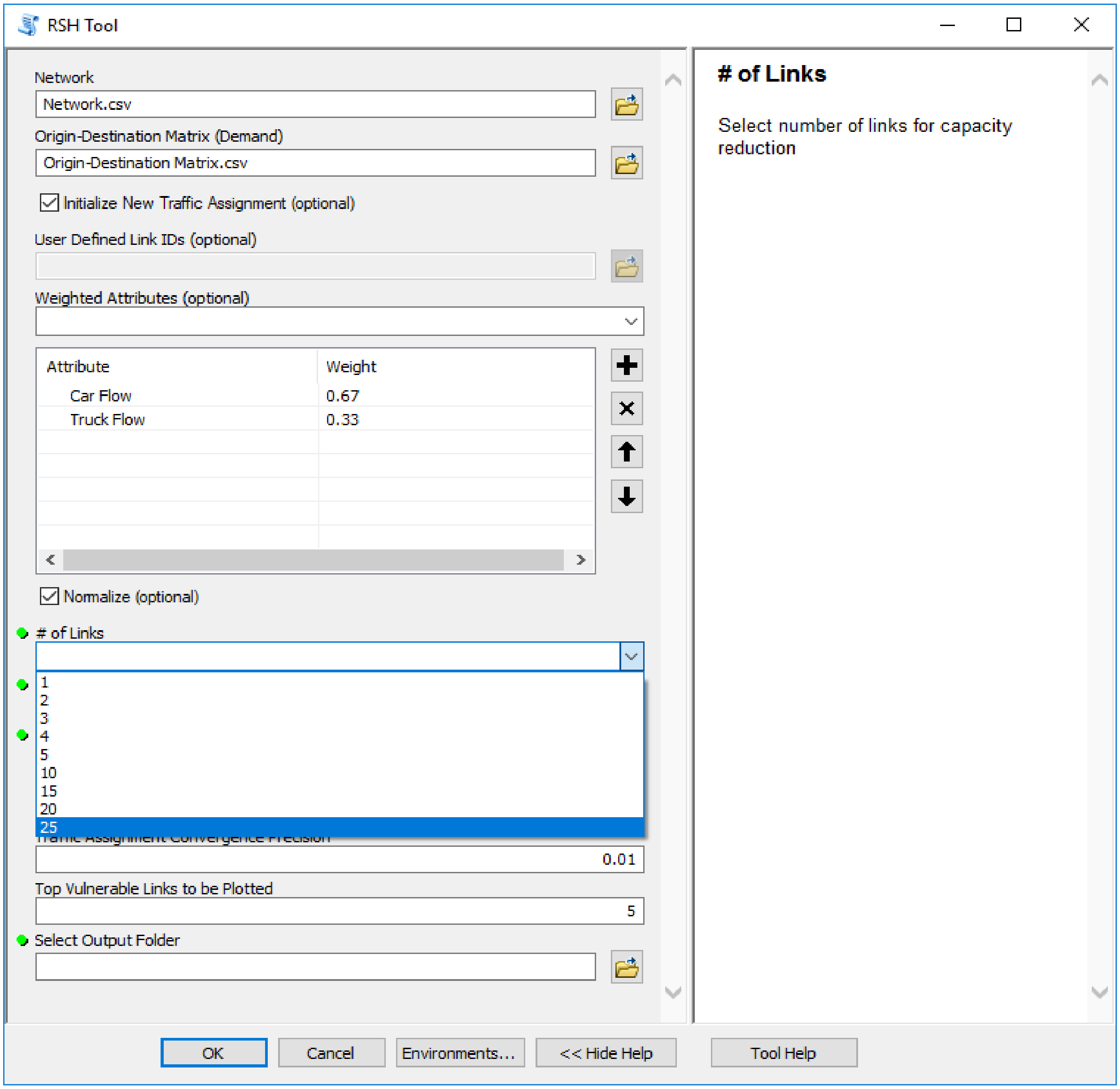


Figure A. 40 Select number of Links

STEP 7 (Option 2)
Select the percentage used to reduce capacity for the top ranked links in input parameter Percentage of Capacity Reduction (%) (see FIGURE A.40).

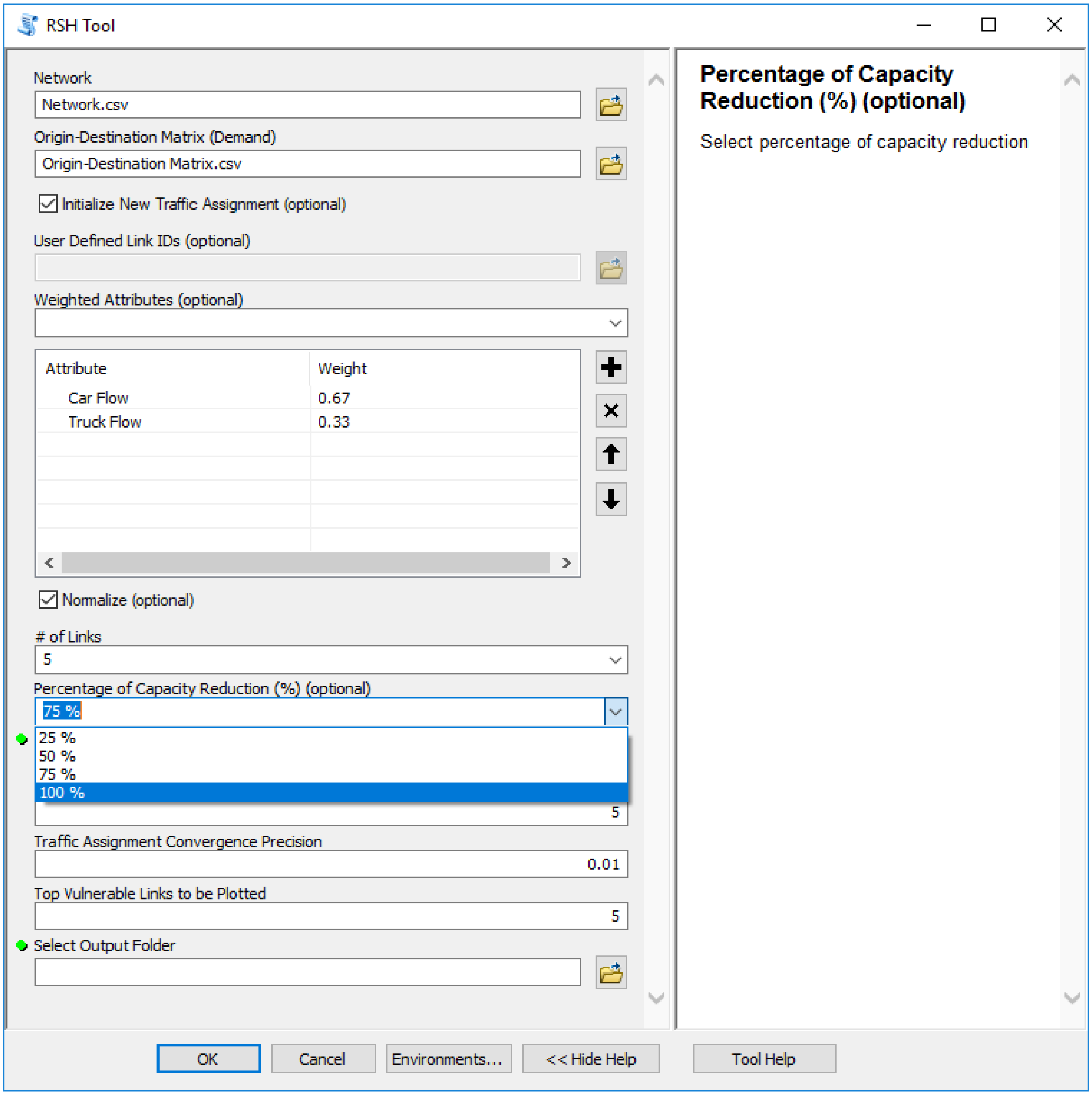


Figure A. 41 Select the Percentage of Capacity Reduction

STEP 8

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

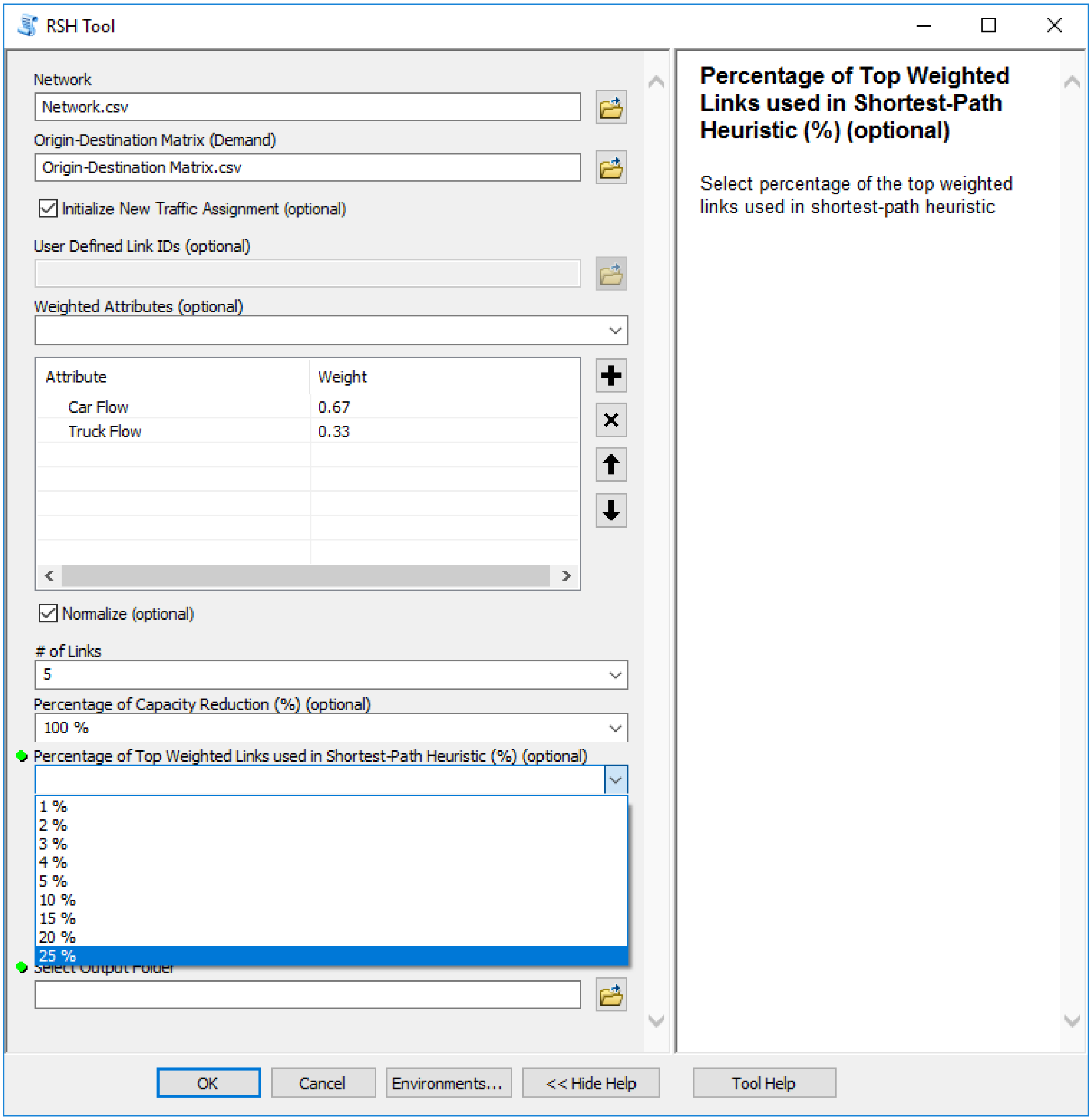


Figure A. 42 Select the Percentage of Top Weighted Links Used in Shortest-Path Heuristic (%)

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).

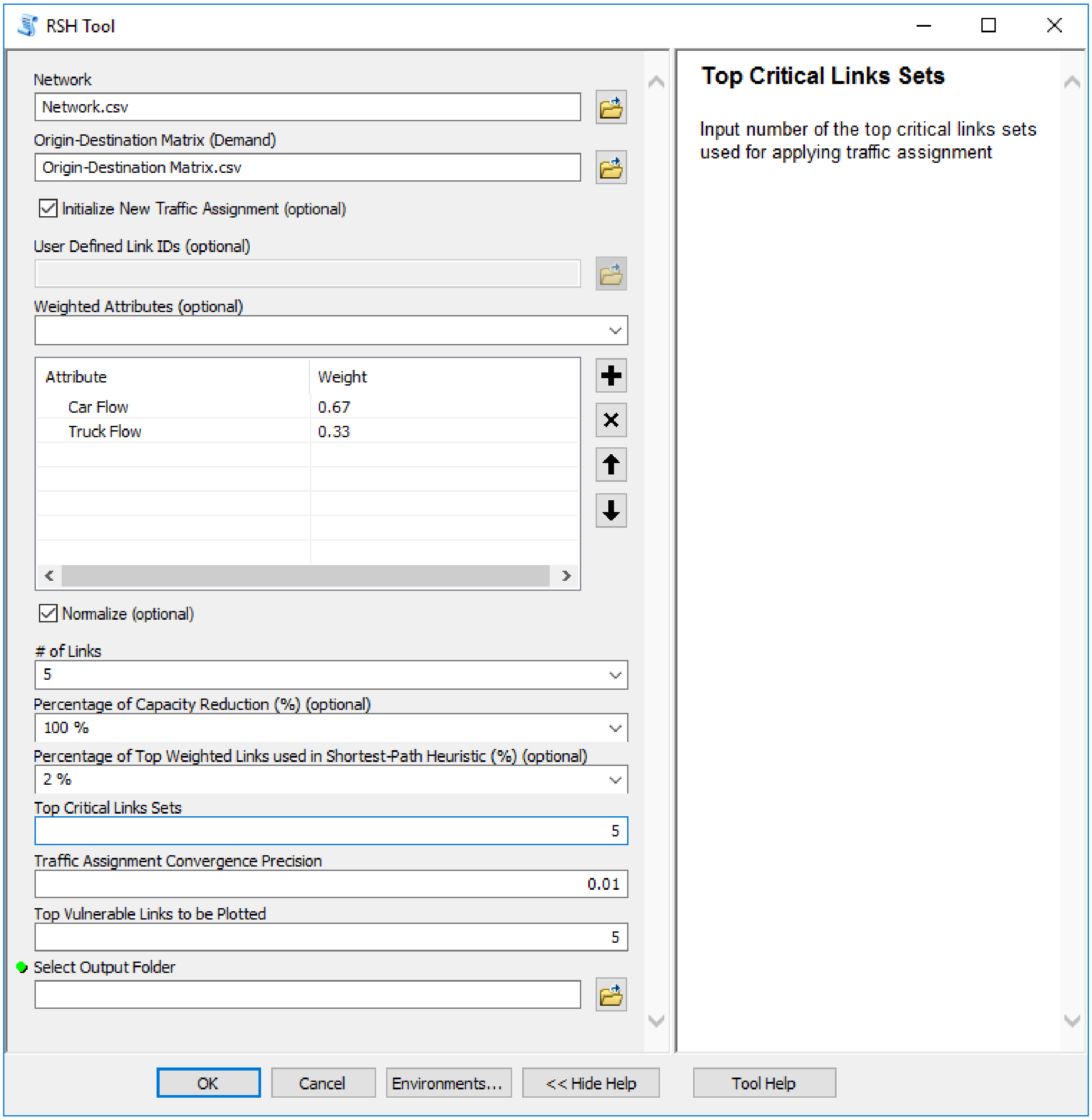


Figure A. 43 Input Number of the Top Critical Link Sets

STEP 10

Input Traffic Assignment Convergence Precision (see FIGURE A.43).

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

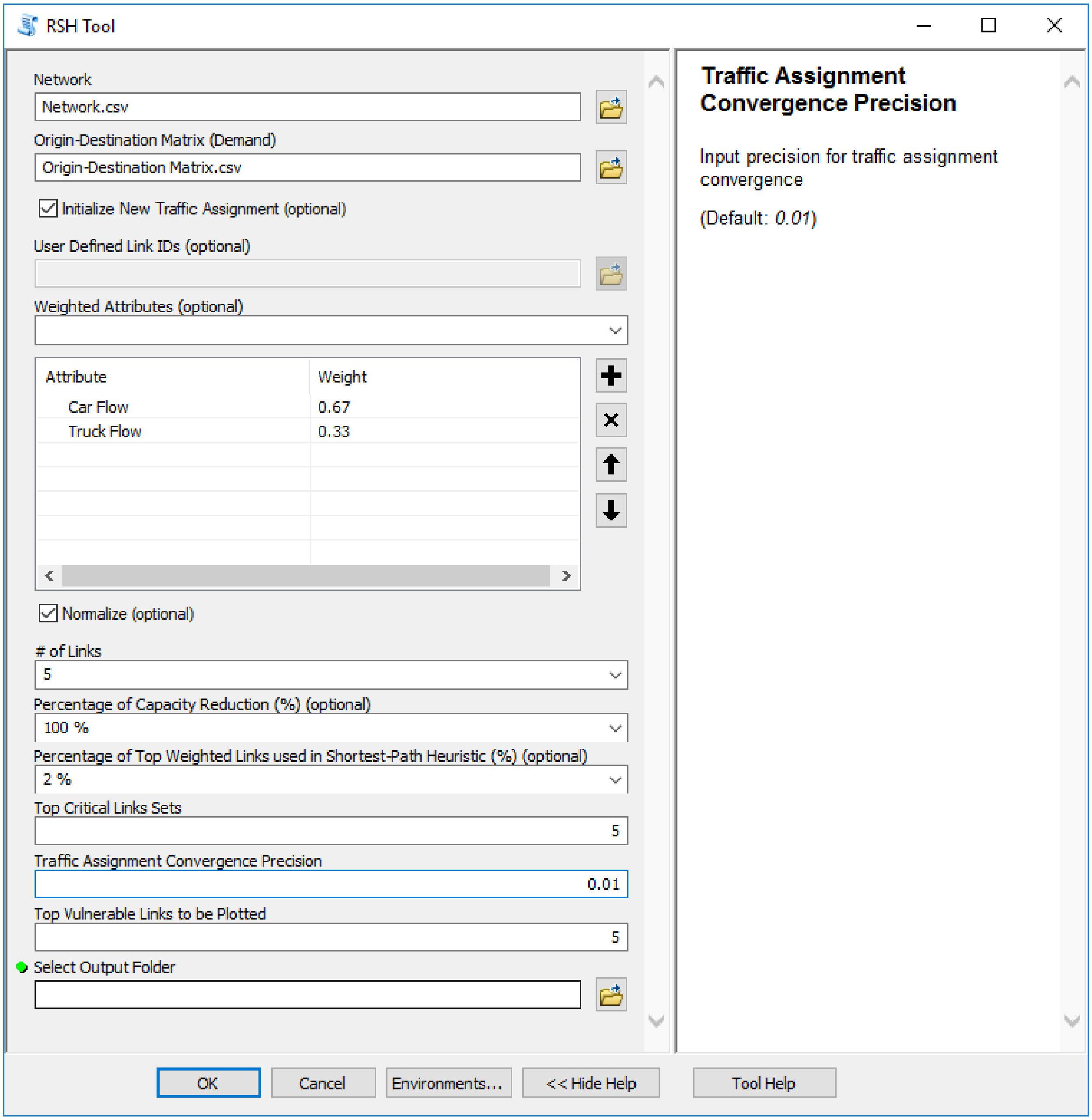


Figure A. 44 Input Traffic Assignment Convergence Precision

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.)

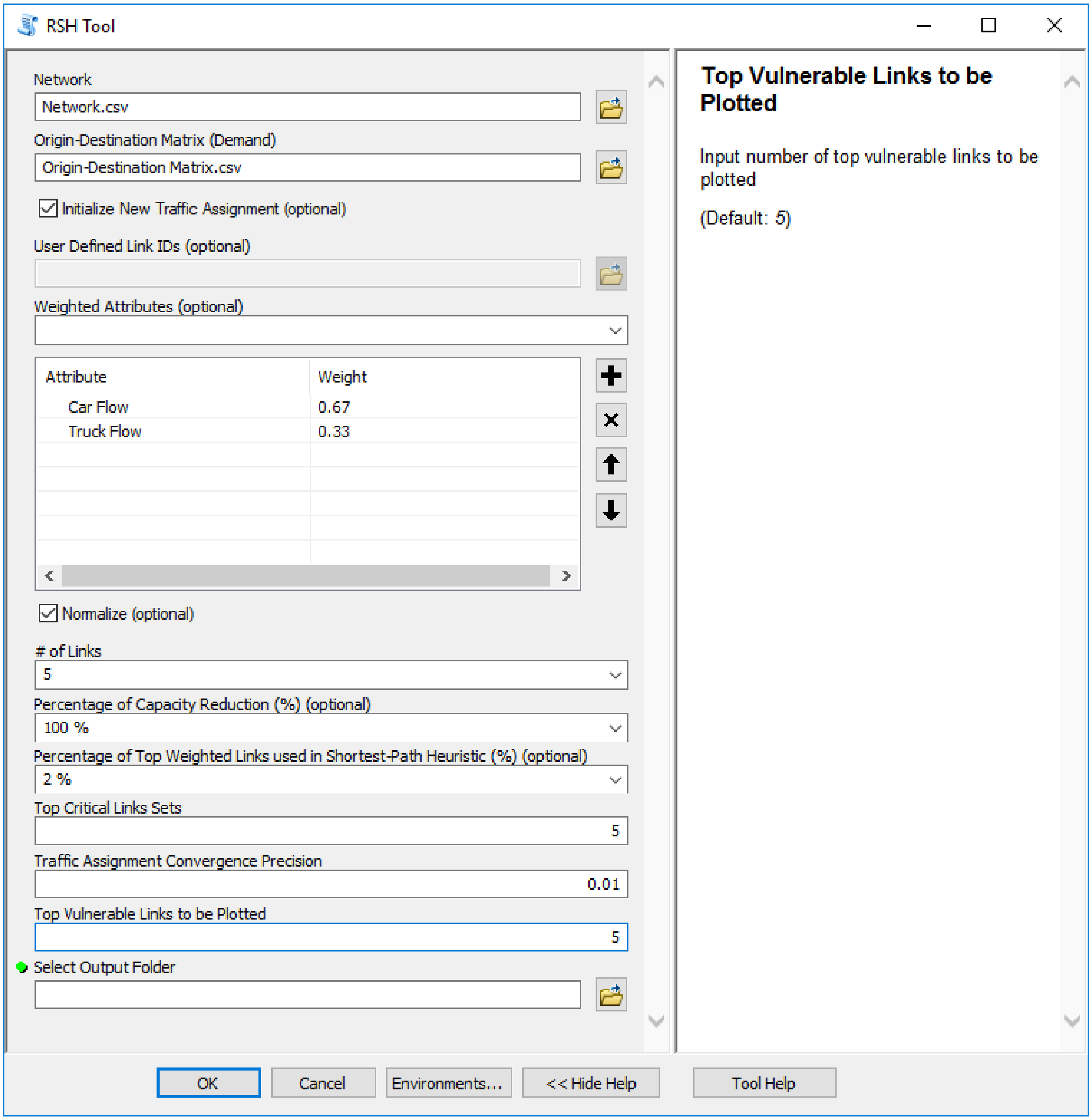


Figure A. 45 Input Top Vulnerable Links to be Plotted

STEP12

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

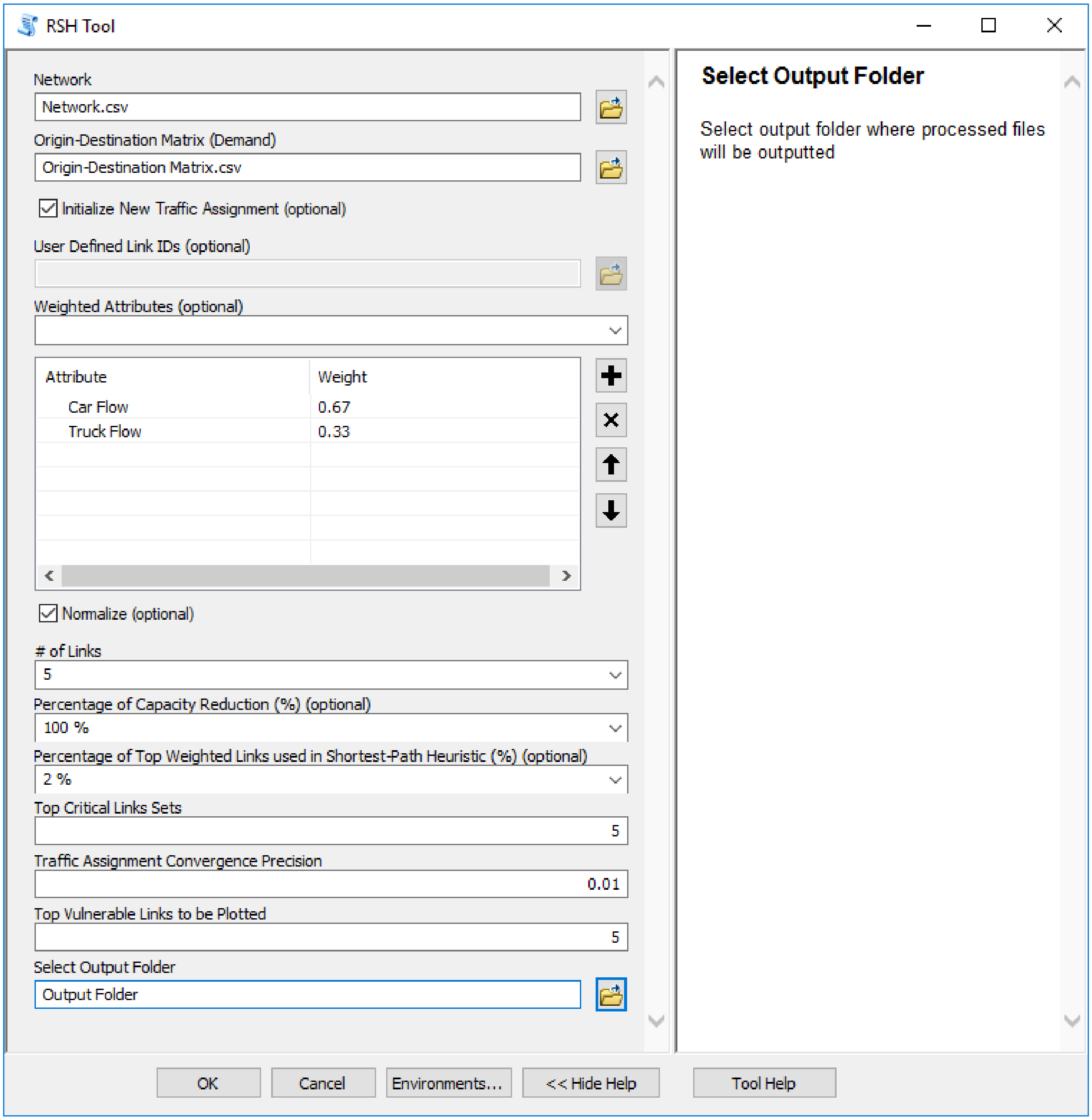


Figure A. 46 Input Output Folder

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 FIGURE A.48 and FIGURE A.49) in (.dbf) format will be imported to ArcMap Display.

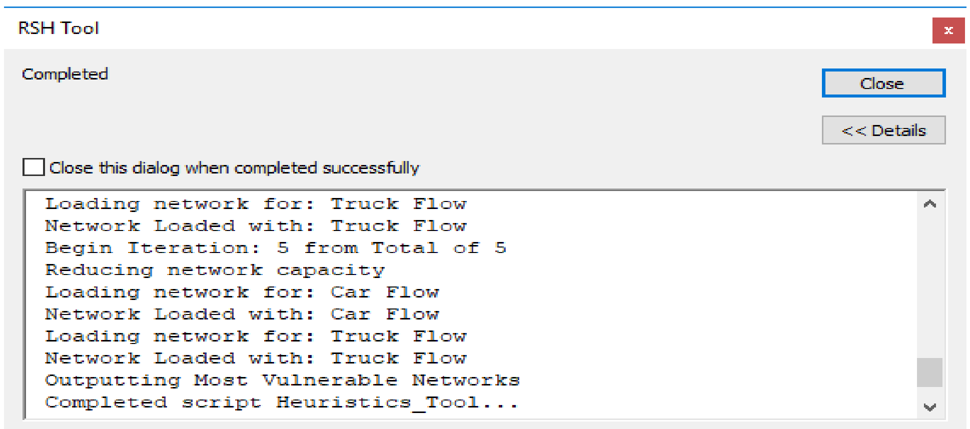


Figure A. 47 Application Performance Task Window

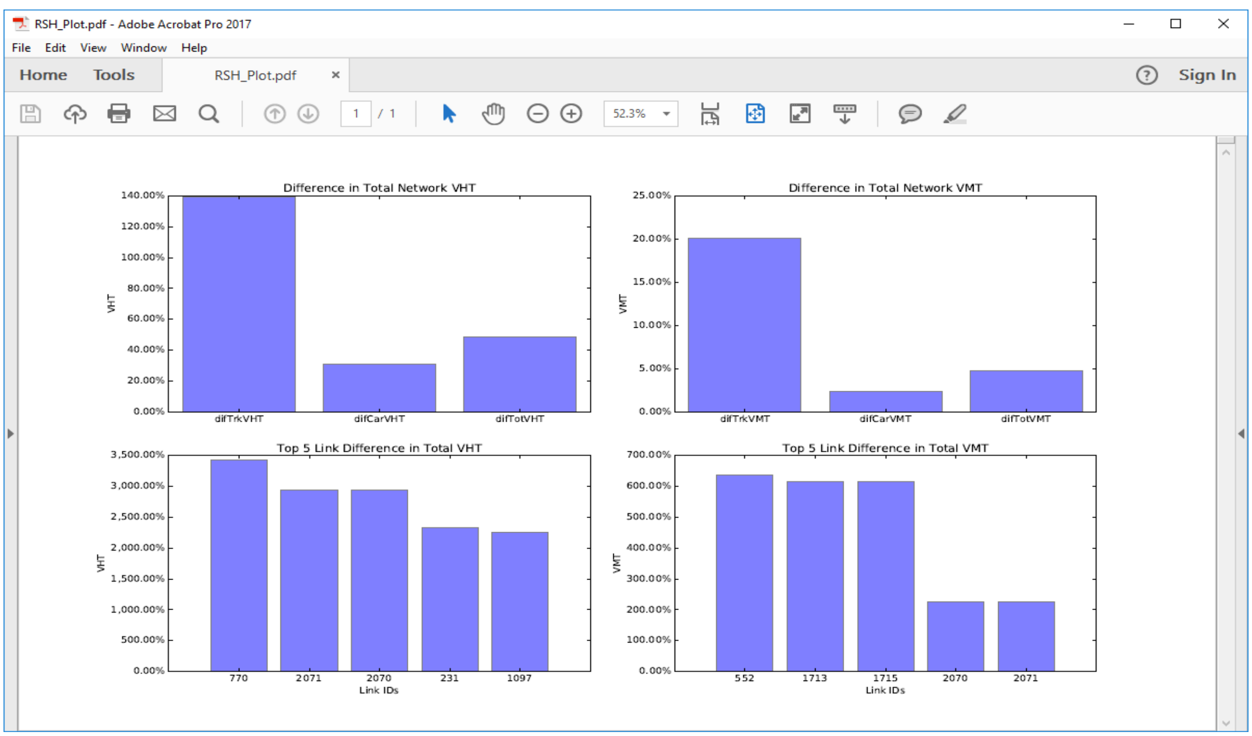


Figure A. 48 RSH Plot

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. 49 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. 50 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).

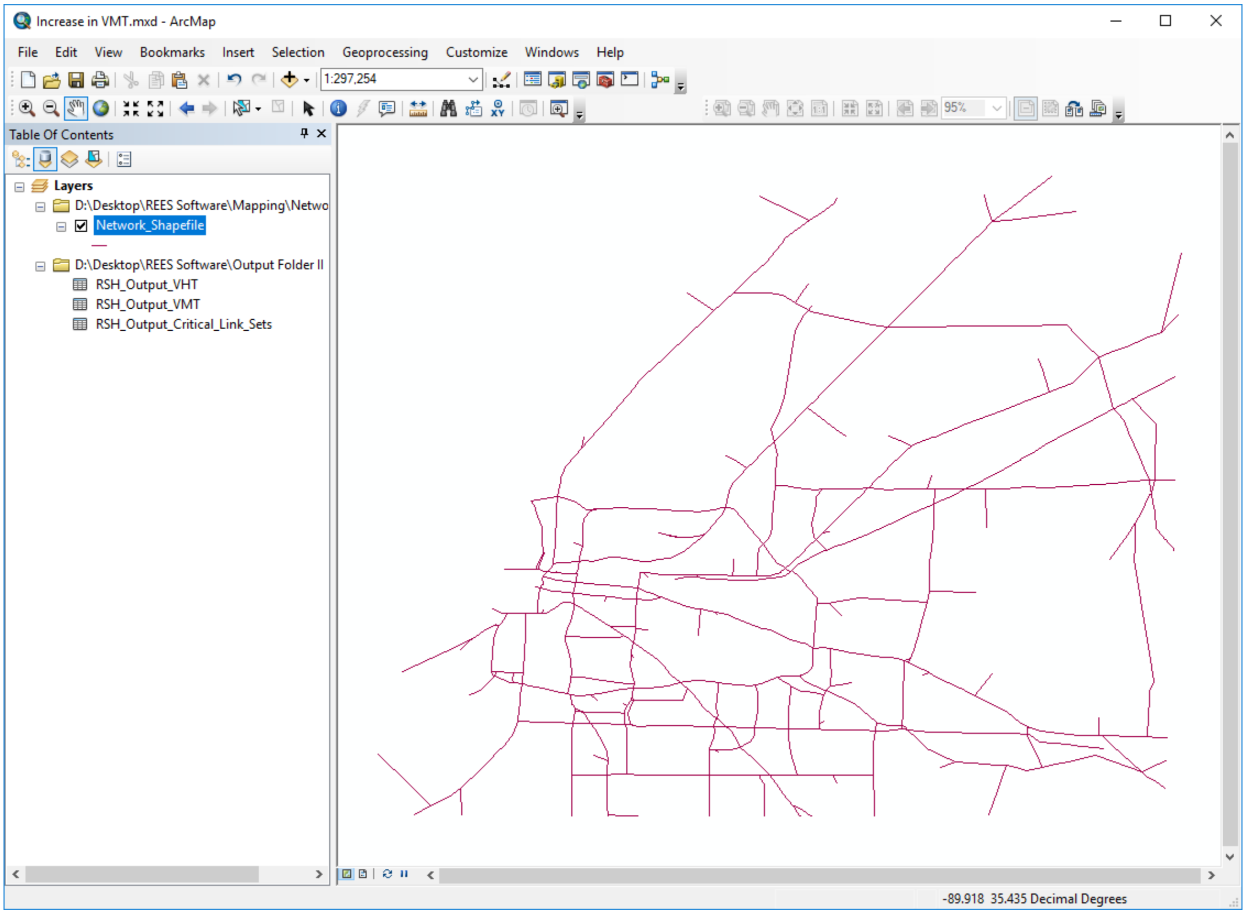
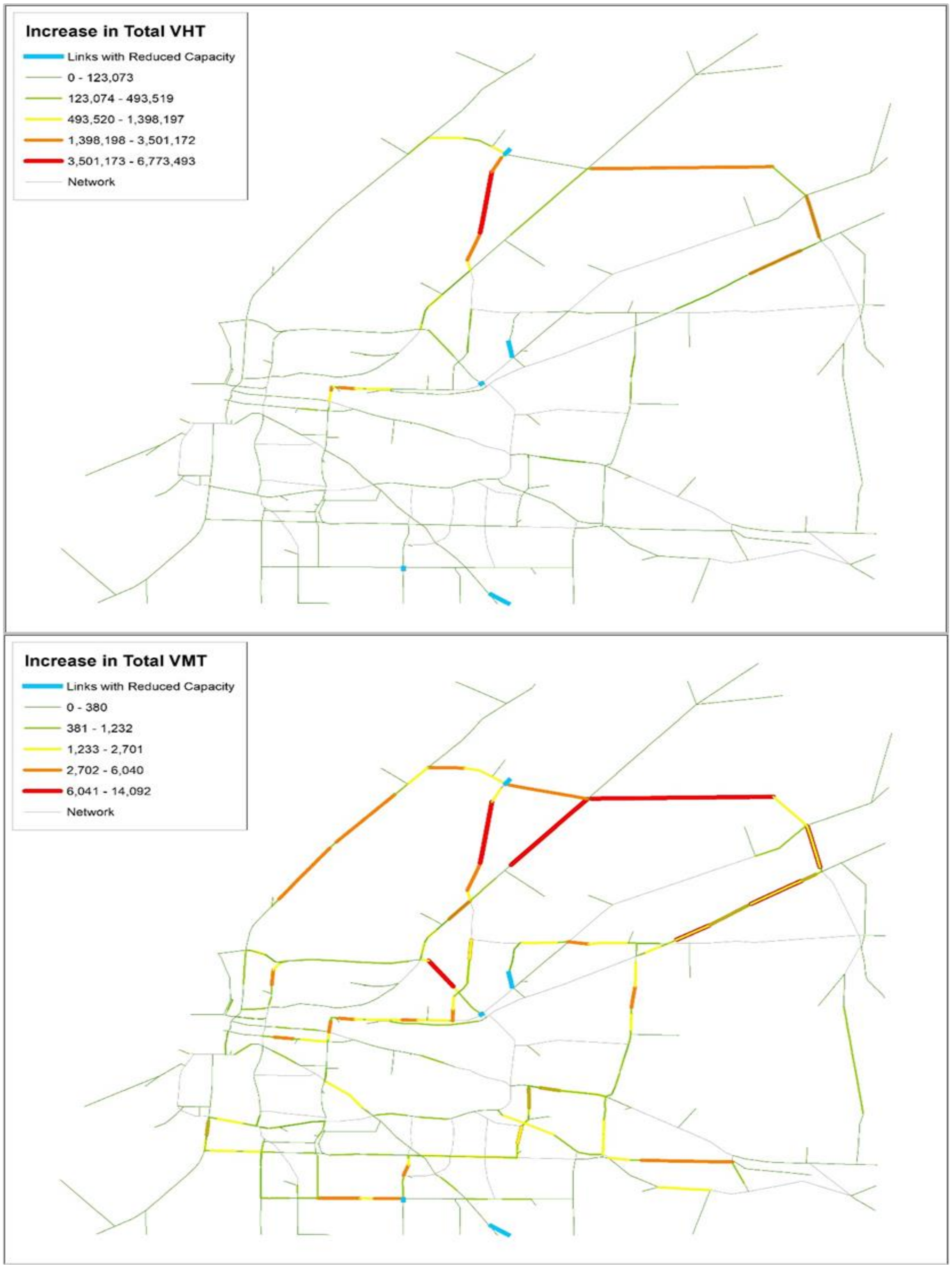


Figure A. 51 Network in a form of Shapefile



Add

Figure A. 52 Visualize the RSH Tool Output

Table A. 2 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. 3 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), BC_Value, TcBC_Value, TfBC_Value.
- **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.

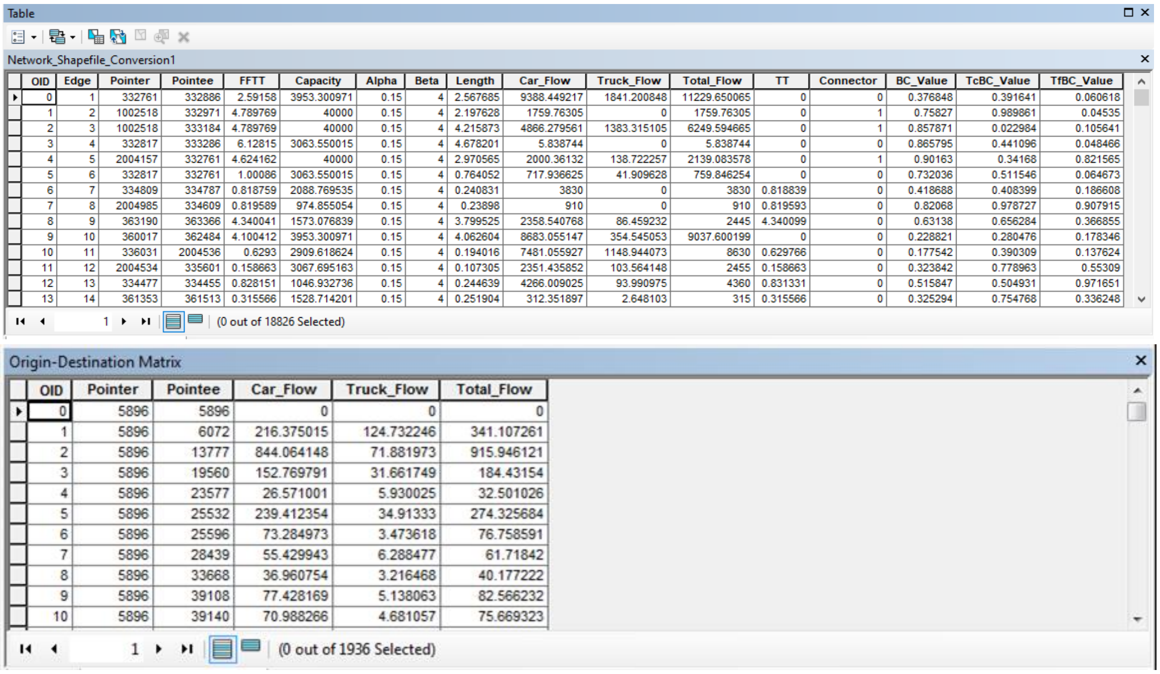
Network

	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	

Origin-Destination Matrix

	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									

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



Table

Network_Shapefile_Conversion1

OID	Edge	Pointer	Pointee	FFTT	Capacity	Alpha	Beta	Length	Car_Flow	Truck_Flow	Total_Flow	TT	Connector	BC_Value	TcBC_Value	TfBC_Value
0	1	332761	332886	2.59158	3953.300971	0.15	4	2.567685	9388.449217	1841.200848	11229.650065	0	0	0.376848	0.391641	0.060618
1	2	1002518	332971	4.789769	40000	0.15	4	2.197628	1759.76305	0	1759.76305	0	1	0.75827	0.989861	0.04535
2	3	1002518	333184	4.789769	40000	0.15	4	4.215873	4866.279561	1383.315105	6249.594665	0	1	0.857871	0.022984	0.105641
3	4	332817	333286	6.12815	3063.550015	0.15	4	4.678201	5.838744	0	5.838744	0	0	0.865795	0.441096	0.048466
4	5	2004157	332761	4.624162	40000	0.15	4	2.970565	2000.36132	138.722257	2139.083578	0	1	0.90163	0.34168	0.821565
5	6	332817	332761	1.00086	3063.550015	0.15	4	0.764052	717.936625	41.909628	759.846254	0	0	0.732036	0.511546	0.064673
6	7	334809	334787	0.818759	2088.769535	0.15	4	0.240831	3830	0	3830	0.818839	0	0.418688	0.408399	0.186608
7	8	2004985	334609	0.819589	974.855054	0.15	4	0.23898	910	0	910	0.819593	0	0.82068	0.978727	0.907915
8	9	363190	363366	4.340041	1573.076839	0.15	4	3.799525	2358.540768	86.459232	2445	4.340099	0	0.63138	0.656284	0.366855
9	10	360017	362484	4.100412	3953.300971	0.15	4	4.062604	8683.055147	354.545053	9037.600199	0	0	0.228821	0.280476	0.178346
10	11	336031	2004536	0.6293	2909.618624	0.15	4	0.194016	7481.055927	1148.944073	8630	0.629766	0	0.177542	0.390309	0.137624
11	12	2004534	335601	0.158663	3067.695163	0.15	4	0.107305	2351.435852	103.564148	2455	0.158663	0	0.323842	0.778963	0.55309
12	13	334477	334455	0.828151	1046.932736	0.15	4	0.244639	4266.009025	93.990975	4360	0.831331	0	0.515847	0.504931	0.971651
13	14	361353	361513	0.315566	1528.714201	0.15	4	0.251904	312.351897	2.648103	315	0.315566	0	0.325294	0.754768	0.336248

1 (0 out of 18826 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. 54 Example input tables in form of (.dbf)

STEP 1

Open newly added REES Tools toolbox and lunch KSP Tool (see FIGURE A.54)

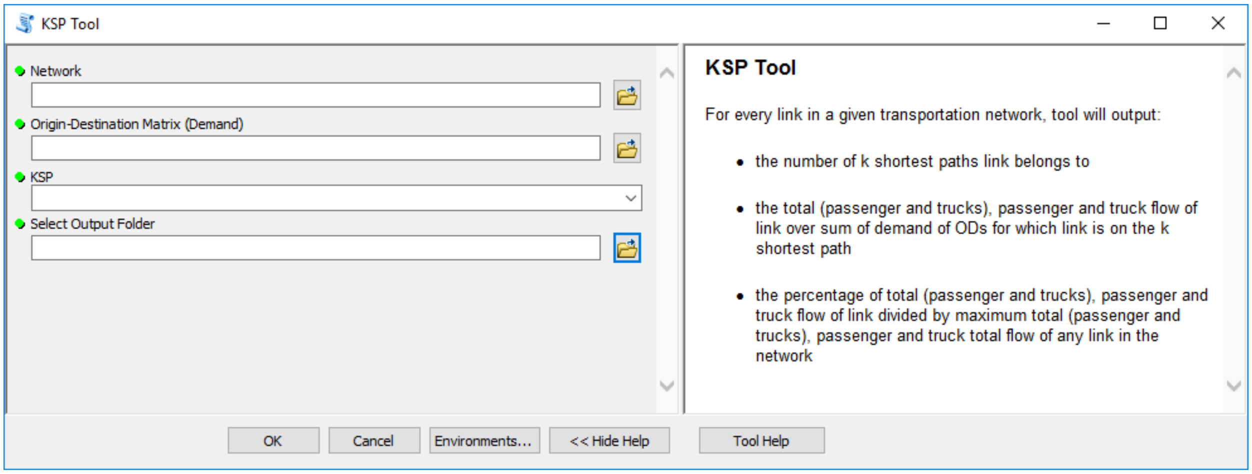


Figure A. 55 KSP Tool

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).

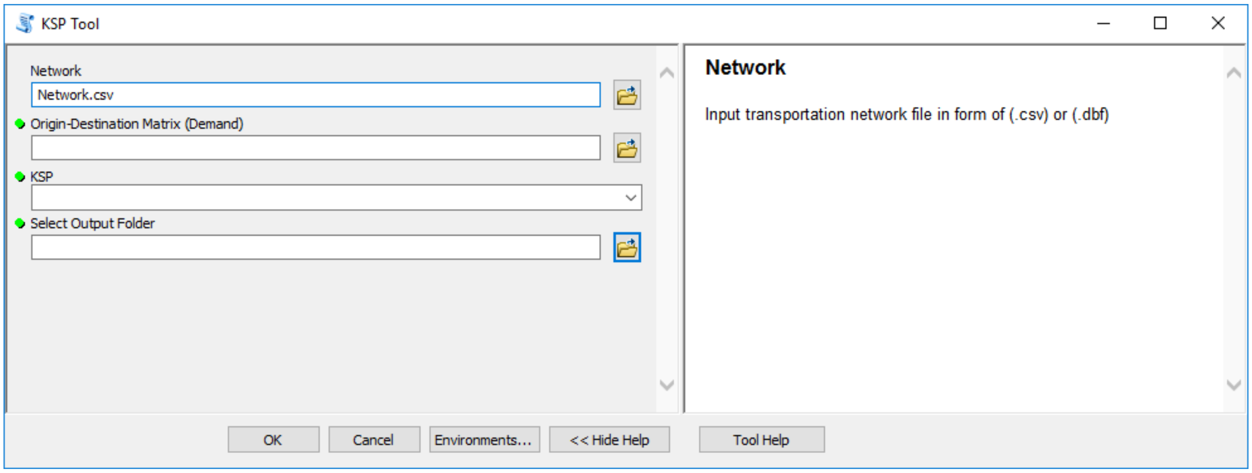


Figure A. 56 Input Network

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).

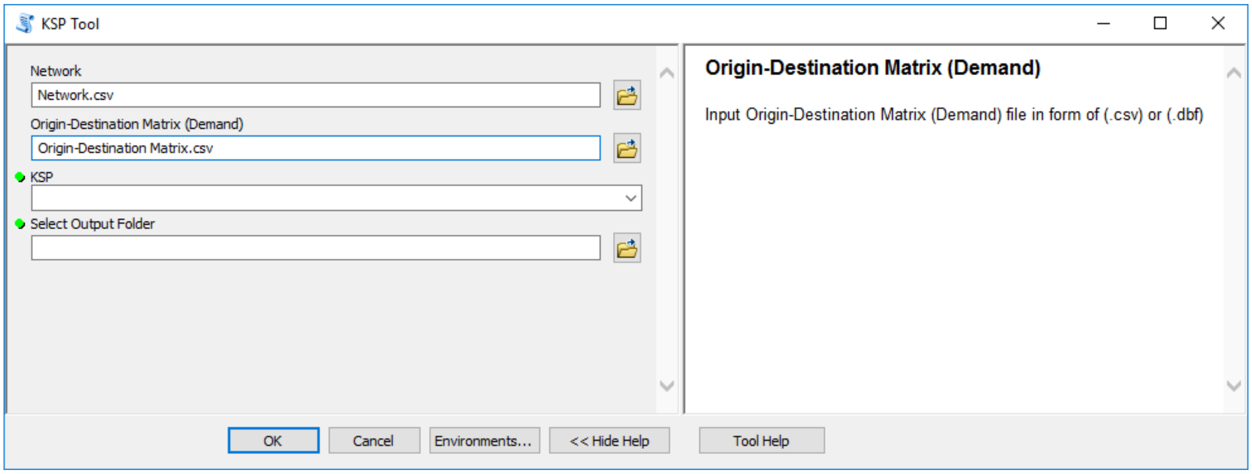


Figure A. 57 Input Origin-Destination Matrix

STEP 4

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

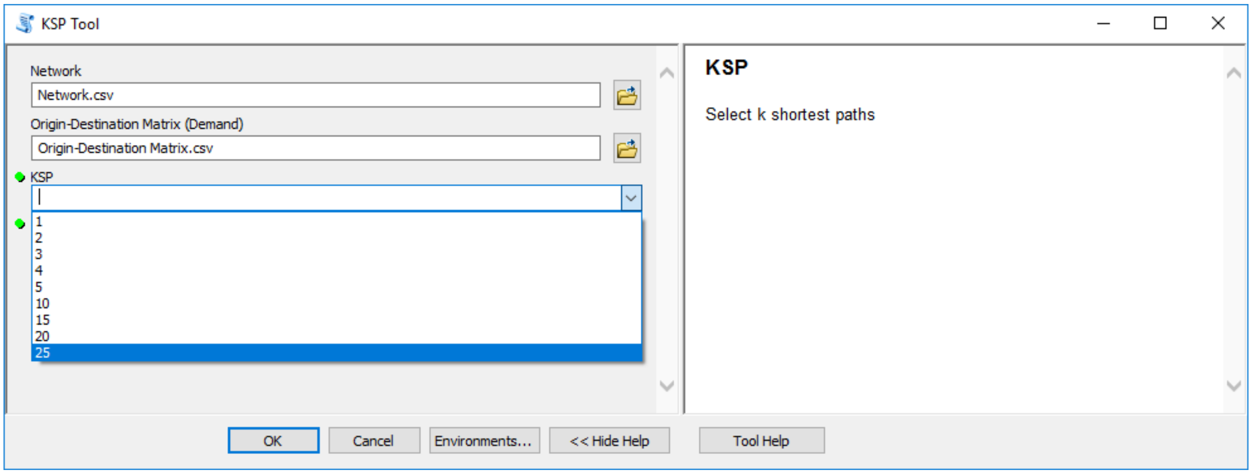


Figure A. 58 Select k Shortest Paths

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).

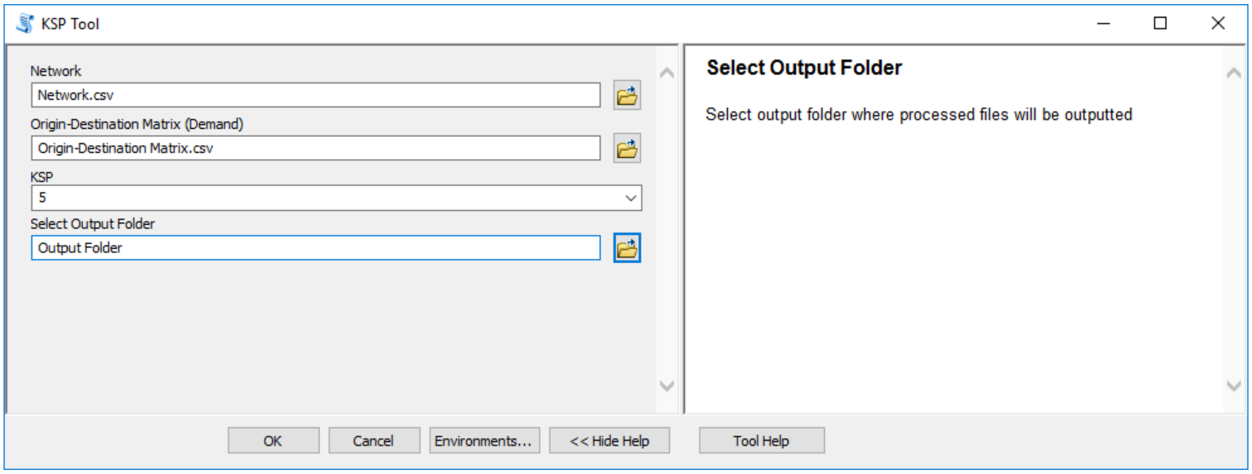


Figure A. 59 Input Output Folder

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.

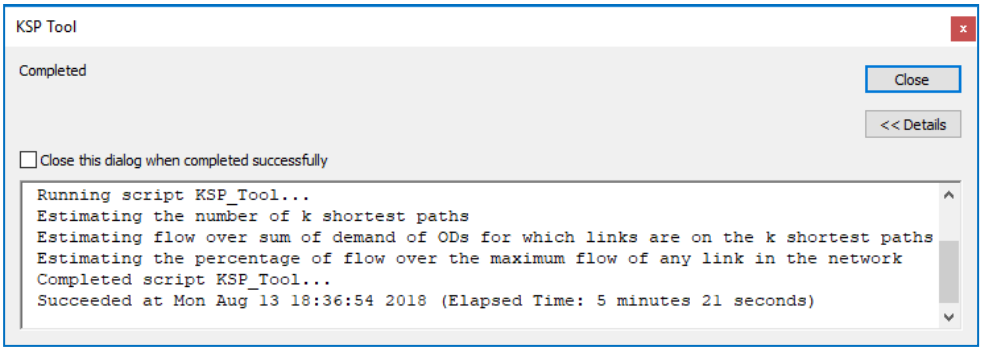
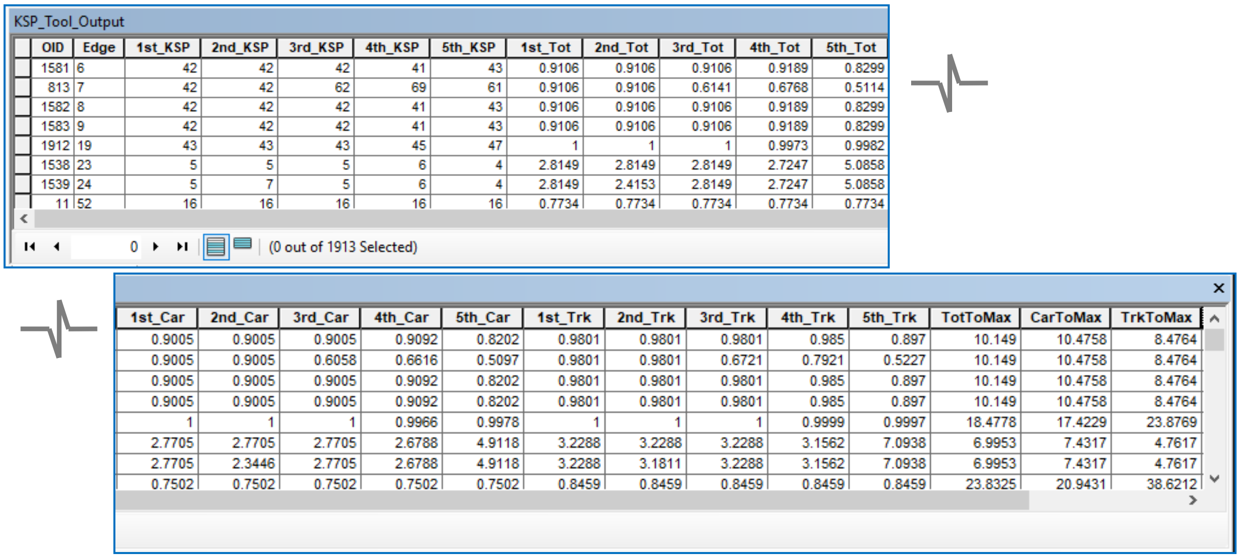


Figure A. 60 Application Performance Task Window



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. 61 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).

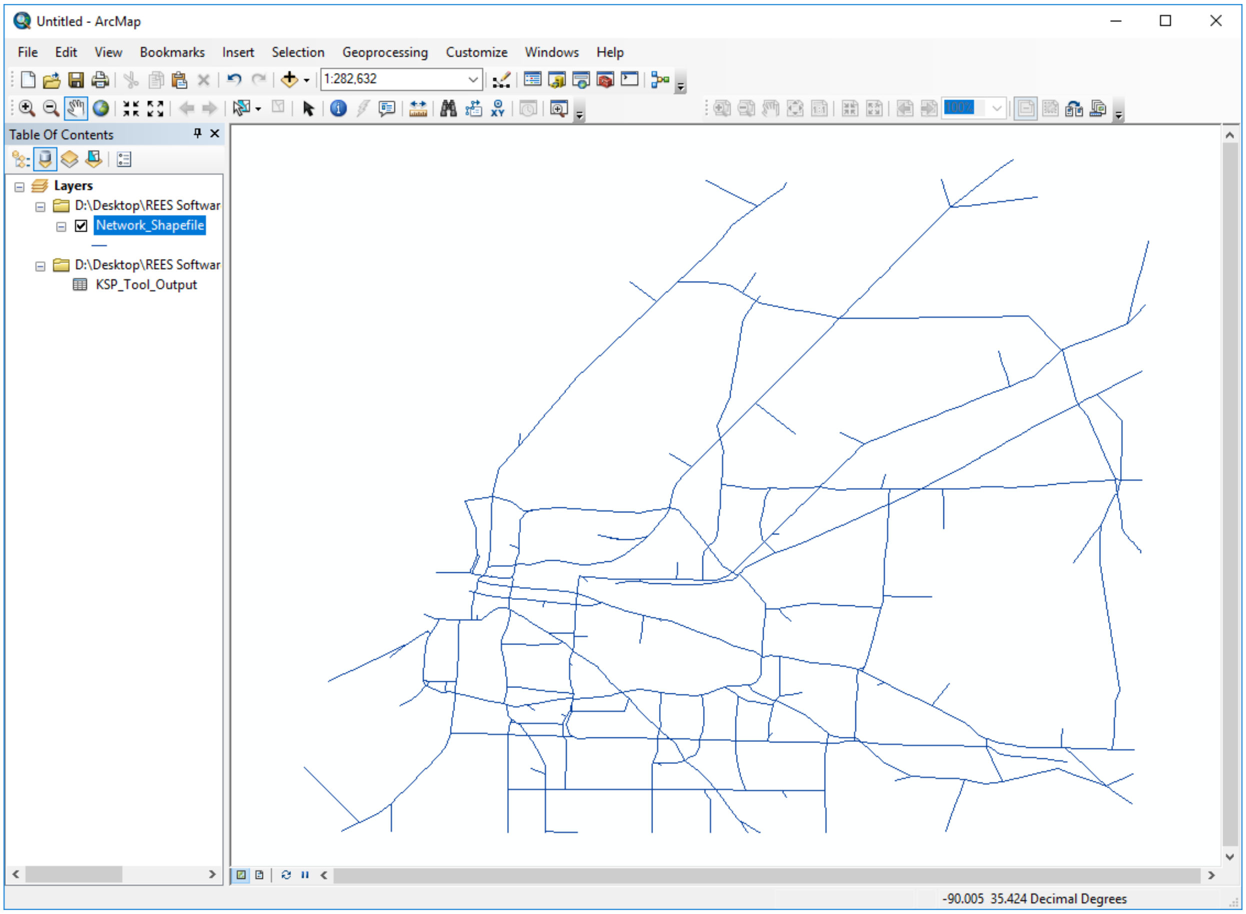
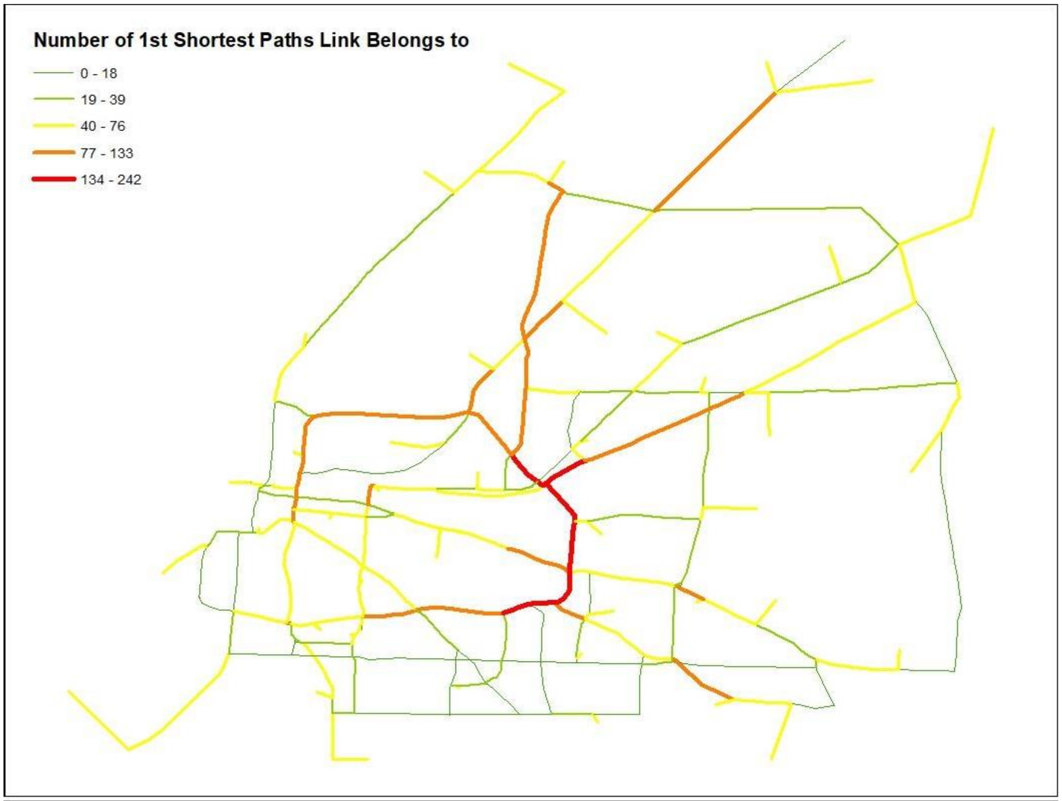


Figure A. 62 Add Network in a form of Shapefile



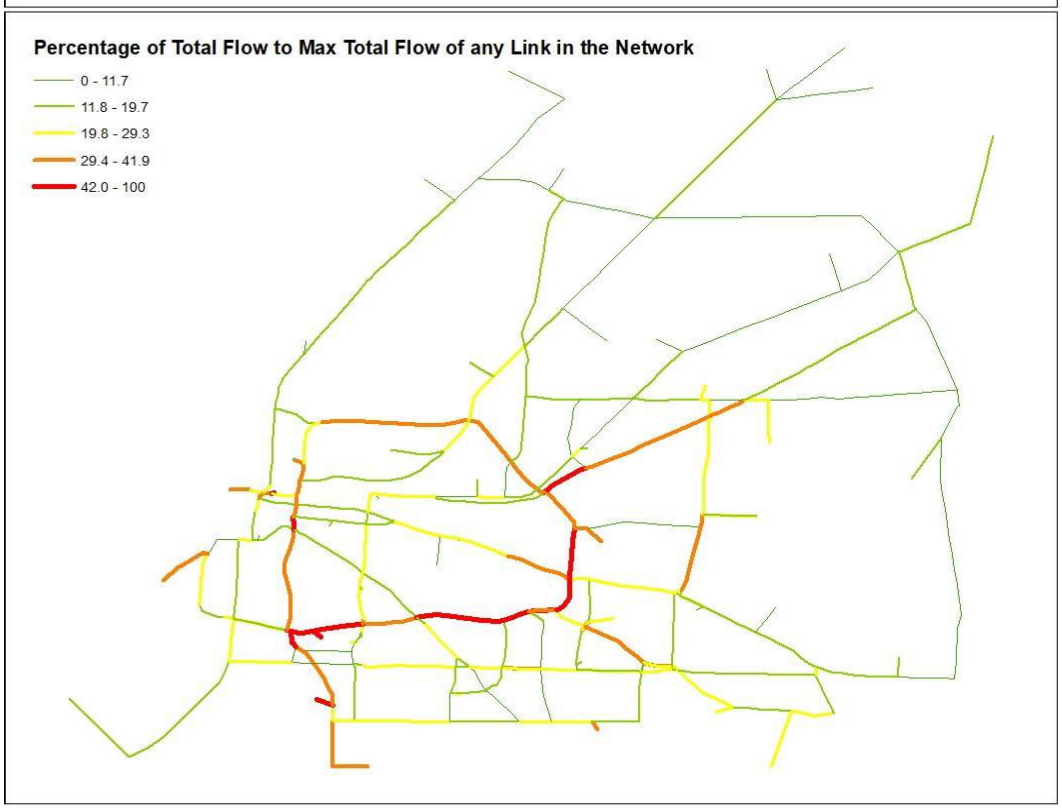


Figure A. 63 Visualize the KSP Tool Output

Table A. 4 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

APPENDIX B: MATLAB CODES FOR VISUALIZING CRITICAL ROUTES

This MATLAB script allows the user to choose an origin and create a shapefile of the Broward County network that includes a dedicated binary column which is equal to **1** if a link is part of the 10 most important paths and **0** otherwise. The user has the option to choose between the 3 different hybrid measures, used to rank paths based on their importance and whether they want to examine passenger cars or trucks.

The steps to use this script are presented below.

Step 1

Open CreatePathMaps.m script

Step 2: Calling the Input

Line 4: Select measure and passenger cars or trucks from available excel files

Step 3

Line 11: Select origin ID for which the most important paths will be printed

Step 4: Change the Output name's string

Line 31: Add measure and passenger cars or trucks according to Step 2

Step 5

Click Run (new shapefile is exported into the same folder as the script)

The script is as follows:

```
%% import paths csv, User select measure and car or truck
selectedMeasure = readtable('OD_Paths_TCADLinks_BC_Passenger.csv');

% change NaN to zero
selectedMeasure= fillmissing(selectedMeasure, 'constant', 0);
selectedMeasure=table2array(selectedMeasure);

%% Extract data for selected Origin (User Select Origin)
origin=306420;
for i=1:length(selectedMeasure)
   if selectedMeasure(i,1)==origin
   selectedOriginPaths(i,:)=selectedMeasure(i,:);
   end
end

%% Print Map (import full network shapefile)
S = shaperead('Boward_County.shp');

% create binary column "LinkFoundInPaths", equal 1 if llink is found in paths of selected OD
for i=1:length(S)
   S(i).LinkFoundInPaths=0;
end
for i=1:length(S)
   if ~isempty(find(S(i).ID==selectedOriginPaths(:,3:end)))
       S(i).LinkFoundInPaths=1;
   end
end

string=['PathsForOrigin_' num2str(origin) 'BCPassenger' '.shp'];
shapewrite(S,string)
```