Methodology for Determining Transportation Network Connectivity Reliability Under Threats of Terrorism

Pamela Murray-Tuite

Synopsis

Predicting the connectivity of a transportation network in terrorist attack scenarios is a challenging problem. Historical information is often not available for any particular network. Furthermore, in the event of an attack, the network is modified by two entities, the terrorists, who damage network links, and law enforcement agencies, who close links in order to secure the network, gather evidence, and capture the terrorists.

This paper provides a methodology to determine, relatively rapidly, the connectivity reliability of the transportation network under threats of terrorist incidents that accounts for:

- The lack of historical or frequency information, with which to determine individual link failure probabilities under extraordinary conditions,
- The effects that attacks on other assets have on the operability of the transportation network links,
- The influence of security policies on the operational state of the transportation network links, and
- The fact that asset failures are not random under terrorism conditions.

This methodology is designed for use without specific intelligence information, but, should such information become available, it can be incorporated easily. This process contributes to advanced planning for terrorism events and evaluates the impact of security policy on the transportation network.

The methodology presented in this paper consists of four steps. The first step determines the terrorists' intent, whether to disrupt national security, inflict casualties, disrupt the target area's economy, and/or lower public morale and evaluates each asset within the network's bounds in terms of the terrorists objective(s). The second step identifies potential attack methods in terms of the terrorist's capabilities and resources, the history of similar attacks, and asset vulnerabilities to those methods. The third step determines the likelihood of transportation link damage whether by intentional targeting or as collateral damage by an attack on adjacent assets. The final step captures the effects of security policies on the operational state of the transportation links and calculates the resulting connectivity reliability.

This methodology is illustrated with a small sample network and notional data. For this particular example, the connectivity reliability is 0.999994, indicating that the decision makers associated with this particular network should not be overly concerned with connectivity of the transportation network between the origin and destination of interest under threats of terrorism and the security policies examined.

The methodology used to derive the connectivity reliability for the transportation network under threats of terrorism is somewhat subjective in the absence of specific intelligence information; however, a lack of detailed information should not preclude the analysis. Decision makers need to plan ahead and determine the potential impact that a terrorist event would have on the network as well as the effects of the security policies they choose to implement. They can also use the estimate of the connectivity reliability (bounded by zero and one) in combination with the importance of the particular origin-destination pair to determine where to best allocate resources when making additions to the transportation network.

This paper has three immediate benefits to security and reliability professionals. First, a method for determining the unreliability of a link under threats of terrorism is identified. Second, the effects of security policy actions are examined in terms of connectivity. Finally, this work offers an approach to integrate threats and security and form a comprehensive picture of their influence on network connectivity.

Methodology for Determining Transportation Network Connectivity Reliability Under Threats of Terrorism

Transportation network reliability can be viewed from three perspectives. First, connectivity reliability, also referred to as terminal reliability, is the probability that at least one path exists between an origin and a destination (Iida, 1999). Second, performance reliability is the probability that drivers can reach their destinations within a given amount of time (Iida, 1999). Third, capacity reliability is the probability that the network can provide a given service level for a certain demand (Chen et al, 2001). Performance and capacity reliability inherently depend on the connectivity reliability of a network since performance and capacity have little meaning for a disconnected network. A long-existing, but newly-recognized, threat to connectivity reliability (and by extension performance and capacity reliability) is terrorism. This paper focuses upon this most fundamental level of reliability in light of the extraordinary conditions arising from terrorism.

Numerous works have presented heuristics to estimate the connectivity reliability of a network under traditional conditions and have explored the computational efficiency of such heuristics (see for example Iida and Wakabayashi, 1989; Yang et al, 1996; Yoo and Deo, 1988; and Chen and Yuang, 1996). These previous studies assume that the reliability of individual network links is known. However, determining the reliabilities of the individual links, particularly for extraordinary events, is arguably the most difficult aspect of reliability calculations. Unlike “normal” events such as traffic accidents, where historical statistics may be used to determine link reliabilities, historical information for extraordinary events may be difficult to obtain due to their infrequency. In the case of terrorist attacks, there may be no previous incidents for a particular network, especially at the individual transportation link level, but that does not indicate that a link will not be damaged by terrorists in the future.

Risk analysis offers one potential source for estimating the probability that a network link is damaged due to terrorism. Risk is comprised of two components, the likelihood that an attack on an asset (e.g. transportation network link, office building) is successful and the impact that asset’s failure will have. For the purposes of this work, the likelihood of a successful attack will be used as the unreliability of a link.

Determining the likelihood of a successful attack presents its own challenges. Ideally, this value would be determined through a cooperative arrangement with intelligence agencies, who have access to information about individual terrorist groups and may have their own probability analysis techniques. Haimes (2004) recommends fully understanding terrorist networks to accurately assess risk and provides a methodology for gathering intelligence. The task of gathering intelligence information can be time consuming and the results are often classified. However, the restricted nature of this information should not prevent initial (and somewhat subjective) analysis of the network and the connectivity ramifications of link damage.

Likelihood values are determined by studying aspects of the threat as well as vulnerabilities of the asset. From the threat perspective, one may consider the history of attacks on similar types of assets, whether successful or unsuccessful, and the capabilities and intent of terrorist groups (adapted from Moteff, 2004). The asset’s vulnerability relates to its inherent susceptibility to the particular attack as well as any protective measures that may be implemented to prevent the success of such an attack. Some initial work into identifying the vulnerability of network links has been conducted by Bell (2003), who developed an approach for determining the most important links for network performance. Murray-Tuite and Mahmassani (2004) developed a metric for evaluating all transportation network links under any condition and applied it to the problem of identifying the links most likely to be targeted by a malicious entity. While these works only focused on the transportation network, this paper considers both the targeting of the transportation links and collateral damage that would be inflicted on the transportation network.

Collateral damage results from the terrorists targeting assets other than the transportation network. For example, buildings and other critical infrastructure assets, such as power or telephone lines, may be intentionally damaged. Due to accessibility demands, most buildings are alongside some aspect of the transportation system; therefore, an attack on a building influences the operability of the adjacent transportation link(s). The cost of right-of-way (ROW) has led to several infrastructures, particularly electrical power and telecommunications, to share ROW with the transportation system. Damage to power or telephone lines and poles also impacts the operational state of the adjacent transportation links. The transportation links' operational dependence on other assets further complicates the determination of the links' reliability during terrorist incidents.

Another complication to determining transportation network reliability during terrorist incidents is the influence of security policies. The security policy implemented immediately following terrorist events will affect the transportation network in various ways. Some attack methods, such as a chemical release, encourage the evacuation of the residents or workers in a given area. In other cases, the attack is fairly contained, such as a kidnapping or hostage situation. For isolated situations, the evacuation area, if any, is smaller and law enforcement officials may contain potential witnesses in the area. Still other attacks are isolated events and do not have the potential to harm people not in the immediate target area. Overall, the tradeoffs made between evacuating the population and attempting to capture the offenders and gather evidence will affect the scope of the terrorist attacks' impacts upon the network.

The final complicating factor is that previously developed heuristics estimating connectivity reliability under "normal" conditions cannot be directly transferred to the case of terrorism. Unlike traditional reliability scenarios, link failures under terrorism conditions are not random and depend on the terrorists' resources. Resources that are expended on damaging one asset cannot be used against another. Since resources are limited, the likelihood that a lone asset is damaged may be different from the likelihood that same asset would be successfully attacked in combination with other assets. For example, the resources may be sufficient to attack one large target but insufficient to attack that target and a smaller one. Thus when multiple targets are considered, the probability of a successful attack on any one of those assets is different from the case when that target is considered in isolation. Therefore, the calculation of network reliability cannot be based solely on the individual link failure likelihoods, unless the terrorists are assumed to select only one target.

This paper provides a methodology to determine, relatively rapidly, the connectivity reliability of the transportation network under threats of terrorist incidents that accounts for the previously mentioned challenges of:

- The lack of historical or frequency information, with which to determine individual link failure probabilities under extraordinary conditions,
- The effects that attacks on other assets have on the operability of the transportation network links,
- The influence of security policies on the operational state of the transportation network links, and
- The fact that asset failures are not random under terrorism conditions.

While this methodology is designed for use without specific intelligence information, should such information become available, it can be incorporated easily.

This paper has immediate benefits to security and reliability professionals. First, a method for determining the unreliability of a link under threats of terrorism is identified. Second, the effects of security policy actions are examined in terms of connectivity a consideration heretofore unexamined in previous works. Finally, this work offers an approach to integrate threats and security and form a comprehensive picture of their influence on network connectivity.

The remainder of this paper is divided into four sections. The first portion provides a description of the problem. The second section provides a general methodology that is easily adaptable to any transportation network and the concerns of the local area. The third part demonstrates the methodology through a small example. The final section provides some conclusions.

PROBLEM DESCRIPTION

The problem addressed in this work is to determine network connectivity reliability ($R_{s,t}^{e,p}$) for origin *s* and destination *t* given a transportation network *G(N,A)* consisting of a set of nodes (*N*) and directed links (*A*), a terrorist threat *e*, and security policy *p*. The network is examined under a general terrorism threat in an open time frame, without any specific intelligence information (if the threat were specific, no analysis of potential targets would be required and the target could be avoided during that time). Transportation network links are not the only potential targets considered; however, other assets are examined in relation to the transportation network link(s) along which they are located. The potential targets are analyzed only in terms of their immediate payoffs to the terrorists. This work also considers security policies that would be implemented in response to the threat and/or a successful attack.

METHODOLOGY

The methodology developed for this work is designed for situations where one does not have access to intelligence information that could be used to predict targets or the likelihood of an attack. Each attack method is considered separately. Six assumptions and simplifications are made in the methodology; these are listed below.

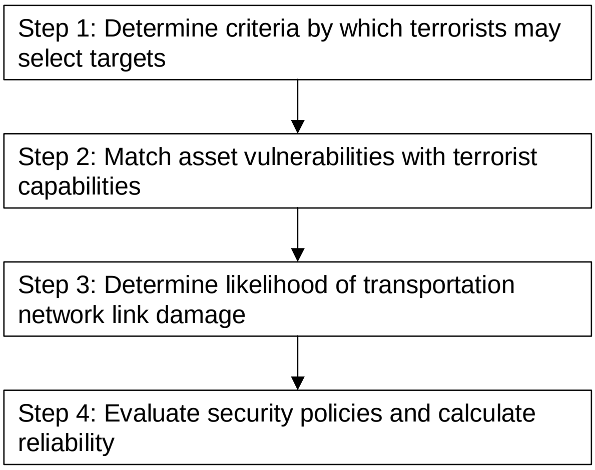
- The timing of the terrorist activity is irrelevant to this study. The time required to plan the event, recruit members, train the executors, and raise funds are considerations in determining terrorist capabilities, but the actual timing of an event is not considered.
- Nodes are 100% reliable. This simplifying assumption is based on the relatively small size (distance) of intersections compared to links.
- The terrorists hit their target(s) with 100% accuracy. This simplifying assumption allows for all of the damage to be directed at the target. Furthermore, collateral damage is not considered, except as the targets affect the transportation network.
- Damaged links will not be used by travelers. This assumption is based on the view that drivers will perceive damaged links as too dangerous for use or that security policies will close the affected links.
- Evaluation of the network occurs after security policies have been implemented. This assumption allows time based considerations to be ignored. Particularly, delays in the implementation of the security policy are ignored, though the methodology could be separated into the terrorist event and the conditional security policy implementation, should more granular results be desired.
- The terrorists will only strike one target. This simplifying assumption eliminates the complexities of considering each asset in all combinations with all others. However, the methodology could easily be extended for such considerations.

The notation used in the description of this methodology is summarized in Table 1.

Table 1: Summary of Notation

Notation	Interpretation
G	Graph
N	Set of nodes
A	Set of directed links
a	Index of set *A*
E	Set of threats (attack methods)
e	Index of set *E*
B	Set of assets, including *A*
b	Index of set *B*
I_b	Measure of the intent to damage asset *b*
$d_{1,b}$	Measure of the disruption to national security that would occur if asset *b* were damaged
$d_{2,b}$	Measure of the mass casualties that would occur if asset *b* were damaged
$d_{3,b}$	Measure of the disruption to the economy that would occur if asset *b* were damaged
$d_{4,b}$	Measure of the disruption to public morale that would occur if asset *b* were damaged
h_b^e	Measure of the history of similar attempted attacks *e* on similar assets types *b*
c_b^e	Measure of the capabilities and resources needed to attack asset *b* by method *e*
v_b^e	Measure of asset *b*’s vulnerability to attack method *e*
Pr_b^e	Probability of a successful attack by method *e* on asset *b*
$y_{a,b}$	Binary variable that takes the value 1 if asset *b* is adjacent to link *a* and 0 otherwise
L_a^e	Likelihood that link *a* is damaged by threat *e*
$p_{a,b}^e$	Operational state of link *a* due to the security policy implemented in response to an attack on asset *b* using method *e*; $p_{a,b}^e$ takes the value 1 if link *a* is operational and 0 otherwise
q_a^p	Binary variable that takes the value 1 if the scenario involving the targeting of link *a* or assets adjacent to it and security policy *p* yields a lack of connectivity between *s* and *t* and 0 otherwise
$R_{s,t}^{e,p}$	Connectivity reliability of origin-destination pair *s,t* due to threat *e* and security policy *p*

The methodology consists of four steps, depicted in Figure 1. Each of the steps is described further below.


Step 1: Determine criteria by which terrorists may select targets

Step 2: Match asset vulnerabilities with terrorist capabilities

Step 3: Determine likelihood of transportation network link damage

Step 4: Evaluate security policies and calculate reliability

Figure 1: Methodology Outline

Step 1 Determine criteria by which terrorists may select targets

The first step is to identify the intent of the terrorists, where the intent indicates the purpose of the attack. This step delves deeper than “revenge” or “to make a statement;” this step requires consideration of how these general objectives are manifested at a more granular level. For instance, President Bush indicates that terrorists intend “to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence” (Bush, 2003, p.1). Using these criteria, or others deemed appropriate, develop a function (f_1) that assigns a value to each potential target. The function f_1 should be designed such that the maximum possible value for any asset is one and the minimum possible value is zero. The sum of the scores of all of the assets should be constrained to be no greater than one, but is not required to be one since there is no guarantee that any particular network will be struck by a terrorist event.

For purposes of this work, assume that the potential targets consist of the set of links in the transportation network, adjacent buildings, and other infrastructures’ assets that share ROW with the transportation network. All potential targets are referred to as assets in future discussion. Evaluate each asset in terms of f_1 and let I_b denote the value of f_1 for asset *b* (see equation 1).

$$I_b = f_1\left(d_{1,b}, d_{2,b}, d_{3,b}, d_{4,b}\right) \tag{1}$$

where
$d_{1,b}$ is a measure of the disruption to national security that would occur if asset *b* were damaged,
$d_{2,b}$ is a measure of the mass casualties that would occur if asset *b* were damaged,
$d_{3,b}$ is a measure of the disruption to the economy that would occur if asset *b* were damaged,
$d_{4,b}$ is a measure of the disruption to public morale that would occur if asset *b* were damaged, and
$0 \le I_b \le 1$.

The value I_b serves as the likelihood that the terrorists would view asset *b* as a desirable target, prior to considering the capabilities that would be required to damage that asset. Since I_b is a surrogate measure of likelihood, its values must take similar bounds, i.e. zero and one. This likelihood of asset selection as a target is used in Step 3.

Step 2 Match asset vulnerabilities to terrorist capabilities

The second step of the methodology is to match asset vulnerabilities with terrorist capabilities and resources. These capabilities and resources may take many forms, such as knowledge, training, weapons, finances, manpower, and transportation. These elements determine a set of attack methods (*E*) that could be used to damage the assets. For each method (*e*) identified, determine the history of similar attempted attacks on similar assets types (h_b^e); these attempts may be successful or unsuccessful. History can indicate that a terrorist group has been practicing a technique and will use it again in the future; however, a lack of history should not detract from measures of capabilities and resources. Each attack method should be evaluated separately, unless a particular attack scenario involves more than one method. These evaluations will be somewhat subjective in the absence of intelligence information.

Using the assessment of history, capabilities, and resources, determine the probability (or a surrogate measure) of a successful attack given the asset's vulnerability (see equation 2). Consider the asset's vulnerability to be a function of its inherent susceptibility to the attack method and the existence and effectiveness of protective measures. Ideally, the asset's vulnerability would be determined from a formal vulnerability assessment, however, such endeavors require the cooperation of the asset's owners, which may be difficult to obtain, especially in the short term. (An example of how this lack of information may be overcome is presented in the Example section below).

$$\Pr_b^e = f_2\left(h_b^e, c_b^e, v_b^e\right) \tag{2}$$

where
Pr_b^e is the probability of a successful attack by method *e* on asset *b*,
h_b^e is a measure of the history of similar attempted attacks on similar assets types,
c_b^e is a measure of the capabilities and resources needed to attack asset *b* by method *e*,
v_b^e is a measure of asset *b*'s vulnerability to attack method *e*, and
$0 \le \Pr_b^e \le 1.$

Since Pr_b^e is a surrogate measure of probability, the form of f_2 should be such that the values of Pr_b^e are between zero and one. The probabilities of success are used in Step 3.

Step 3 Determine likelihood of transportation network link damage

The third step is to determine the unreliability, or likelihood of damage, for each transportation network link. The likelihood of link damage is a function of the likelihood the transportation link is a target and successfully attacked, as well as the likelihood that the assets adjacent to the link are targets and attacked successfully. Equation (3) presents the calculation of the damage likelihood of the transportation network link.

$$L_a^e = \min\left[1.0, \left(\sum_{b \notin A}\left(y_{a,b}\Pr_b^e I_b\right) + \Pr_a^e I_a\right)\right] \tag{3}$$

where
L_a^e is the likelihood that transportation network link *a* is damaged by attack method *e*,
$y_{a,b}$ is a binary variable that takes the value 1 if asset *b* is adjacent to link *a* and 0 otherwise,
Pr_b^e is defined as in Step 2,
I_b is defined as in Step 1,
Pr_a^e is the probability of a successful attack on link *a* by method *e*, and
I_a is the likelihood that the terrorists would view transportation network link *a* as a desirable target.

In equation (3), the assets are associated with particular transportation links through a binary variable. The likelihood of successfully attacking each asset adjacent to link *a* is added to the likelihood that link *a* is, itself, a target and successfully attacked. Equation (3) constrains the likelihood of damage to link *a* due to attack method *e* to values between zero and one.

Step 4 Evaluate security policies and calculate reliability

The fourth step is divided into two parts. First, evaluate security policies in terms of their effects on transportation link operations. When a link is intentionally damaged, a security agency will naturally close the link for safety reasons. An attack upon an asset adjacent to the link, however, may have a similar effect upon the link. For example, a security agency may close transportation links bordering the block on which a building collapse occurs, regardless of whether the link was damaged. Law enforcement agencies may also close bridges and tunnels to prevent more terrorists from entering the city, contain those who executed the attack, and protect citizens from secondary attacks. Let $p_{a,b}^e$ represent the state of link *a* due to the security policy that is implemented in response to an attack on asset *b* using method *e* and let $p_{a,b}^e$ take the value zero if link *a* is closed and one otherwise.

The second part of Step 4 is to calculate the origin-destination connectivity reliability of the transportation network based on the state of the network resulting from the terrorist activity and the security policies that are implemented in response. Similar to previous works (see for example Iida, 1999), the operability of a link is denoted by a binary variable. However, unlike cases where link failures are random, the state of the whole network depends on which asset or set of assets is targeted because resources expended to damage one asset cannot be used on another target. In the case of terrorism, the network must be evaluated on a scenario basis. In this methodology, each scenario is defined by the link that is affected either through direct attack or by the destruction of adjacent assets. The likelihood of each scenario is L_a^e as calculated in Step

3. After implementing the security policies, the state of each link is denoted by $p_{a,b}^{e}$. Dijkstra's, or another path calculating algorithm, is used to determine whether destination *t* can be reached from origin *s*. Let q_a^p be a binary variable taking the value one if the scenario leads to a case where *s* and *t* are not connected and zero otherwise. The connectivity reliability ($R_{s,t}^{e,p}$) of the network resulting from a particular attack method and security policy is calculated as in equation (4).

$$R_{s,t}^{e,p} = 1.0 - \min\left(1.0, \sum_{a}\left(q_a^p L_a^e\right)\right) \tag{4}$$

Examination of equation (4) indicates that the maximum possible value of the network reliability is one, while the minimum is zero. The decision makers associated with a network with the reliability of one, need not be concerned with acts of terrorism within their geographic area. Otherwise, the origin-destination pair has a $R_{s,t}^{e,p}$ percent chance of remaining connected due to terrorist activity and security policies implemented in response to such events.

EXAMPLE

A small sample network is shown in Figure 2 and is used to illustrate the methodology discussed in the previous section. Suppose that the network is in the United States (US). The network consists of 18 nodes and 28 links. The origin node is labeled *s* and the destination node is labeled *t*. One link represents a bridge, another is a tunnel, and the rest are surface streets. Between the origin and destination nodes are two schools, an open field, a library, a bank, three office buildings, five retail centers, three restaurants, warehouses, a fire station, a sports stadium, a gas station, a bus depot, five apartment buildings, and twelve single family homes. Figure 2 also shows the electrical power and telecommunications lines that are adjacent to the transportation network links.

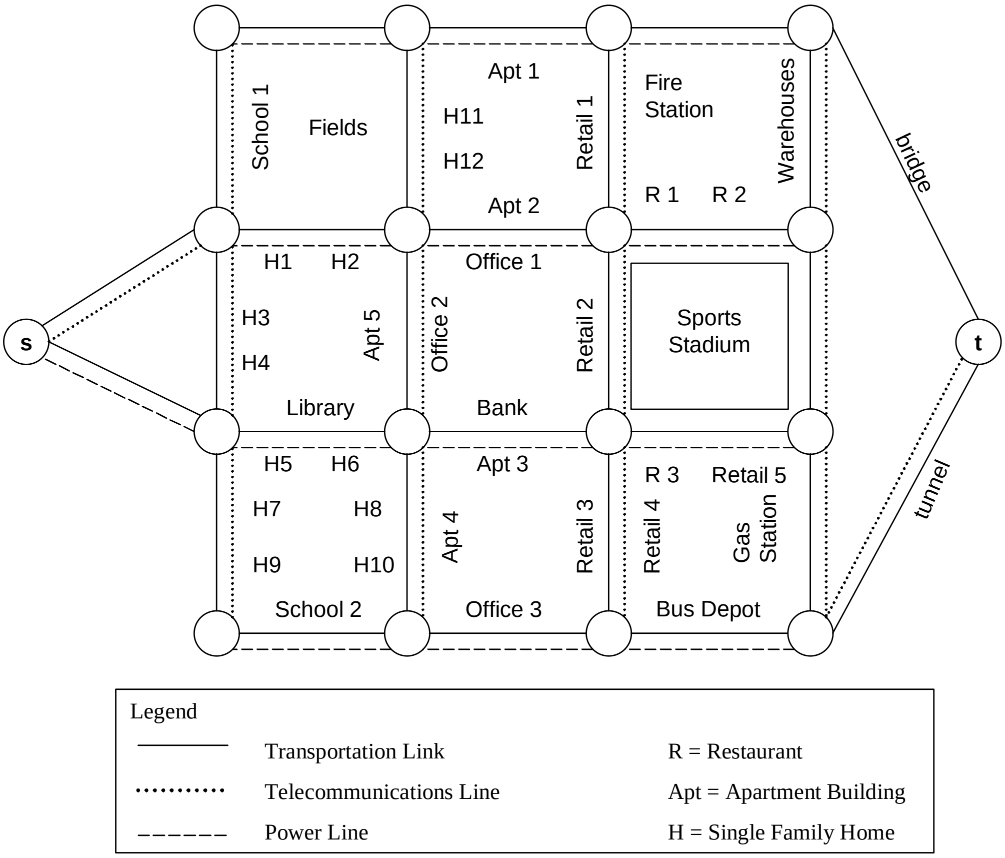


Figure 2: Sample Network with Multiple Infrastructures

Due to the detail shown in Figure 2, a separate figure (Figure 3) presents the link labels for the transportation network links.

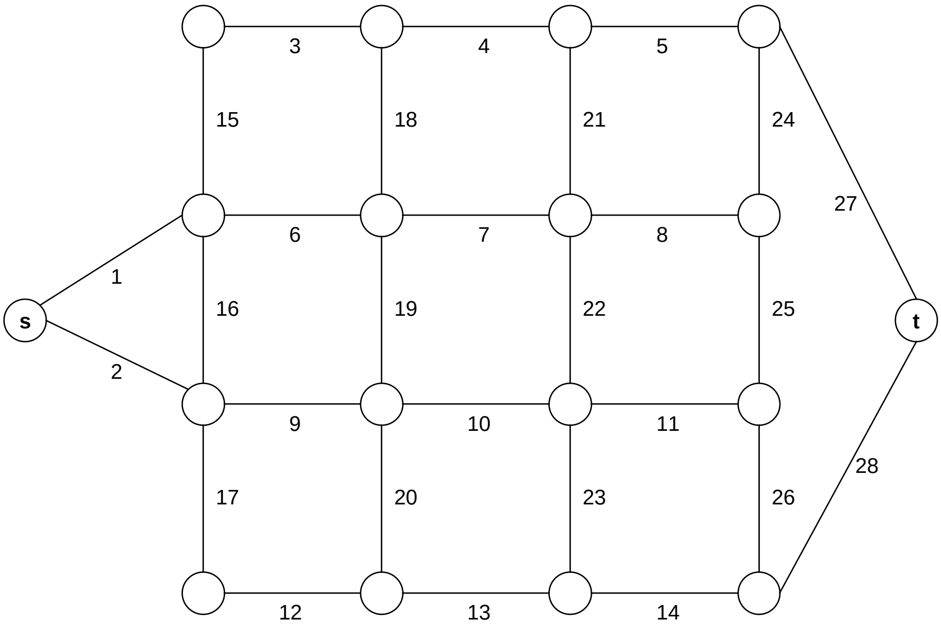


Figure 3: Transportation Network Link Labels

The methodology described in the previous section is applied to the sample network shown above. The results are displayed in a step-by-step fashion, as indicated by the methodology.

Step 1 Determine criteria by which terrorists may select targets

The criteria terrorists use to select targets are varied, but as mentioned above, may be grouped into four motivational categories: the desire to disrupt national security, inflict casualties, disrupt the target area's economy, and lower public morale. For the sake of simplicity in the discussion, suppose target selection is based solely on the number of casualties that would result from the destruction of an asset. Equation (1) then becomes a function of $d_{2,b}$ only, as shown in equation (5). In this example, the value of I_b for each asset *b* is the percentage of the US population that would be harmed if terrorists attacked asset *b*. The US population is approximately 300,000,000 (United States Census, 2005).

$$I_b = \frac{d_{2,b}}{300{,}000{,}000} \tag{5}$$

Table 2 shows the maximum number of casualties associated with each asset and the likelihood that the asset would be selected as a target. All of the casualty information is notional.

Table 2: Likelihood of Selection for Targeting

Asset	Number of Casualties $d_{2,b}$	Likelihood of Selection I_b	Asset	Number of Casualties $d_{2,b}$	Likelihood of Selection I_b
Link 1	20	6.67 x 10^{-8}	Sports Stadium	60,000	2.00 x 10^{-4}
Link 2	25	8.33 x 10^{-8}	Office Building 1	3000	1.00 x 10^{-5}
Link 3	30	1.00 x 10^{-7}	Office Building 2	5000	1.67 x 10^{-5}
Link 4	60	2.00 x 10^{-7}	Office Building 3	1000	3.33 x 10^{-6}
Link 5	75	2.50 x 10^{-7}	Apartment Building 1	75	2.5 x 10^{-7}
Link 6	20	6.67 x 10^{-8}	Apartment Building 2	500	1.67 x 10^{-6}
Link 7	70	2.33 x 10^{-7}	Apartment Building 3	750	2.5 x 10^{-6}
Link 8	100	3.33 x 10^{-7}	Apartment Building 4	1000	3.33 x 10^{-6}
Link 9	45	1.50 x 10^{-7}	Apartment Building 5	800	2.67 x 10^{-6}
Link 10	60	2.00 x 10^{-7}	School 1	500	1.67 x 10^{-6}
Link 11	150	5.00 x 10^{-7}	School 2	400	1.33 x 10^{-6}
Link 12	35	1.17 x 10^{-7}	Bus Depot	300	1.00 x 10^{-6}
Link 13	65	2.17 x 10^{-7}	Retail 1, 2, or 3	100	3.33 x 10^{-7}
Link 14	80	2.67 x 10^{-7}	Retail 4	75	2.5 x 10^{-7}
Link 15	40	1.33 x 10^{-7}	Retail 5	50	1.67 x 10^{-7}
Link 16	15	5.00 x 10^{-8}	Restaurant 1	200	6.67 x 10^{-7}
Link 17	30	1.00 x 10^{-7}	Restaurant 2	150	5.00 x 10^{-7}
Link 18	45	1.50 x 10^{-7}	Restaurant 3	50	1.67 x 10^{-7}
Link 19	200	6.67 x 10^{-7}	Warehouses	40	1.33 x 10^{-7}
Link 20	80	2.67 x 10^{-7}	Library	20	6.67 x 10^{-8}
Link 21	50	1.67 x 10^{-7}	Bank	15	5.00 x 10^{-8}
Link 22	175	5.83 x 10^{-7}	Fire Station	10	3.33 x 10^{-8}
Link 23	55	1.83 x 10^{-7}	Gas Station	10	3.33 x 10^{-8}
Link 24	50	1.67 x 10^{-7}	Fields	10	3.33 x 10^{-8}
Link 25	95	3.17 x 10^{-7}	Any Single Family Home	4	1.33 x 10^{-8}
Link 26	40	1.33 x 10^{-7}	Power Line	2	6.67 x 10^{-9}
Link 27	1000	3.33 x 10^{-6}	Telecommunications Line	1	3.33 x 10^{-9}
Link 28	750	2.50 x 10^{-6}			

Based solely on the number of casualties that could be inflicted, the terrorists would target the sports stadium because the score is an order of magnitude greater than any other potential target. The relatively small size of the network and the limited population associated with the network, compared to the US as a whole, cause the likelihood of selecting any particular asset in this network to be small.

Step 2 Match asset vulnerabilities to terrorist capabilities

Once the likelihood of terrorists selecting each asset has been determined, the methods for attacking the assets are evaluated. For this section, additional notation is used; a summary is presented in Table 3.

Table 3: Summary of Additional Notation

Notation*	Interpretation
k_b	Confidence in the terrorists having knowledge related to target *b*
k^e	Confidence in the terrorists having knowledge related to threat method *e*
w_b^e	Confidence in the terrorists being able to acquire the weapons to execute threat *e* on asset *b*
m_b^e	Confidence that the terrorists have sufficient monetary funds to execute an attack by method *e* on target *b*
j_b^e	Confidence that the terrorists have sufficient personnel to execute an attack by method *e* on target *b*
g_b^e	Confidence that the terrorists are able to acquire sufficient "get-away" and other transportation vehicles to attack target *b* by method *e*
u_b^e	Confidence that the construction material of asset *b* will fail under attack method *e*
z_b^e	Binary variable taking the value 1 if protective measures against attack method *e* are in place at asset *b* and 0 otherwise
x_b^e	Percent effectiveness of the protective measures in place at asset *b* against attack method *e*
α	Parameter, greater than 1.0, indicating the escalating influence of the history of similar attacks

* All of the variables are constrained to take values between 0 and 1, unless otherwise indicated.

For this example, five attack methods are identified as potentially causing casualties in the network. These methods consist of stationary explosive devices, car bombs, airplanes crashing into the asset, hazardous material release, and a gun assault. The capabilities of the terrorists are evaluated in terms of knowledge of the weapon (k^e), knowledge of the asset construction (k_b), the ability to obtain the weapons (w_b^e), the finances (m_b^e) and personnel (j_b^e) required to carry out the attack, and the ability to transport the weapons and personnel (g_b^e). Table 4 summarizes the history of the attack methods, in general, and the notional capability requirements for each method.

Table 4: Notional Attack Method Information

Attack Method	History	Knowledge	Weapons	Finances	Personnel	Transportation
Stationary Explosive Device	Spanish railroad, military operations, bank robberies, first attempt on World Trade Center, Oklahoma City	Specific knowledge of device and general knowledge of target construction	Explosives (1 device per 2500 intended victims)	Moderate	1 per 10,000 intended victims	1 car per 80,000 intended victims
Car bomb	Daily success in Iraq, past success in Ireland, attack on Marine quarters in Beirut	Basic knowledge of combustible materials	Explosives	Minor	1	Not applicable
Airplane crash	9/11, plans for similar attacks on Paris c. 1999 or 2000	Specific knowledge of airplane operations	Knife/gun, airplane, fuel	Moderate	3-4 per plane	Not applicable
Hazardous Material Release	Japanese subway, anthrax in U.S., nuclear accidents, accidental chemical and HazMat spills	Specific knowledge of hazardous material and transportation of such	Hazardous Material	Moderate	1 per 100 intended victims	1 car per 400 intended victims
Gun assault	School assault in Russia, attempted assault on US Capitol (mid 1990s), gang activities	Basic knowledge of firearms	Guns	Minor - Moderate	1 per 25 intended victims	1 car per 100 intended victims

Although each attack method is analyzed individually, only the analysis for an explosive device is shown below.

Predicting someone else's capabilities is a subjective process. In this work, capability is determined from one's confidence that a group would be able to meet each of the attack method requirements for the target, as in equation (6).

$$c_b^e = k_b k^e w_b^e m_b^e j_b^e g_b^e \tag{6}$$

where

k_b represents confidence in the terrorists having knowledge related to target *b*,
k^e represents confidence in the terrorists having knowledge related to threat method *e*,
w_b^e represents confidence in the terrorists being able to acquire the weapons to execute threat *e* on asset *b*,
m_b^e represents confidence that the terrorists have sufficient monetary funds to execute an attack by method *e* on target *b*,
j_b^e represents confidence that the terrorists have sufficient personnel to execute an attack by method *e* on target *b*, and
g_b^e represents confidence that the terrorists are able to acquire sufficient "get-away" and other transportation vehicles to attack target *b* by method *e*.

For all of the assets in Figure 2, the capability measure (c_b^e) is determined to be 1.0, indicating that it is reasonable to assume that a terrorist group could easily obtain explosive material, or create it from a variety of innocuous supplies, the knowledge required to handle explosives and create the device is relatively easy to acquire, information on the construction of each asset is readily accessible, the available finances are sufficient, the terrorist group consists of at least six members, and the group would have access to two vehicles.

Like the prediction of terrorist capabilities in the absence of intelligence information, determining a value for the vulnerability of a given asset to a particular attack method is somewhat subjective. Even with intelligence information, one cannot know the exact details of an attack, such as the angle of attack and the weight and combination of materials. Since the method being considered in this example is physical, vulnerabilities are determined from the construction material of the asset and the ease with which an attack could be executed against such an asset. The ease of attack is assessed by considering protective measures, such as security personnel, physical barriers, and security devices, and the effectiveness of those protective measures. Full vulnerability assessments that test the effectiveness of the protective measures are often conducted by experts. In the absence of assessments on every possible target, this work uses equation (7) to determine the vulnerability of an asset to explosive devices:

$$v_b^e = u_b^e\left(1 - z_b^e x_b^e\right) \qquad (7)$$

where

u_b^e represents percent confidence that the construction material of asset *b* will fail under attack method *e*,
z_b^e is a binary variable taking the value 1 if protective measures against attack method *e* are in place at asset *b* and 0 otherwise, and
x_b^e is the percent effectiveness of the protective measures in place at asset *b* against attack method *e*.

In equation (7), the maximum value of the vulnerability of asset *b* to attack method *e* is one and the minimum is zero. If protective measures are less than 100% effective, the value of the protective measures is reduced. Together, the protective measures and their effectiveness lessen the overall vulnerability of the asset to an explosive device. Table 5 presents the vulnerability calculation elements for the assets in Figure 2.

Table 5: Asset Vulnerability

Asset	Construction material failure u_b^e	Protective measures z_b^e	Protective measures' effectiveness x_b^e	Vulnerability v_b^e
Links 1-26	1	0	0	1
Link 27 (bridge)	1	1	0.05	0.95
Link 28 (tunnel)	1	1	0.12	0.88
Sports Stadium	1	1	0.27	0.73
Office Building 1	1	1	0.20	0.80
Office Building 2	1	1	0.23	0.77
Office Building 3	1	1	0.20	0.80
Apt Building 1 or 4	1	0	0	1
Apt Building 2, 3, or 5	1	1	0.04	0.96
School 1 or 2	1	1	0.05	0.95
Bus Depot	1	1	0.03	0.97
Retail 1, 2, 3, 4, or 5	1	1	0.05	0.95
Restaurant 1-3	1	1	0.02	0.98
Warehouses	1	1	0.03	0.97
Library	1	1	0.05	0.95
Bank	1	1	0.30	0.70
Fire Station	1	1	0.10	0.90
Gas Station	1	1	0.10	0.90
Fields	0	0	0	0
Single Family Home 1-12	1	0	0	1
Power Line	1	0	0	1
Telecommunications Line	1	0	0	1

The second column of Table 5 indicates that all of the assets in Figure 2 are constructed of a material that would fail due to explosive devices, except the fields. While an explosion would damage the fields, the device could not be attached to anything in particular and the fields would not collapse. The third column indicates which assets have protective measures in place. In this example, the bridge, tunnel, sports stadium, bank, library, bus depot, fire station, gas station, restaurants, and warehouses are monitored by video and the police conduct routine patrols along or around these assets. The office buildings, some apartment buildings, schools, and retail stores are also monitored by video but have private security on the premises. The bank also has private security personnel and alarms. The effectiveness of the security measures pertaining to each asset are estimated in the fourth column of Table 5. Finally, the overall vulnerability of the assets to explosive devices is given in the fifth column.

Combining both the vulnerability and capability results, the surrogate probabilities of successful attacks are calculated using equation (8).

$$\Pr_b^e = \left(\min\left(1.0,\ \alpha^{h_b^e} c_b^e \right) \right) v_b^e \tag{8}$$

where

h_b^e is a binary variable taking the value 1 if assets similar to *b* have been attacked by method *e* and 0 otherwise and

α is a parameter, greater than 1.0, indicating the escalating influence of the history of similar attacks (in this work, α=1.1).

In this example, a history of attacks by explosive device enhances the confidence in the terrorists having the capabilities to execute such a threat. Equation (8) ensures that the effect of the enhancement does not exceed 1.0. The capabilities are matched to the asset vulnerability to determine the likelihood that the attack is successful. Table 6 shows the results of the calculations for each asset in Figure 2.

Table 6: Probability of Success of an Attack by Explosive Device

Asset	Probability of success $\Pr_b^e$	Asset	Probability of success $\Pr_b^e$
Link 1	1	Sports Stadium	0.73
Link 2	1	Office Building 1	0.80
Link 3	1	Office Building 2	0.77
Link 4	1	Office Building 3	0.80
Link 5	1	Apartment Building 1	1
Link 6	1	Apartment Building 2	0.96
Link 7	1	Apartment Building 3	0.96
Link 8	1	Apartment Building 4	1
Link 9	1	Apartment Building 5	0.96
Link 10	1	School 1	0.95
Link 11	1	School 2	0.95
Link 12	1	Bus Depot	0.97
Link 13	1	Retail 1, 2, or 3	0.95
Link 14	1	Retail 4	0.95
Link 15	1	Retail 5	0.95
Link 16	1	Restaurant 1	0.98
Link 17	1	Restaurant 2	0.98
Link 18	1	Restaurant 3	0.98
Link 19	1	Warehouses	0.97
Link 20	1	Library	0.95
Link 21	1	Bank	0.70
Link 22	1	Fire Station	0.90
Link 23	1	Gas Station	0.90
Link 24	1	Fields	0
Link 25	1	Single Family Home	1
Link 26	1	Power Line	1
Link 27	0.95	Telecommunications Line	1
Link 28	0.88		

Table 6 indicates that an explosive device would be highly successful against the assets in the example network. Aside from the fields, the asset with the least likelihood of being successfully attacked is the sports stadium because of its protective measures.

Step 3 Determine likelihood of transportation network link damage

Once the likelihoods of target selection and attack success have been assessed for each asset, the effect of their damage on the transportation network is determined. Damage to assets adjacent to transportation links causes debris to fall onto the transportation system, rendering the link inoperable, or at least partially so. This effect, combined with the likelihood that the transportation link is, itself, the target, determines the total likelihood that the link is damaged by the attack. Table 7 lists which assets are adjacent to the individual transportation links in Figure 2 and the likelihood that the links are affected, calculated according to equation (3).

Table 7: Asset Adjacency and Likelihood of Transportation Link Damage

Link	Adjacent Assets	Likelihood of link damage	Link	Adjacent Assets	Likelihood of link damage
1	Telecommunications line	7.00×10^{-8}	15	Telecommunications line, School 1	1.72×10^{-6}
2	Power line	9.00×10^{-8}	16	Telecommunications line, Home 3, Home 4	8.00×10^{-8}
3	Power line, School 1, Fields	1.67×10^{-6}	17	Telecommunications line, Home 5, Home 7, Home 9	1.43×10^{-7}
4	Power line, Apartment Building 1	4.57×10^{-7}	18	Telecommunications line, Fields, Home 11, Home 12, Apartment Building 1, Apartment Building 2	2.03×10^{-6}
5	Power line, Fire Station, Warehouses	4.16×10^{-7}	19	Telecommunications line, Apartment Building 5, Office Building 1, Office Building 2	2.41×10^{-5}
6	Power line, School 1, Fields, Home 1, Home 2	1.68×10^{-6}	20	Telecommunications line, Apartment Building 4, Home 8, Home 10, Office 3	6.30×10^{-6}
7	Power line, Apartment Building 2, Office Building 1	9.84×10^{-6}	21	Telecommunications line, Retail 1, Fire Station, Restaurant 1	1.17×10^{-6}
8	Power line, Restaurant 1, Restaurant 2, Sports Stadium	1.47×10^{-4}	22	Telecommunications line, Retail 2,Sports Stadium	1.47×10^{-4}
9	Power line, Library, Home 5, Home 6	2.47×10^{-7}	23	Telecommunications line, Retail 3, Retail 4, Restaurant 3	9.04×10^{-7}
10	Power line, Bank, Apartment Building 3	2.64×10^{-6}	24	Telecommunications line, Warehouses	2.99×10^{-7}
11	Power line, Sports Stadium, Restaurant 3, Retail 5	1.47×10^{-4}	25	Telecommunications line, Sports Stadium	1.46×10^{-4}
12	Power line, School 2	1.39×10^{-6}	26	Telecommunications line, Retail 5, Gas Station	3.25×10^{-7}
13	Power line, Office Building 3	2.89×10^{-6}	27	None	3.17×10^{-6}
14	Power line, Bus Depot	1.24×10^{-6}	28	Telecommunications line	2.20×10^{-6}

The values in the third and sixth columns of Table 7 represent the total likelihood that a particular transportation link is damaged due to being a target and collateral damage from adjacent assets. The links most likely to be affected are links 8, 11, and 22, which border the asset with the greatest possible casualties (stadium) and provide access to various other assets. Link 25, which also borders the stadium, is slightly less likely to be damaged because it does not serve assets other than the stadium. Link 1 is the least likely to be intentionally damaged by an explosive device because it only shares ROW with a telecommunications line and very few casualties would be achieved by targeting the transportation link itself. The information provided by Table 7 is used in the second part of Step 4.

Step 4 Evaluate security policies and calculate reliability

In response to the detonation of an explosive device anywhere in Figure 2, the security policy is to:

- Close the tunnel
- Set a security check point at either end of the bridge
- Close the link adjacent to the event
- Close the links with nodes common to the affected link (i.e. adjacent to or the exact location of, the event) and on the same grid block as the event (see Figure 4).

An example of the implemented security policies is shown in Figure 4. In this illustration, the attack occurs on an asset adjacent to link 7, denoted with an "X." The heavy lines indicate which links would be closed as a result of the security policies.

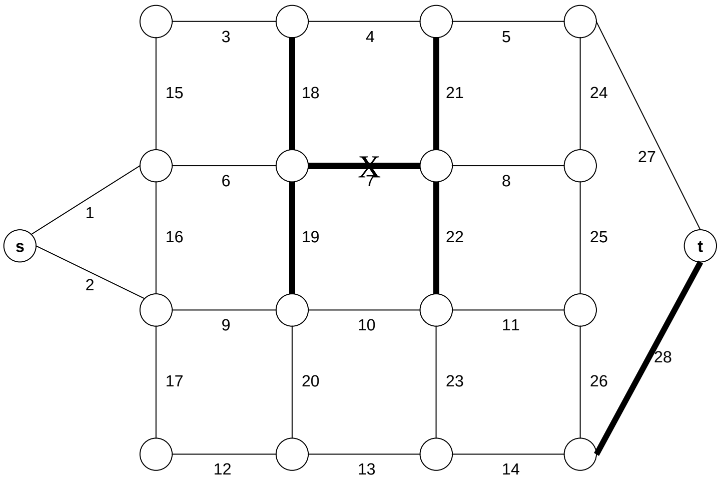


Figure 4: Illustration of Security Policy Link Closures

The probability that a link would be closed due to security policies is determined from the probability that both it and other links are damaged. Table 8 presents the scenarios of link damage, the links closed as a result of the security policy, and the state of connectivity between *s* and *t*.

Table 8: Link Damage Scenarios and Resulting Network Connectivity States

Link	Security Closures	State of Connectivity	Likelihood of Scenario	Link	Security Closures	State of Connectivity	Likelihood of Scenario
1	1,2,15,16,28	disconnected	7.00x10^{-8}	15	1,3,6,15,28	connected	1.72x10^{-6}
2	1,2,16,17,28	disconnected	9.00x10^{-8}	16	1,2,6,9,16,28	disconnected	8.00x10^{-8}
3	3,15,18,28	connected	1.67x10^{-6}	17	2,9,12,17,28	connected	1.43x10^{-7}
4	4,18,21,28	connected	4.57x10^{-7}	18	3,4,6,7,18,28	connected	2.03x10^{-6}
5	5,21,24,28	connected	4.16x10^{-7}	19	6,7,9,10,19, 28	connected	2.41x10^{-5}
6	6,15,16,18, 19,28	connected	1.68x10^{-6}	20	9,10,12,13, 20,28	connected	6.30x10^{-6}
7	7,18,19,21, 22,28	connected	9.84x10^{-6}	21	4,5,7,8,21,28	connected	1.17x10^{-6}
8	8,21,22,24, 25,28	connected	1.47x10^{-4}	22	7,8,10,11,22, 28	connected	1.47x10^{-4}
9	9,16,17,19, 20,28	connected	2.47x10^{-7}	23	10,11,13,14, 23,28	connected	9.04x10^{-7}
10	10,19,20,22, 23,28	connected	2.64x10^{-6}	24	5,8,24,27,28	disconnected	2.99x10^{-7}
11	11,22,23,25, 26,28	connected	1.47x10^{-4}	25	8,11,25,28	connected	1.46x10^{-4}
12	12,17,20,28	connected	1.39x10^{-6}	26	11,14,26,28	connected	3.25x10^{-7}
13	13,20,23,28	connected	2.89x10^{-6}	27	5,24,27,28	disconnected	3.17x10^{-6}
14	14,23,26,28	connected	1.24x10^{-6}	28	14,26,27,28	disconnected	2.20x10^{-6}

Using equation (4) and the information in Table 8, the reliability of the network in this example is 0.999994. With such a high value for the reliability of the network connectivity, the decision makers associated with the network in Figure 2 should not be overly concerned with connectivity of the transportation network between *s* and *t* under threats of terrorism and the security policies outlined in this step.

CONCLUSION

This paper has presented a methodology to estimate the connectivity reliability of a transportation network under threats of terrorism and the resulting security policies. Because predicting terrorist behavior is not an exact science, some subjectivity is incorporated into the methodology. The likelihoods that individual assets are targeted are based on the terrorists' intent. The likelihood of a successful attack against the assets, using a specific method, is based on the capabilities of the terrorists and the vulnerability of the assets to that particular attack method. The methodology uses the proximity of the assets to the transportation network links to capture the likelihood that the link is affected by collateral damage. Decision makers can use the value of the connectivity reliability (bounded by zero and one) in combination with the importance of the particular origin-destination pair under consideration to determine where to best allocate resources when making additions to the transportation network.

REFERENCES

BELL, M.G.H. (2003), "The Use of Game Theory to Measure the Vulnerability of Stochastic Networks", *IEEE Transactions on Reliability*, volume 52, number 1, pp. 63-68.

BUSH, G.W. (2003), *Homeland Security Presidential Directive/HSPD-7*, Office of the Press Secretary, The White House, Washington, D.C. http://www.fas.org/irp/offdocs/nspd/hspd-7.html , accessed March 23, 2005.

CHEN, A., YANG, H., LO, H.K., and W.H. TANG (2001), "Capacity reliability of a road network: an assessment methodology and numerical results", *Transportation Research Part B*, volume 36, pp. 225-252.

CHEN, Y.G., and M.C. YUANG (1996), "A Cut-Based Method for Terminal-Pair Reliability", *IEEE Transactions on Reliability*, volume 45, number 3, pp. 413-416.

HAIMES, Y.Y. (2004), "Risk Modeling, Assessment, and Management of Terrorism," Chapter 17 in *Risk Modeling, Assessment, and Management*, Second Edition, Wiley, New York.

IIDA, Y. (1999), "Basic Concepts And Future Directions of Road Network Reliability Analysis," *Journal of Advanced Transportation*, volume 33, number 2, pp. 125-134.

IIDA, Y. and H. WAKABAYASHI (1989), "An Approximation Method of Terminal Reliability of Road Network Using Partial Minimal Path and Cut Sets", in *Transport Policy, Management & Technology Towards 2001: Selected Proceedings of the Fifth World Conference on Transport Research*, Yokohama~shi, Japan, pp. 367-380.

MOTEFF, J. (2004), *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, Congressional Research Service, The Library of Congress, http://fpc.state.gov/fpc/36529.htm , accessed April 23, 2005.

MURRAY-TUITE, P.M. and H.S. MAHMASSANI (2004), "Methodology for the Determination of Vulnerable Links in a Transportation Network", *Transportation Research Record 1882*, pp. 88-96.

UNITED STATES CENSUS BUREAU (2005), http://www.census.gov/population/www/ accessed March 27, 2005.

YANG, S-L., HSU, N-S., LOUIE, P.W.F., and W. W-G. YEH (1996), "Water Distribution Network Reliability: Connectivity Analysis", *Journal of Infrastructure Systems*, June, pp. 54-64.

YOO, Y.B. and N. DEO (1988), "A Comparison of Algorithms for Terminal-Pair Reliability", *IEEE Transactions on Reliability*, volume 37, number 2, pp. 210-215.