A Fuzzy Approach for Assessing Transportation Infrastructure Security

Michelle S. Dojutrek, Samuel Labi, and J. Eric Dietz

Abstract. The security of any transportation infrastructure can be defined as a combination of threat likelihood, infrastructure resilience, and consequence. In view of their inherently dynamic and highly unpredictable nature, threat likelihood and consequence data is difficult to determine with certainty. Due to this problem, this paper presents a new fuzzy methodology to qualitatively determine the overall security level, in terms of a security rating, for transportation infrastructure by duly considering the uncertainties of the environmental threats it faces, its resilience to damage, and the consequences of the infrastructure damage. The method is useful when data is unavailable or imprecise, allowing the security rating to be determined using a qualitative expert-assigned level that each factor contributes to overall security. The evaluation of the security factors are represented as fuzzy triangular numbers with accompanying membership rules that define the extent of contribution by each factor to overall infrastructure security. Through a case study, the paper applies the methodology to illustrate how general data can be used in the method to determine the overall security of specific infrastructure.

1 Introduction

Transportation comprises many modes of travel including air, rail, vehicle, waterway, and pipeline. Due to their typical large diversity, size, and connectedness, national transportation systems are vital to the economy and

Michelle S. Dojutrek · Samuel Labi
Purdue University, Department of Civil Engineering, West Lafayette, IN, USA

J. Eric Dietz
Purdue University, Department of Computer and Information Technology,
Purdue Homeland Security Institute, IN, USA
e-mail: {mdojutre,labi,dietz}@purdue.edu

F. Boulanger et al. (eds.), *Complex Systems Design & Management*,
DOI: 10.1007/978-3-319-11617-4_15

security. The abundance of infrastructure networks has led to their criticality in performing the functions of everyday life as well as their interconnectedness with other infrastructure networks, industries, and workforces that rely upon them (Barker et al., 2013). The transportation industry enables a monumental amount of passengers and goods to move throughout the world annually (Polzin 2012; DHS, 2011). Activities in the U. S. transportation sector make up 12% of the gross domestic economy and most businesses rely on a functioning transportation system to move their products. The U.S.'s Marine Transportation System, including ports, waterways, and vessels, handles more than $900 billion in international commerce every year (Lundquist, 2011). Freight revenue on U.S. railroads in 2010 was $56.3 billion with coal taking up 43% of the total commodities shipped (AAR, 2012). Airlines in the U.S. totaled $134.7 billion for 2011 revenue, 6.8% higher than the previous record set in 2008 (Herbst, 2012).

The failure of transportation infrastructure could occur as a result of any of multiple types of events. Unintended termination of transportation infrastructure is caused by infrastructure failure such as design flaws, fatigue, advanced deterioration and other internal causes (Labi, 2014). Infrastructure is also affected by unintended outside forces such as overloading, accidents, natural events and other external causes. Additionally, infrastructure may be damaged by intentional man-made forces such as terrorism. Transportation infrastructure makes attractive targets of intentional harmful attacks because of their visibility, accessibility, and capacity to carry large numbers of commuters in a relatively confined space (Steffey, 2008). Maritime and surface transportation systems are vulnerable to attacks by terrorists who seek to attract publicity, inflict high numbers of civilian casualties, and cause political and economic disruption (Harris et al, 2012). The range of potential threats to infrastructure is wide and if the infrastructure can withstand these effects by being bolstered against likely threats, consequences can be reduced. Due to the need for openness and accessibility at thousands of entry points, the wide geographic distribution of infrastructure, and the static nature of some routes, complete protection of surface transportation infrastructure is simply not feasible (Steffey, 2008). Therefore, creating infrastructure that is resilient would mitigate the need for continuous efforts to oversee the security of infrastructure with limited manpower.

Ezell et al, 2000 framed five key steps to risk management to provide evidence for security investments to subsequently reduce the overall infrastructure damage in the event of disaster:

- **Measure** the threat likelihood posed by external or intentional threats to the asset
- **Monitor** the threat likelihood over time
- **Assess** the effectiveness of actions intended to reduce consequences
- **Communicate** this information to the general public and legislators
- **Provide** evidence for appropriate resources

It has been argued that both the scale and nature of transportation systems necessitate that a reasonable degree of risk must be accepted, even for critical infrastructure, because complete mitigation is not feasible. Formal methodologies for assessing and managing risks to transportation security provide a valuable conceptual structure and practical tools for allocating resources in cost-effective ways to improve public safety (Steffey, 2008). The United Kingdom policy, Publicly Available Specification 55 Part 2 (PAS 55-2), states that risk management is fundamental for proactive infrastructure management and that its purpose is to understand the cause, effect and likelihood of adverse events occurring in order to manage these risks to an acceptable level; Also, the International Infrastructure Management Manual (IIMM), a guidance document focused on experience in Australia, New Zealand, UK, South Africa and the US (INGENIUM, 2006), recommends that core infrastructure management should identify critical infrastructure and events and apply risk management to these infrastructure (Hooper et al., 2009).

The uncertain nature of security factors such as threat likelihood, infrastructure resilience, and consequence must be considered in any security metric (Dojutrek et al, 2014). For example, hazards are highly non-deterministic such as the magnitude of earthquakes or the number of accidents, and cannot be predicted at 100% accuracy. The failure to consider uncertainty could lead to infrastructure being unprepared for the potential range of hazards that will act on the infrastructure and therefore cause greater consequences (Dojutrek et al, 2014). Additionally, infrastructure that is highly resilient to hazards in the area could potentially withstand the threat and therefore cause little resulting consequences. Uncertainty can be accounted for by using historical data trends, predictive models, and expert opinion to provide a range of threat likelihood, consequence, and resilience scenarios that would potentially affect the infrastructure. Unexpected damage from natural occurrences and man-made incidents increase infrastructure repair costs and lives lost. If infrastructure is made resilient against these threats, damage and costs can be reduced. Thus, a metric for identifying infrastructure in need of improvements for security purposes can help prioritize infrastructure for the limited funds dedicated to transportation needs. To capture the dynamic nature of the security factors, fuzziness will be used in the development of the security metric. Furthermore, due to the uncertain nature of threats (their occurrence and magnitudes cannot be predicted with complete certainty (Dojutrek, 2014)), it is vital to incorporate concepts of uncertainty in any analysis that deals with risk prediction and security investment evaluation. Failure to consider uncertainty can lead to overestimation or underestimation of the likelihood of the threat, damage to the infrastructure, and consequences of the damage to the community. Uncertainty can be quantified by analyzing historical data trends and developing models for threat likelihoods and magnitudes, infrastructure damage due to the threat, resilience enhancement due to the security investments, and community consequences of threat occurrence.

2 A Review of Past Work

The Oxford English Dictionary (online) defines risk as "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility." Different definitions of risk exist, but in relation to infrastructure management, a risk definition should involve the combination of probability and consequence of any uncertain event (Hooper et al., 2009). Quantifying and assessing risk involves the calculation and comparison of probabilities, but most expressions involve compound measures that consider both the probability of harm and its severity; thus, quantitative risk assessment is an important growing component of the larger field of risk assessment that includes priority setting and management of risk (Melnick and Everitt, 2008).

Due to the difficulties in quantifying key components of threat, vulnerability, and consequence assessments, analyses of transportation security risk typically employ qualitative methods in making judgments about the relative magnitudes of various risk scenarios (Steffey, 2008). There is concern that in the allocation of general resources or security-specific funding, only high valued infrastructure would receive high priority. A weighted qualitative approach could be used to ensure that the lower-valued infrastructure receive due consideration during the evaluation process (Dojutrek et al, 2014). For example, a specific measure involving asset size or asset cost could be weighted higher or lower to allow other factors to gain more importance in the framework.

Threat, resilience, and consequence information are involved in risk assessment while risk management involves deciding which protective measures to take based on an agreed upon risk reduction strategy (Moteff, 2005). Risk is a multidimensional concept which is often expressed as the Cartesian product in the context of risk analysis for critical infrastructure (McGill et al., 2008):

$$Risk = threat \bullet infrastructure\ vulnerability\ or\ resilience \bullet consequence \quad (1)$$

Where, *threat* is an adverse event, *consequence* is the repercussions of the infrastructure loss, and *infrastructure vulnerability or resilience* is the target weaknesses that can be exploited by an adversary to achieve a given degree of loss or cause the infrastructure to fail during a natural hazard.

The TMC Risk Assessment Methodology (TCM RAM) is a combination from three different sources, the Systematic Assessment of Facility Risk (SAFR), a methodology developed by the DHS Office of Domestic Preparedness in its toolkit, and ideas from AASHTO's Guide for Vulnerability Assessment (SAIC, 2005). The steps in this method include: infrastructure identification, threat assessment, consequence assessment, vulnerability assessment, and countermeasure development, and it evaluates risk in terms of a terrorist attack using Equation 2.

$$RR = TA \cdot T \cdot C \cdot (1 - LD) \cdot (1 - LS) \quad (2)$$

Where, *RR* (Relative Risk) is a function of the overall threat to the infrastructure or facility, *T*; the attractiveness of a particular target to a given adversary, *TA*; the potential consequences of a successful attack on a target, *C*; the ability to deter an adversary from attempting an attack, *LD* (expressed in terms of the inability to deter, or *1-LD*); and the effectiveness of the system to prevent an attack should one be attempted, *LS* (expressed in terms of system ineffectiveness, or *1-LS*).

This method evaluates vulnerability and criticality in terms of relative risk and target attractiveness. However, calculating the relative risk for specific infrastructure has limited value because it indicates only the risk associated with that infrastructure relative to the highest and lowest possible *RR* values (Venna and Fricker, 2009). The TMC RAM is a theoretically good model, but requires a lot of expert effort to quantify the value of subjective criteria which could introduce inconsistency and variance into the model.

Xia et al. (2004) developed a framework for risk assessment that includes static and dynamic infrastructure characteristics in the event of a terrorist attack. The risk score of a highway component is defined as a linear combination of three indices:

$$R = (\propto A + \beta B) \cdot \frac{C}{100} \tag{3}$$

Where, *R* is the risk score of highway network component; *A* is the static characteristic index; *B* is the dynamic characteristic index; *C* is the attack potential index; α is the weight of the static characteristic index; and β is the weight of the dynamic characteristic index.

The static characteristics (Index A) include: structural stability, number of alternatives, and response resources of highway components. The dynamic characteristics (Index B) include: dynamic traffic flow information such as volume, speed, occupancy, vehicle classification, and queue length as well as weather details and work zone activities. The potential of a terrorism attempt (Index C) is estimated in terms of functional significance and symbolic importance of a highway component (Xia et al, 2004). The study did not include uncertainty.

The score of Indices A, B, and C are calculated as:

$$A = aW_{A1} + bW_{A2} + cW_{A3} + dW_{A4} \tag{4}$$

$$B = eW_{B1} + fW_{B2} + gW_{B3} + hW_{B4} + iW_{B5} \tag{5}$$

$$C = jW_{C1} + kW_{C2} \tag{6}$$

Where, *W*'s are the weights predetermined with the help of experts; and *a, b, c, d, e, f, g, h, i, j, k* are characteristics pertaining to each index.

McGill and Ayyub (2008) used fuzzy logic to approximate the true functional relationship between the effectiveness of six security system capabilities (access control, personnel barriers, vehicle barriers, surveillance systems, guard force, and reaction force with heavy weapons) and probability of adversary success. The goal of the model is to provide a system based on approximate reasoning that produces an estimate for the probability of adversary success based on the subjective evaluation of several or more defensive criteria. $Pr(S|A_i)$ is the probability of adversary success (S) given the occurrence of initiation event A_i and the complementary event $Pr(\bar{S}|A_i)$ as the security system effectiveness. Each defensive criterion (six security system capabilities) can take on a linguistic value of "Low," "Medium," or "High" defined on a constructed scale for effectiveness with membership functions. The consequent Pr(S|A) may take on linguistic values such as "Likely," "Certain," or "Even Chance." There is the possibility that each defensive criterion may require its own set of linguistic phrases for effectiveness, for example if one criteriaon was based on a constructed scale and another on a crisp scale such as time. A user (security expert) can subjectively assign a value to each premise of criterion on a scale of 0-10 or an alternate scale for a given facility of infrastructure and attack type once the fuzzy inference rules are defined.

Another study by Yazdani et al., (2012) identified the risk criteria and used Fuzzy TOPSIS as an uncertainty-based multi-criteria decision-making technique to determine the weights of each criterion and the importance of investment alternatives with respect to the risk criteria. This framework extends the Risk Analysis and Management for Critical Infrastructure Protection (RAMCAP) method by introducing new parameters to assess the effects on risk value. According to the authors, the TOPSIS method helps decision-makers carry out analysis and comparisons in ranking their preference of the alternatives with vague or imprecise data. It is based on the concept that the chosen alternative should have the shortest distance from the most ideal solution and the farthest distance from the least ideal solution.

A study by Yang et al. (2009) uses a fuzzy evidential reasoning (ER) method to conduct maritime security assessments. The authors developed a subjective assessment and management framework using fuzzy ER approaches. The consequence parameter is a security parameter which can be derived from multiple risk parameters: will, damage capability, recovery difficulty, and damage probability. *Will* is the likelihood of a threat-based risk, which directly represents the lengths a malicious attacker goes through in taking a certain action. To estimate *will*, one may choose to use such linguistic terms such as "Very weak," "Weak," "Average," "Strong," and "Very strong." The combination of *damage capability* and *recovery difficulty* represents the consequence severity of the threat-based risk. Specifically speaking, *damage capability* indicates the destructive force/execution of a certain action and *recovery difficulty* hints at the resilience of the system after the occurrence of a failure or disaster (Yang et al., 2009). The following linguistic terms can be considered as a reference to be used in subjectively describing the two sister parameters: "Negligible," "Moderate,"

"Critical," and "Catastrophic" for *damage capability* and "Easy," "Average," "Difficult," and "Extremely Difficult" for *recovery difficulty*. *Damage probability* means the probability of the occurrence of consequences and can be defined as the probability that damage consequences happen given the occurrence of the event, and could be described using terms such as "Unlikely," "Average," "Likely," and "Definite" (Yang et al., 2007; Yang et al., 2009).

The TMC RAM methodology identified key aspects of infrastructure that terrorists may consider in an attempt to cause destruction and developed a risk equation to capture these factors, but did not consider dynamic concepts or uncertainty of the variables. The method developed by Xia et al, (2004) addressed the dynamic nature of specific infrastructure aspects without including uncertainty. McGill and Ayyub (2008) developed a fuzzy approach to assess the effectiveness of security system capabilities from the terrorist perspective, but did not look specifically at infrastructure characteristics or the natural threat perspective. Yazdani et al, (2012) added two new criteria into the traditional risk equation and input the new criteria into a fuzzy framework. Yang et al, (2009) further developed the variables used in the traditional risk equation to include new parameters based on terrorist attack for maritime transport and input these into a fuzzy evidential reasoning framework. The method does not break down the variables into infrastructure specific subcategories.

Based on limitations of past studies, the method described in the next section is further developed to include fuzzy logic to capture the dynamic and uncertain nature of each identified security factor for transportation infrastructure. The method further breaks down each factor into additional measures and attributes which are also fuzzified. This allows each infrastructure characteristic to be qualitatively assigned a level of influence based on expert opinion. The fuzzy output therefore provides decision makers with a method to capture the security level of an infrastructure without precise or detailed data; rather it allows experts to make decisions based on their experience by qualitatively assigning levels to each variable of security in the method.

3 Methodology

3.1 Security Rating

A synthesis of past work has generally shown that the security of an infrastructure is a function of three main factors: the Threat Likelihood, Infrastructure Resilience, and Consequence (Dojutrek et al, 2014). The combined effect of these three factors is a security rating metric. This paper duly accommodates the fact that all three factors are characterized by a significant degree of uncertainty and therefore introduces fuzziness in the levels of these factors and subsequently, in their outcome (i.e. security rating). The enhancements to the method with allow experts to use the security rating method without imprecise data. Figure 1 illustrates the framework used in the paper.

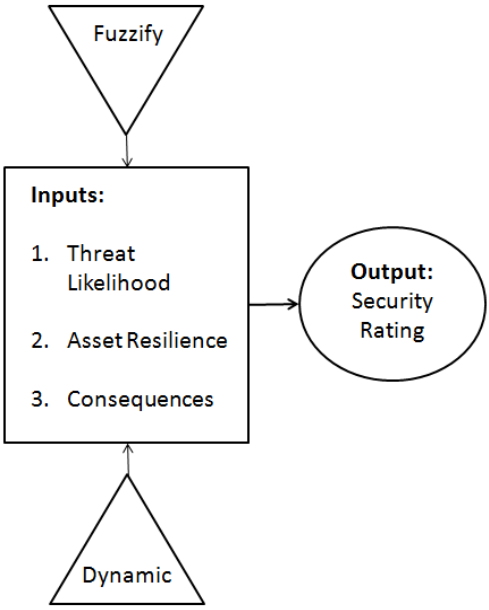

Fig. 1 Framework

The three inputs that influence infrastructure security are herein referred to as security factors. Each factor has a set of measures that quantify how much the factor contributes to overall infrastructure security. Each measure is further decomposed into a set of associated attributes that determine the level of the measure rated on a scale to define the overall amount that the measure contributes to the factor (Dojutrek, 2014). Most attributes have different units, therefore the attribute data were scaled to address these dimensional inconsistencies by rating them on a scale of 1 to 5, 1 representing an attribute level associated with high security and 5 representing an attribute level associated with low security.

The formulation of the security rating expression is shown in Figure 2. The overall security rating equation used to determine the level of infrastructure security is shown in Equation 7. For a high level of threat likelihood and consequence, and a low level of resilience, the security rating decreases. For a high level of resilience, and a low level of threat likelihood and consequence, the security rating increases. This metric is useful in determining if infrastructure is secure and how the infrastructure compares to others in the system.

Factor	$F_i = w_1 M_1 + \cdots + w_j M_j$ Where F_i is security factor i, w_j is weight of measure j, and M_j is security measure j
Measure	$M_j = \frac{s_1 \times \cdots \times s_N}{N}$ Where s_N is security attribute of measure j
Attribute	$s_N \rightarrow s_N^*$ Where S_N^* is the scaled attribute
Security Rating	$\text{Security Rating} = \frac{\sum \text{factors associated with high security}}{\sum \text{factors associated with low security}}$

N is the total number of security attributes for measure j of factor i

Fig. 2 Security Rating Formulation

The overall security rating equation (Equation 7) divides the resilience factor (factor associated with high security) by the factor of threat likelihood and consequence factors (factors associated with low security).

$$SR_a = \frac{F_{Ra}^{\alpha}}{\left(F_{TLa}^{\delta} + F_{Ca}^{\lambda}\right)} \tag{7}$$

Where SR_a is the Security Rating for infrastructure a; F_{TLa} is the threat likelihood factor of infrastructure a; α is the exponential weight of the resilience factor; F_{Ca} is the consequence factor of infrastructure a; δ is the exponential weight of the threat likelihood factor; F_{Ra} is the resilience factor of infrastructure a; and λ is the exponential weight of the consequence factor.

The security rating can be placed on a scale and interpretations made as seen in Figure 3 and Table 1 which are for illustrative purposes for the case study (Dojutrek et al, 2014). The scale and cut-offs can be established at any specific agency to suit their policies.

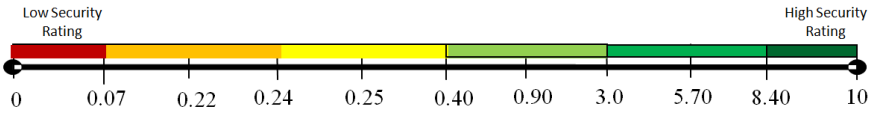

Fig. 3 Security Rating Scale

Table 1 Interpretation of Security Rating

Security Rating	Example Interpretation
≤ 0.21	Indicates a great need for security improvement of the infrastructure. The infrastructure has generally very low security thus immediate action should be undertaken to enhance its resilience and thus to reduce the possible consequences of threats.
0.21 – 0.25	Indicates significant need for security improvement needs of the infrastructure. For this infrastructure, the agency should be poised to undertake actions in the very near future, to enhance resilience and thus to reduce possible consequences of the infrastructure failure.
0.25–0.40	Indicates medium-to-high security improvement needs. Facilities within this range can be monitored at a frequency slightly exceeding standard frequency. The risk of failure can be tolerated until a normal capital project (to enhance resilience and thus reduce consequences, among other benefits) is carried out.
0.40–0.95	Indicates low-to-medium security improvement needs. Unexpected failure can be avoided during the remaining service life of the infrastructure by performing standard scheduled inspections with due attention to specific design features that influence the infrastructure possible consequences.
0.95–3.03	Indicates low security improvement need. Often reflective of the likelihood of threat to a civil engineering system built to the current design standards in a low threat likelihood environment.
3.03–10	Indicates little or zero security improvement needs.

3.2 Fuzzy Logic Framework

A fuzzy logic framework for subjective fuzzification (Figure 4) of measures and attributes for resulting fuzzy output factors is useful when decision makers do not have access to infrastructure specific information for each factor. This method inputs fuzzy data into the security rating equation to find a fuzzy output. Matlab Fuzzy Toolbox was used to program the framework (MathWorks, 2013). For example, each factor can be fuzzified to output a level of that specific factor as seen for the resilience factor in Figure 5. Each measure has a degree of membership ranging from low to high on a determined scale. The value of the resilience factor depends on the level of each measure and the measure levels are determined by respective attributes. Each fuzzified factor value is then input into the overall security rating fuzzy system that results in a fuzzy security rating for a specific infrastructure (Figure 6).

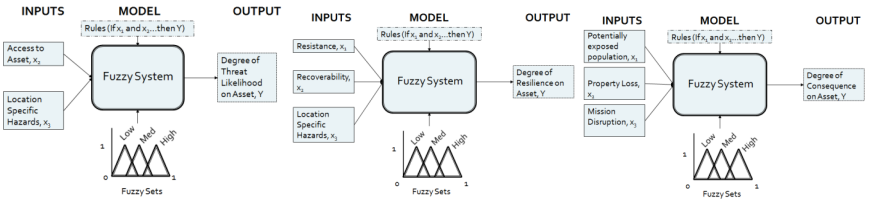

Fig. 4 Fuzzy Logic Models of Security Rating Factors

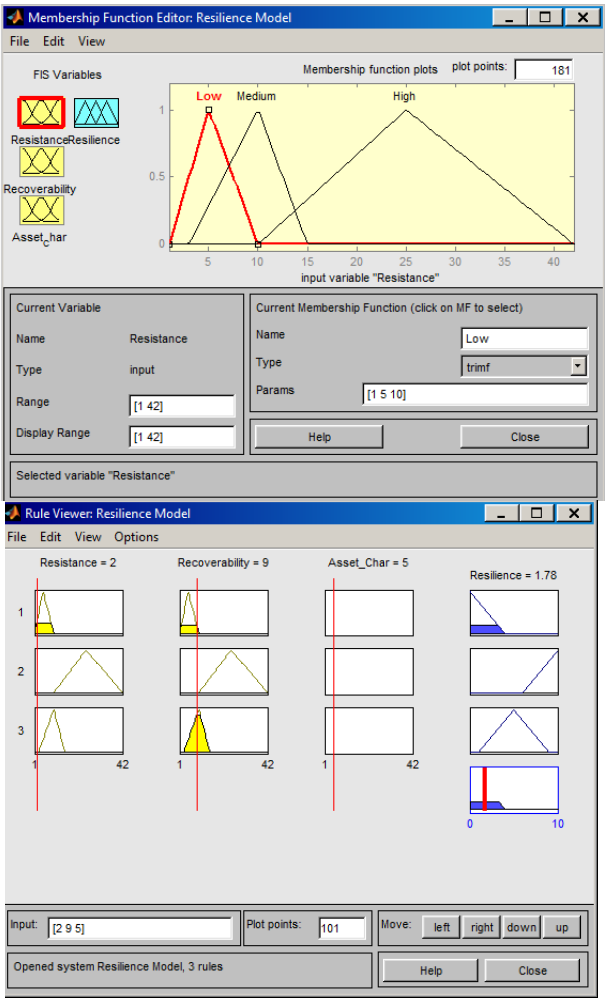

Fig. 5 Fuzzy Consequence Factor and Attributes

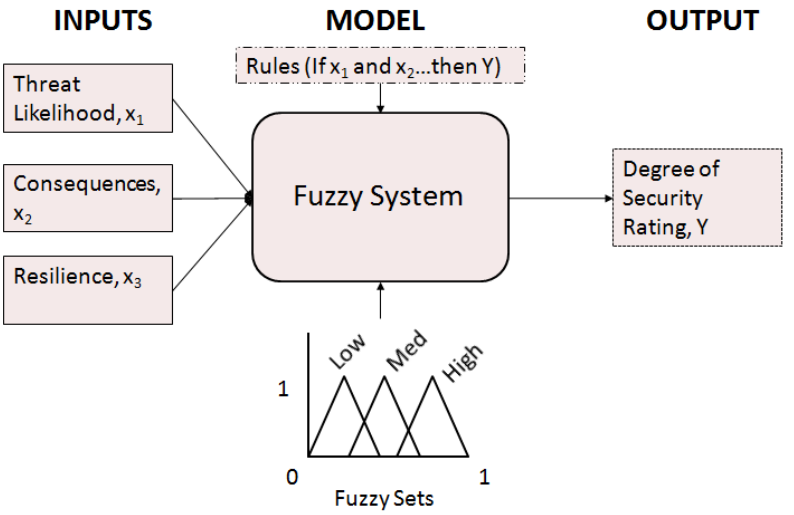

Fig. 6 Fuzzy Security Rating

3.3 Rules

Fuzzy rules were developed to determine the fuzzy security rating output for the fuzzy logic system. The rules give mathematical meaning to the different linguistic levels of each factor in the security rating framework. Thus, a complete fuzzy inference system is created. Fuzzy membership functions for the security rating are shown in Figure 7.

Rules:
If *resilience* is high, *consequence* is low, and *threat likelihood* is low, then *SR* is high
If *resilience* is high, *consequence* is high, and *threat likelihood* is high, then *SR* is medium
If *resilience* is high, *consequence* is medium, and *threat likelihood* is medium, then *SR* is medium
If *resilience* is medium, *consequence* is medium, and *threat likelihood* is medium, then *SR* is medium
If *resilience* is medium, *consequence* is low, and *threat likelihood* is low, then *SR* is medium
If *resilience* is medium, *consequence* is high, and *threat likelihood* is high, then *SR* is low
If *resilience* is low, *consequence* is medium, and *threat likelihood* is medium, then *SR* is low
If *resilience* is low, *consequence* is high, and *threat likelihood* is high, then *SR* is low
If *resilience* is low, *consequence* is low, and *threat likelihood* is low, then *SR* is medium

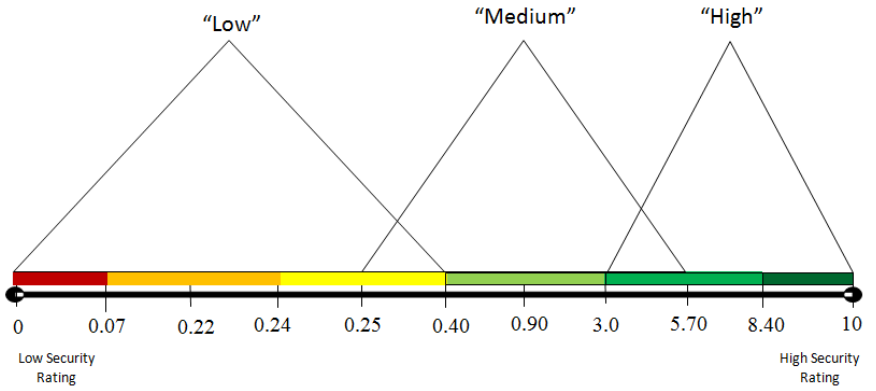

Fig. 7 Fuzzy Membership Functions

4 Case Study

To demonstrate the study methodology, the National Bridge Inventory structure number B05015800100000, the Leo Frigo Memorial Bridge in Brown County, Green Bay, Wisconsin was used (Figure 8). Data was gathered from the National Bridge Inventory dataset available online.

Fig. 8 Leo Frigo Memorial Bridge, Green Bay, Wisconsin

The factors, measures, and attributes used for the case study are described in Figure 9.

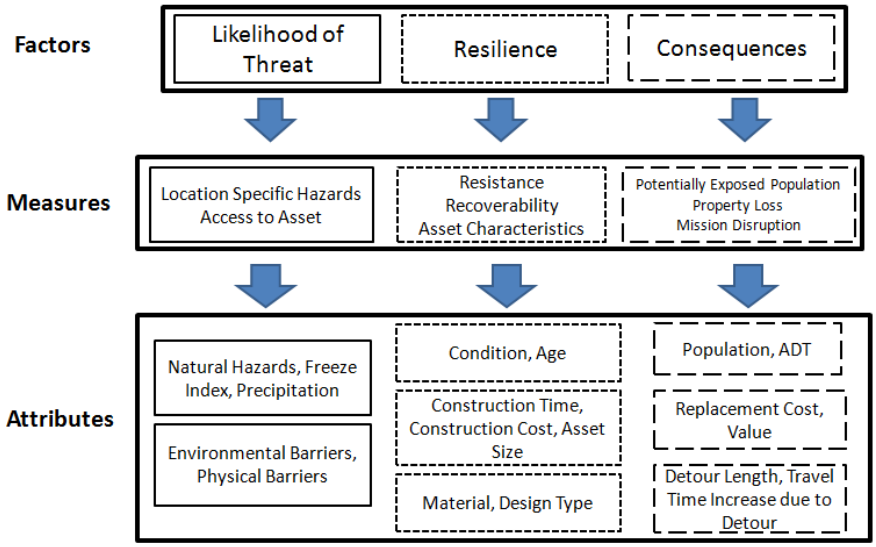

Fig. 9 Detailed Framework for Case Study

A number of assumptions were made for the case study. First, the construction time was based on the bridge size. Second, environmental barriers were assumed to be the waterway under the bridge. The detour travel speed was assumed to be 45mph and all weights in the security rating equation (α, δ, λ) and measures equation were assumed to be equal. Threat likelihood measures, attributes, and scales can be seen in Table 2. The result of each measure is the scaled attributes multiplied together and normalized by the number of attributes for each measure, then multiplied by the measure's weight. Measure weights were assumed to be equal, therefore a value of one was used. After the results are input into the fuzzy threat likelihood factor system, a fuzzy degree of threat likelihood is determined.

Table 2 LFM Bridge Threat Likelihood Factor Data

Measure	Attributes	Data	Scaled	Results
Access to Infrastructure	Env Barriers	Over Fox River	3	3
	Physical Barriers	Independent bridge protection	2	
Location Specific Hazards	Natural Hazards	High Winds, Fog	4	2.66
	County Freeze Index	189.3	2	
	County Precipitation	29.52	1	

The resilience measures, attributes, and scales are listed in Table 3. After the results are input into the fuzzy resilience factor system, a fuzzy degree of resilience is 1.53.

Table 3 LFM Bridge Resilience Factor Data

Measure	Attributes	Data	Scaled	Results
Resistance	Condition	Deck: 8	1	2
		Superstructure: 7	1	
		Substructure: 6	2	
	Age	35 yrs	4	
Recoverability	Const. Time	3yrs	3	9
	Const. Cost	$6.85M	3	
	Infrastructure Size	39,115 ft^2	3	
Infrastructure Characteristics	Material	Steel	2	5
	Design Type	Thru-Arch	5	

The consequence measures, attributes, and scales are listed in Table 4. After the results are input into the fuzzy consequence factor system, a fuzzy degree of consequence is 1.78.

Table 4 LFM Bridge Consequence Factor Data

Measure	Attributes	Data	Scaled	Results
Potentially Exposed Population	Population	Green Bay: 104,868 Brown County: 253,032	4	6
	AADT	31,400	3	
Property Loss	Replacement Cost	$6.92M	3	3
	EDMC Value	$4.34M	2	
Mission Disruption	Detour Length (miles)	~6 miles	2	4
	Inc. in travel time due to detour	8 min	4	

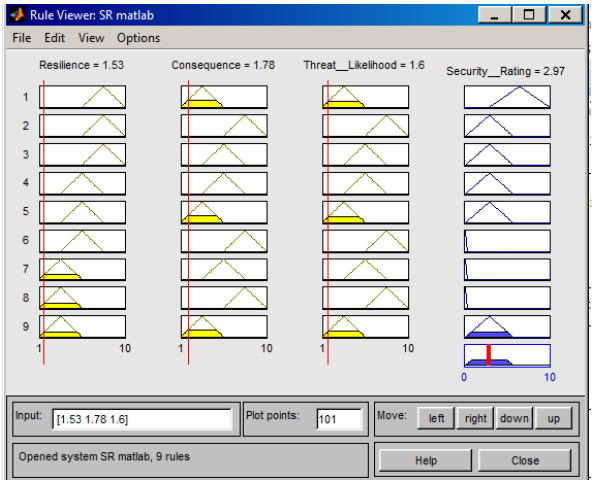

Fig. 10 Overall Fuzzy Security Rating

Each fuzzy factor value was then input into the fuzzy security rating system to result in a fuzzy security rating output for the Leo Frigo Memorial Bridge of 1.6. The overall fuzzy Security Rating of the Leo Frigo Memorial Bridge is then 2.97, which corresponds to a security rating of "medium" as shown in Figure 10.

5 Conclusion and Discussion

Previous literature either did not consider the dynamic or uncertain nature of security data and factors or focused on a terrorist perspective. Threats also include a natural element, such as earthquakes, floods, hurricanes, climate changes, etc. A method that is adaptable to both natural and man-made threat perspectives would require less initial work on the decision-makers' part. Additionally, a method that can transform qualitative information into a quantitative form would be useful to help prioritize among infrastructure for security funding allocation purposes.

This paper first presents a framework to quantify security based on a metric that includes the key factors of risk (threat likelihood, infrastructure resilience, and consequence). These factors have an inherently dynamic and uncertain nature which creates difficulty in accurately predicting their values. Therefore, a methodology to quantify these principal security components through a qualitative method of fuzzy logic was further developed. A qualitative method will enable decision-makers to make decisions about the relative magnitudes of these difficult to quantify security variables. Each security factor was fuzzified using "high," "medium," and "low" levels of its respective measures and membership functions. The fuzzified factors were then input into a fuzzy security rating framework that output the resulting fuzzy security rating for specific infrastructure. A fuzzy system captures the dynamic and uncertain nature of each security factor by creating a fuzzy set of numbers for each level of membership.

The Leo Frigo Memorial Bridge in Green Bay, Wisconsin, U.S.A. was used as a case study for the framework. Data were taken from the United States National Bridge Inventory database to use as an example for determining security measure levels and membership functions for each security factor. All attribute data was scaled and the respective measures fuzzified for input into the overall fuzzy security rating framework. Based on the output, the Leo Frigo Memorial Bridge resulted in a "medium" security rating of 2.97. The case study illustrated how the fuzzy security rating can be determined accounting for the dynamic and uncertain nature of the data.

References

1. Barker, K., Ramirez-Marquez, J.E., Rocco, C.M.: Resilience-based network component importance measures. Reliability Engineering & System Safety 117, 89–97 (2013)
2. Steffey, D.L.: Homeland Security and Transportation Risk. Encyclopedia of Quantitative Risk Analysis and Assessment. John Wiley & Sons, England (2008)
3. Polzin, S.E.: Security Consideration in Transportation Planning. STC White Paper. Center for Urban Transportation Research, University of South Florida (2012) (accessed December 10, 2012)
4. Lundquist, E.H.: International Port Security Program. Defense Media Network (2011), http://www.defensemedianetwork.com/stories/international-port-security-program/ (March 17, 2011)
5. AAR. Class I Railroad Statistics. Association of American Railroads (May 10, 2012)
6. Herbst, B.: Airline Industry-Year 2011 (2012), http://www.airlinefinancials.com/uploads/Airline_Industry-Year_2011ReviewOutlook.pdf, AirlineFinancials.com (March 30, 2012)
7. Labi, S.: Introduction to Civil Engineering Systems. Wiley, Hoboken (2014)
8. Harris, S.P., Dixon, D.S., Dunn, D.L., Romich, A.N.: Simulation Modeling for Maritime Port Security. Journal of Defense Modeling and Simulations: Applications, Methodology, Technology 10(2), 193–201 (2012)
9. Ezell, B.C., Farr, J.V., Wiese, I.: Infrastructure risk analysis model. ASCE Journal of Infrastructure Systems 6(3), 114–117 (2000)
10. INGENIUM, International Infrastructure Management Manual. International Edition, Version 3.0, INGENIUM, Thames, New Zealand (2006), http://www.nams.org.nz/International%20Infrastructure%20Management%20Mannual
11. Hooper, R., Armitage, R., Gallagher, A., Osorio, T.: Whole-life Infrastructure Infrastructure Management: Good Practice Guide for Civil Infrastructure. CIRIA, London (2009)
12. Dojutrek, M.S., Labi, S., Dietz, J.E.: A Multi-criteria Methodology for Measuring the Resilience of Transportation Infrastructure. International Journal of Disaster Resilience in the Built Environment (2014)
13. Dojutrek, M.S.: A Stochastic Multi-criteria Assessment of Transportation Security Investment (working doctoral dissertation), Purdue University, W. Lafayette, IN (June 2014)

14. Melnick, E.L., Everitt, B.S.: Encyclopedia of Quantitative Risk Analysis and Assessment. John Wiley & Sons, West Sussex (2008)
15. Moteff, J.: Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Congressional Research Service. The Library of Congress (2005)
16. McGill, W.L.: Critical Infrastructure and Portfolio Risk Analysis for Homeland Security. Ph. D. Dissertation. University of Maryland. Department of Civil and Environmental Engineering. College Park, MD (2008)
17. SAIC, Reducing Security Risk for Transportation Management Centers. Presented at the 84th Annual Research Board Meeting (2005)
18. Venna, H.R., Fricker, J.D.: Synthesis of Best Practices in Transportation Security, vol. I. Vulnerability Assessment, Joint Transportation Research Program, Indiana Department of Transportation and Purdue University, West Lafayette, IN (2009)
19. Xia, J., Chen, M., Lie, R.: A Framework for Risk Assessment of Highway Network. Presented at the 84th Annual Transportation Research Board Meeting (2004)
20. McGill, W.L., Ayyub, B.M.: Multicriteria Security System Performance Assessment Using Fuzzy Logic. Journal of Defense Modeling and Simulation Applications, Methodology, Technology 4(4), 1–21 (2008)
21. Yazdani, M., Alidoosti, A., Basiri, M.H.: Risk Analysis for Critical Infrastructure Using Fuzzy TOPSIS. Journal of Management Research 4(1), 1–19 (2012)
22. Yang, Z.L., Bonsall, S., Fang, Q.G., Wang, J.: Maritime Security-Assessment and Management. Journal of International Association of Maritime University 5(1), 56–72 (2007)
23. Yang, Z.L., Wang, J., Bonsall, S., Fang, Q.G.: Use of Fuzzy Evidential Reasoning in Maritime Security Assessment. Risk Analysis 29(1), 95–120 (2009)
24. MathWorks, MATLAB and Fuzzy Toolbox Release, The MathWorks, Inc., Natick, Massachusetts, United States (2013)