Evaluating Risk of Terrorist Attack on a Cable Stayed Bridge: A Probabilistic Structural Analysis based Approach

M. Bensi, B. Bhattacharya, M. J. Chajes
University of Delaware, Newark, Delaware, USA

Abstract

It is undeniable that the security environment in the United States has changed. Acts of terrorism in the U.S. and across the globe have warranted that particular attention be paid to the vulnerability of civil infrastructure in this new environment. As a result, it is important that planners and administrators are able to evaluate risks to infrastructure in their jurisdiction in a rational manner. This will enable them to take optimal actions to manage these risks given budgetary constraints. This paper develops a method for quantifying the vulnerability of infrastructure to attack and for examining the magnitude of consequences of such an attack. It includes consideration of uncertainty in the magnitude and type of initiating events. Structural reliability principles are used to ascertain the probabilistic nature of damage to a structure given the random initiating events. Consequences of infrastructure damage are considered in terms of various costs. A case study involving a fictionalized cable stayed bridge is illustrated in this paper.

Keywords: risk, structural reliability, terrorism, vulnerability, bridge

1 Introduction

In recent years, terrorist attacks in the United States and across the globe have dramatically altered the security environment in counties around the world. This new environment has caused policy and decision makers to reassess the security and

vulnerability of their jurisdictions. Civil infrastructure is among these vulnerabilities and it has been widely accepted in the civil engineering community that transportation infrastructure, specifically bridges and tunnels, are vulnerable to terrorist attacks. While in general the highway system in the U.S. is relatively robust and redundant, major bridges and tunnels are critical structures that serve important roles for transportation, economic, and emergency management purposes. [2]. It has been estimated that an attack on any of approximately 1000 U.S. bridges could result in massive loss of life, economic disturbance, and other negative consequences on society including social and political disruption [1]. Funds for mitigating threats to infrastructure are limited and planners and administrators must make decisions on where and how to best allocate funds.

While the literature has provided ways in which planners and administrators can assess their infrastructure and even rank infrastructure for remedial actions according to specific importance criterion, much of this analysis tends to focus on *qualitative* measures of vulnerability.[1] Large organizations such as the American Association of State Highway Transportation Officials (AASHTO) and government organizations such as the Federal Highway Administration (FHWA) have made reports available to guide jurisdictions in assessing their infrastructure. Because of the comprehensive nature of these reports and other literature addressing qualitative determination of vulnerability, we do not focus on this issue in the paper and refer the reader to other sources.

A paper prepared by the Blue Ribbon Panel on Bridge and Tunnel Security (BRP) as requested by the AASHTO Transportation Security Task Force did address the issue from the perspective of risk. The intent of that paper was to make recommendations regarding polices and actions that could be implemented to reduce the probability that catastrophic consequences from an attack on infrastructure. It offers a risk assessment process that considers a variety of factors and recommends prioritization of bridge and tunnels, risk assessment to guide allocation of funds, and implementation of cost-effective security measures and design standards. [1]

We suggest that decisions regarding mitigation should first and foremost be based on probability of a structure experiencing some catastrophic measure of damage. There is, as papers such as the BRP note, uncertainty surrounding nearly all issues relating to acts of terrorism on infrastructure including the type, magnitude, and location of attack. Once an attack occurs, the performance of the structure is also random in nature. Thus, in order for owners to make rational decisions regarding mitigation, they must understand possible threats to their infrastructure as well as the uncertainty surrounding those threats and their consequences. A structural engineer familiar with a given bridge could easily enumerate a variety of ways that bridge could fail. The engineer could also identify various “worst-case scenarios” in which

[1] The literature in this area is plentiful and though a complete literature is preferable, space constraints for this paper limit the discussion of previous work.

the bridge could fail with catastrophic consequences as a result of a specific attack scenario. In an ideal world, the engineer would share this information with a bridge owner who would take the results of such as assessment and perform remedial measures, such as structural hardening, to mitigate the risk to the facility. However, in the real world, resources (including time and money) are limited. Bridge owners must make decisions regarding if, where, and how they should allocate limited dollars for mitigation. As a result, it may not be reasonable for bridge owners, who may have many bridges in their inventories competing for funds, to make decisions on worst-case scenarios. Rather, they may make decisions based on a range of possible outcomes are well as a measure of the mostly likely outcome. This would allow owners to take into account the great deal of uncertainty surrounding risk to their infrastructure so they can make rational decisions regarding necessary mitigation. In this paper, we outline a methodology that would provide owners with a means to determine what that range of outcomes regarding adverse scenario as well as a means to calculate potential costs associated with an attack of a random nature. We emphasize the use of Monte Carlo simulation coupled with structural analysis to help bridge owners assess their infrastructure.

2 Proposed Assessment Methodology

2.1 Overview

It seems reasonable to assume that most bridge owners do not know the exact likelihood that their facilities will be the target of a terrorist attack because the probability of a structure being attacked is not available. As a result, the best most owners can hope to understand is the probability that a structure will experience damage given an attack. Letting: I = Initiating event; T_i = Event that a terrorist attack occurs; D = Event that there is damage to the structure; C = Cost; we seek $P[D(I) \mid T_i]$ and $E[C \mid T_i]$.We also seek a measure of expected damage:

$$\overline{D} = \sum_{i=1}^{N} E\langle D \mid T_i \rangle P(T_i), \text{ where } \sum_{i=1}^{N} P(T_i) = 1.$$

The methodology can be performed in three major steps:

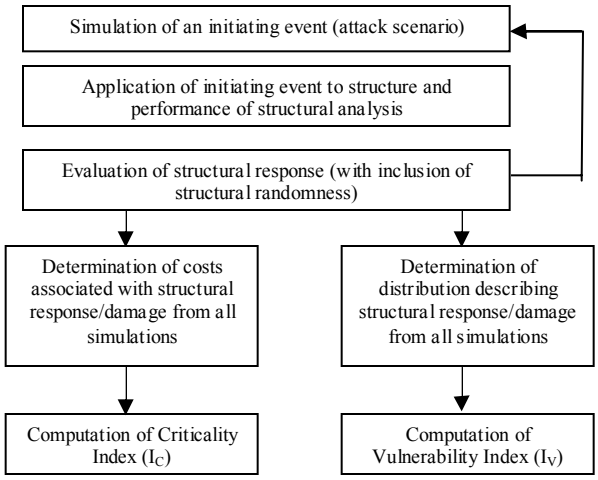
1. Designation of an initiating event and a probability distribution describing the magnitude or severity of the initiating event. Examples of initiating events include blast pressures, collisions, load reversals, or loss of cross-sectional area of a girder or loss of cables.
2. Designation of a means to measure damage and a probability distribution to quantify damage based on an initiating event. Examples of damage measurements include deflections, cables lost, girder cross-section destroyed, or loss in ADT.

3. Determination of costs associated with damage and a loss function to describe expected loss given an attack. Examples of costs include reconstruction costs, loss in toll revenues, loss of life, or other socio-economic costs.

A graphical representation of this method is presented in Figure 1.

These three steps will yield two values: a Vulnerability Index and a Criticality Index. The Vulnerability Index (I_v) is a value based primarily on the strength and geometric properties of the structure. It gives a normalized value representing the how likely a structure is to experience damage given an initiating event. The Criticality Index is likewise a normalized value that provides an indicator of the relative importance of a structure in the inventory. It is based primarily on the expected value of the loss due to damage (losses range from reconstruction costs to loss of life to economic disruption). The Indices are designed to be numerical indicators that can be used to compare structures for infrastructure management purposes.

Figure 1: Methodological Overview



2.2 Definition of Initiating Events and Measures of Damage

Descriptions of random initiating events (attack scenarios) require some subjectivity and acquaintance with the bridges and threat environment; we must hypothesize reasonable malevolent extreme events that a structure could experience. The methodology outlined in this paper requires one to quantify all possible

components of the initiating event (I_j) (i.e. magnitude, location) to describe it completely in terms of a probability distribution $p[I_j \mid T_i]$.

Once we have determined the distribution from which to draw random initiating events we must choose how to quantify damage to the structure: Will we use deflection or loss in load carrying capacity or some other indicator of damage?

Once the initiating event and critical structural response have been determined, we then use finite element structural analysis programs to analyze the structure's response to the event (i.e. how does the bridge deflect when a fraction of the girders in removed). We repeat this Monte Carlo process many times, randomly simulating an event, analyzing the structure and recording the structure's response. This allows us to derive a distribution of damage based on the initiating event. That is, we derive $p[D(I) \mid T)]$.

2.3 Calculation of Vulnerability Index

The Vulnerability Index can be interpreted as an indicator of the potential for experiencing damage (vulnerability) given that a terrorist attack occurs. When we repeat the simulations and analysis many times, we essentially have a "database" of results. From this we can draw inferences about the average damage, mean value of the initiating event, etc. Most importantly, within the context of this paper, we can use these results of calculate a Vulnerability Index (I_v). I_v is weighted average of normalized measures of damage.

$$I_v = \sum_{i=1}^{n} \alpha_i \frac{E[\text{damage measure}_i]}{\text{Critical}[\text{damage measure}_i]}.$$

Where α_i is determined subjectively to reflect the relative importance of one damage measure over another and such that $\sum_i \alpha_i = 1$ and n is the number of damage measures to be used.

2.4 Calculation of Expected Loss and Criticality Index

After calculating the distribution of damage, we then utilize the results to calculate a distribution of loss. Losses can include, but are not limited to, loss of life, reconstruction costs, loss in ADT, loss of revenue, emergency route closure and user delay costs. The BRP determined that "loss of a critical bridge or tunnel at one of the numerous "choke points" in the highway system could result in hundreds or thousands of causalities, billions of dollars worth of direction reconstruction costs, and even greater socio-economic costs." [1] Thus, it is important to consider these costs when assessing the status of bridges in an inventory. For each initiating event, there is an associated amount of damage to the structure. We can then calculate the Criticality Index (I_c) based on the total costs (or individual cost components) of a

structure. Unlike the Vulnerability Index which is based strictly on the individual structural response of one bridge, the Criticality Index is based on a value normalized with other bridges in the inventory. Letting $C_i^{(m)}$ = cost component *i* of bridge *m* and β_i = a weight associated with the importance of cost measure *i*, the Vulnerability Index for bridge *m* in the system of *j* bridges is defined as follows:

$$I_C^{(m)} = \sum_{i=1}^{n} \beta_i \frac{E[C_i^{(m)}]}{\sum_{k=1}^{j} E[C_i^{(k)}]}.$$

Thus, the Criticality Index provides a measure of relative loss to the owner and/or society given an attack. In other words, it indicates how critical the loss of the structure would be relative to other bridges in the inventory.

Now that the owner has both indices in hand, they will allow for a direct means of comparison. While many well-known decision criterion provide similar results, we have diverged in that we attempt to compare and make decision regarding vastly different structures. We conjecture that the decision should be made jointly based on structural reliability and the expected loss associated with it. For example, using the Vulnerability Index, an owner may learn that signature *A* (say, a cable-stayed bridge) is more structurally vulnerable than bridge *B* under the same kind of attack. However he losses associated with bridge *B* may be relatively higher than bridge *A*. The following section provides a case-study for illustration of the above method.

3 Illustrative Example Utilizing a Cable-stayed Bridge

In order to illustrate the methodology outlined in this paper, a case study has been developed. The methodology will be used to evaluate a rudimentary model of a cable-stayed bridge. Because of security concerns, a fictionalized structure has been utilized so as not to jeopardize any existing structure. The bridge has an overall length of approximately 2000 ft with an approximately 1000 foot main span, cable diameter of 1 foot, and 42 cables per pylon. It should be noted that the structural analysis used in the case study (using STAAD.Pro 2003) only accounts for elastic response and is performed for purely illustrative purposes and should not be a used as an indicator of an actual cable-stayed bridge performance in the event of an attack.

As part of this case study, we have made several assumptions that have simplified the analysis to allow for ease in explanation of it as an illustrative example. We begin by designating our initializing event: an attack on the structure that occurs on the bridge's main span and that destroys only cables. We only consider loss of cables as a result of an attack on the main span as a simplifying assumption, however as noted in the BRP report: the cables, pylons, deck, cable saddle, approach structures, connections, and piers [1] are all vulnerable components

of a cable stayed bridge. Next, we consider as our measure of damage the displacement of the deck (δ_{max}) as well as the length of deck damaged (L_D). Like our initiating event, one may choose to consider alternate measures of damage in addition to displacement; however inclusion of such would make this example more complicated.

For this example, we quantify the initiating event by three components: location of the centroid of an attack on the main span (X_D), number of cables to the left destroyed (N_L), and the number of cables to the right destroyed (N_R). In the absence of other information, we assume that X_D is equally likely to occur anywhere along the main span and is thus distributed according to the distribution with the most entropy: the uniform distribution. We utilize information from the BRP report and National Needs Assessment for Ensuring Transportation Infrastructure Security – Contractor's Final Report to obtain a distribution from which to draw the magnitude of attack (N_L and N_R). We consider threats that range from portable, hand placed charges to car and boat delivered explosions to larger vehicle (i.e. semi-trailers) explosive delivery or ramming. [2]. The BRP suggests the highest probability attack with conventional explosives is a car bomb and with regards to collision the highest probable vehicle is an H-15 truck [1]. Because we have relatively more information regarding attack magnitude we assume that the distribution from which to draw N_L and N_R, is binomial distribution with parameters p= ½, n=10. An example of one attack scenario is presented in Figure 2.

We take the information above and perform 33 simulations of random initiating events and impose those attacks on the structure. We then analyze the structure to obtain the displacements of all nodes on the structure. For example, if in one iteration, we randomly selected cable 25 as our centroid and next selected that 4 cables to the left and 5 cables to the right would be destroyed on each side, we would run an analysis with those 10 cables removed and record the displacement of each node of the structure. We extrapolate the location and magnitude of the maximum displacement experienced by the structure as a result of each attack. To account for structural randomness (or variability in the strength and response of structural components) we multiply the maximum displacement experienced by the structure by a "randomness factor" based on a lognormal distribution with mean=1.05 and coefficient of variation=20%. The results of the simulations and analyses are contained in Table 1.

The I_v for this case study is a weighted average of the ratio of mean magnitude of the maximum displacement and the largest displacement experienced by the structure and the ratio of average distance from the center of the maximum displacement and the absolute farthest distance from the center (it is assumed that the farther the maximum is from the center the more damage the structure will experience because of the steepness of the angle). If we take α_1= 0.8 and α_2= 0.2, then

$$I_v = \alpha_1 \frac{\overline{\delta_{max}}}{\delta_{max}^*} + \alpha_2 \frac{\overline{L_D}}{L_D^*} = 0.8\frac{23\text{in}}{80\text{in}} + 0.2\frac{224in}{250in} = .41$$

Where δ_{max}^* is the critical displacement and is equal to (Span Length)/150. L_D^* is the critical length of deck damaged and is equal to 25% of the main span length. This number provides a measure of the relative magnitude of the average structural response to the critical structural response. That is, it provides an indictor of how likely a structure is to experience some critical level of damage. In general, the overarching idea is that a similar method would be used for other bridges in the inventory to obtain a vulnerability index for each bridge in the inventory. Then, the vulnerability indices can be compared with structurally inadequate bridges having a higher index.

For simplicity, in this example, we consider only costs incurred by the owner as a result of an attack on the bridge (cost of cable and deck replacement) and do not account for lost revenue from tolls, user costs from delays, economic consequences, loss of life, and other socioeconomic consequences. Information regarding costs is provided in Table 1. It is important to note that because we are working with an entirely fictionalized structure, the costs are likewise fictional. Cost functions have been selected merely to provide results that are somewhat reasonable but that may not reflect actual losses from an attack. Unfortunately, because we are only considering one bridge, it is not possible to compute a Criticality Index because this value is based on the expected cost associated with an attack on the bridge in relation to the expected cost of attacks on other bridges in the inventory. As such, calculation of this value is not included. Graphs summarizing the example are contained in Figures 3, 4 and 5.

4 Conclusion

In this paper we developed a methodology for assessing, in a rational manner, the vulnerability of a bridge to terrorism as well as costs associated damage from an attack. We accounted for uncertainty in attack magnitude as well as a structural performance using Monte Carlo techniques. The methodology includes calculation of Vulnerability and Criticality Indices for purposes of quantifying risks to structures independently as well as relative to other structure in an inventory. A illustrative example of a cable-stayed bridge was used to demonstrate the methodology.

Table 1: Results Summary

scenario	Number of cables des-troyed	Location of δmax from end	Approx. distance of δmax from center span	Cost for cables	Cable Installation Costs	Length of deck damaged	Cost of deck replace-ment	Total cost	δmax
		(feet)	(feet)	(thousands)	(thousands)	(feet)	(thousands)	(thousands)	(inches)
1	13	726	198	$1,950	$1,140.00	824.15	$2,678	$5,768	33.19
2	9	968	22	$1,350	$948.00	146.92	$477	$2,775	14.45
3	13	924	0	$1,950	$1,140.00	474.22	$1,541	$4,631	56.91
4	11	1408	462	$1,650	$1,048.00	495.91	$1,611	$4,309	10.59
5	7	1430	484	$1,050	$836.00	92.68	$301	$2,187	1.90
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
30	11	924	0	$1,650	$1,048.00	391.36	$1,271	$3,969	46.96
31	15	968	22	$2,250	$1,224.00	71.25	$231	$3,705	7.01
32	10	1166	220	$1,500	$1,000.00	660.62	$2,147	$4,647	24.77
33	11	1364	418	$1,650	$1,048.00	1997.70	$6,492	$9,190	46.28

Figure 2: Bridge Layout and Example of Attack Scenario

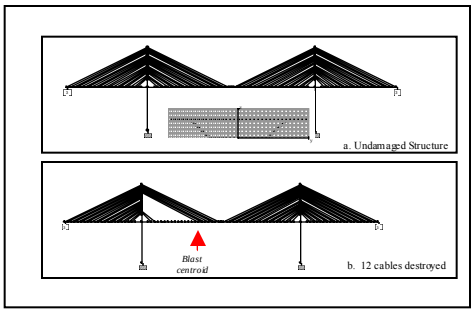


Figure 3: Magnitude and Location of δ_{max} on Bridge

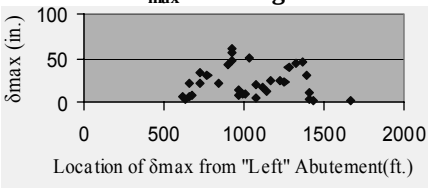
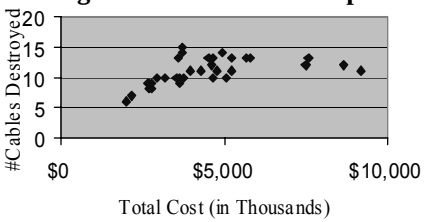


Figure 4: Total Cost Compared to Number of Cables Destroyed and δ_{max}



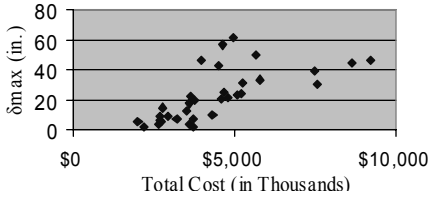


Figure 5: δ_{max} Compared to Attack Magnitude and Location

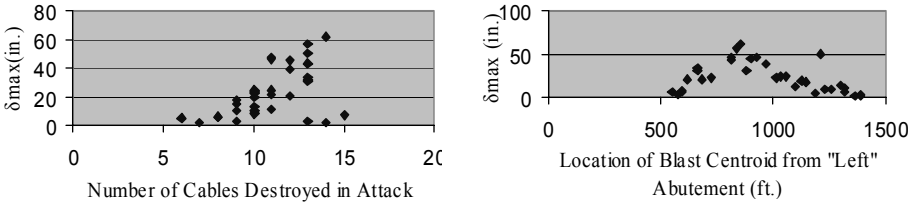
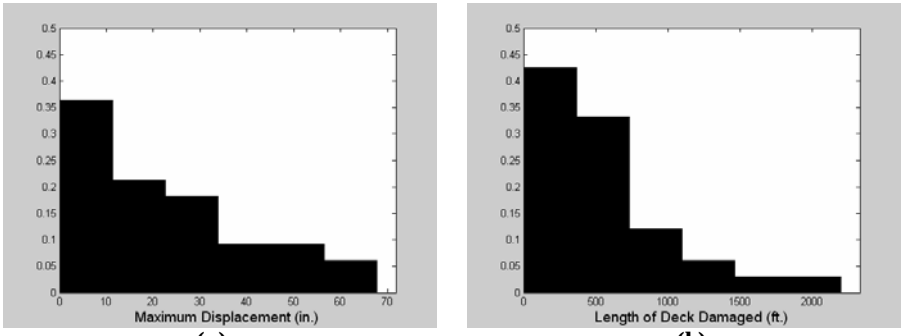


Figure 6: Histograms of δ_{max} (a) and Length of Deck Damage (b)



(a) **(b)**

References

[1] The Blue Ribbon Panel on Bridge and Tunnel Security- FHWA and AASHTO, *Recommendations for Bridge and Tunnel Security* September, 2003.

[2] Ham, D.B., Lockwood, C. (Parsons Brincerhoff and Science Applications International Coorperation, National Needs Assessment for Ensuring Transportation Infrastructure Security, October, 2002.

[3] Science Applications International Corporation, *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002.