https://doi.org/10.26552/com.C.2013.4.58-62

Michal Titko - Adam Zagorecki *

MODELLING VULNERABILITY OF TRANSPORTATION NETWORK USING INFLUENCE DIAGRAMS

The transportation network (TN) is important to serve the national priorities such as economic sustainability and growth, but it as well plays important role in disaster management and is subject to hazards. The understanding of the TN resilience and vulnerabilities is important for the national security. In this work we focus on the notion of TN vulnerability. We propose the use of a decision-theoretic approach based on Influence Diagrams (IDs). We argue that the use of IDs (1) provides an improved framework for risk assessment through more elaborate combining probabilities and consequences, and (2) facilitates knowledge elicitation from human experts through a structured approach to the problem. The proposed methodology is intended to be applied to the critical infrastructure.

Keywords*: Vulnerability, transportation, critical infrastructure, influence diagrams.*

1. Introduction

The recent years have witnessed several examples of the transportation infrastructure being affected by extreme natural hazards such as the earthquake in Kobe (1995) and hurricane Katrina (2005) as well as man-made threats such as terrorist attacks (Madrid 2004, London 2005) or industrial accidents [1]. Even, if the transportation infrastructure is not directly affected during such incidents, it plays critical role in providing security for public as it plays key role in delivering disaster relief, or facilitating mass evacuations. Some parts of the transportation network are more important than the others, resulting in identification of the notion of critical infrastructure – a subset of the transportation infrastructure that is of the particular importance and interest.

The transportation network (TN) is important to serve the national priorities such as economic sustainability and growth, social development, providing security and public order, operational capability of the armed forces, etc. Analysis of TN should always be viewed in a broader context – with relation to geo-spatial, industrial, social context, etc. Reliability and performance of TN have significant influence on services which are provided by the other sectors, and in many instances TN spans these sectors. Therefore, the understanding of the TN weak points and its resilience to disasters is important in general, and in particular critical for the national security.

In this work we focus on the notion of TN vulnerability. Understanding vulnerability is not only essential to disaster management, but also important in transportation planning, development, and management. Berdica [2] argues that reducing vulnerability can hence be regarded as reducing risks involved in various incidents. We can interpret vulnerability as the measurement of the degradation or loss of TN's functions, but as we will discuss it, the exact definition is a subject of active academic debates.

In this paper we use a decision-theoretic approach based on Influence Diagrams (IDs) as a tool for model vulnerability. We argue that the use of IDs can address two important aspects of vulnerability modelling: (1) provide an improved framework for risk assessment through more elaborate combining probabilities and measures of consequences than it is the case in current approaches, and (2) facilitate knowledge elicitation from human experts through a structured approach to the problem.

2. Relevant work

The key function of a TN is to provide means to move people and goods between the origin and destination, usually by optimizing the transport costs. Typically transportation network infrastructure is modelled as a graph where links represent connections between two points and nodes represent hubs.

The elements of the graph have typically some attributes associated with them that are intended to represent properties of the elements of the TN such the number of lanes, average number of vehicles per day, etc. Such models can be used to simulate different disruptions and predict how the TN would respond to those conditions. Consequences resulting from the disruption of the transport element can vary depending on many factors such as network topology, properties of particular network element, the population characteristics around it, likelihood of disruptive events, etc. In ordinary cases TN has certain capacity to absorb some degree of disruptions. When larger scale events such as natural disasters are considered, there is possibility of more extreme effects on network infrastructure, including its partial

* [1]**Michal Titko,** [2]**Adam Zagorecki**
[1]Department of Crisis Management, Faculty of Special Engineering, University of Zilina, Slovakia, E-mail: Michal.Titko@fsi.uniza.sk
[2]Cranfield University, Department of Informatics and Systems Engineering, Defence Academy of the United Kingdom, United Kingdom

failure. In recent years it has been of interest of academic and practitioners' communities to quantify these effects. Eventually, the concept of *vulnerability* has been introduced.

There is no consensus on the definition of vulnerability in the context of TN. One can define the vulnerability as overall susceptibility to a specific hazardous event. It is also the magnitude of the damage given the occurrence of that event [3]. Some authors [4 and 5] argue that a system might be vulnerable to certain events but be resilient to others; therefore, it is important to account for the specific risk and threat profiles to the area under analysis.

There is common agreement that the vulnerability in the context of TN represents a measure of loss of the TN's capabilities to perform its functions [2 and 6 - 9]. However, there are individual interpretations. According to Taylor and D'Este's a vulnerable network node is such a node for which a loss (or substantial degradation) of a small number of links significantly diminishes the accessibility of the node. Their model described in [6] is used as the basis for the probabilistic algorithm for the choice of certain section by a passenger (carrier). Model is based on the definition of the vulnerability which can be simplified as: in case the "best" route is not available, how much worse (more expensive) would the second best option be than the third one and so on. Berdica [2] defines vulnerability as susceptibility of TN to incidents that can result in considerable reduction in TN serviceability. Yang, Qian developed a method for the assessment of TN vulnerability using the users' final lost time as measurement [7]. Jenelius et al. [8] focused on the socio-economic impacts of transport network dysfunction. This approach represents an effort to express the vulnerability of the transport network using the measure of satisfaction of the demand for transport services at the time when a section of the network is unavailable. Husdal [9] defined vulnerability as the consequential cost of the lack of reliability, and this consequential cost must compromise not only the immediate toll on the network-users, but the overall socio-economic costs on the community that this vulnerability would entail.

One of the interpretations of vulnerability in the transportation context is closely related to reliability. Linking these two concepts should give the means to define vulnerabilities as costs resulting from a lack of reliability [2, 6, 8 and [9] and in our work we follow this trend. In wider interpretation, reliability can be regarded as a complement of vulnerability. Berdica [2] proposed the following definition: vulnerability in road transportation system is reliability, meaning adequate serviceability under the operating conditions encountered during a given time period. Between vulnerability and reliability are certain differences which could be expressed as follows: appropriate measures to improve reliability may not have to be suitable to reduce the vulnerability. Vulnerable does not have to imply unreliable and vice-versa.

The concept of vulnerability is more often understood as the consequences of link failure, irrespective of the probability of the failure. In some cases, link failure may be unlikely but the resulting impact on the community may be devastating [6]. Slivone [10] claims that ignoring the probability of failure is justified, as in some instances producing probabilities for some events are virtually impossible (warfare, sabotage, terrorist attack, etc.). However, as was argued, vulnerability must be related to specific hazardous events and, therefore, ignoring the event's probability deprives the definition from an important element, as it is the likelihood of events that often differentiates more vulnerable areas from those less vulnerable.

The aim of vulnerability assessment is not to provide overall value of the vulnerability measure of the TN as a whole but to identify the weak points (most vulnerable) of the network. If one wants to analyse vulnerability of the TN it is necessary to divide the network into atomic elements – links and nodes for which the vulnerability scores would be determined. The patterns of connectivity for the TN are also important for modelling of the TN. Simple example of TN is shown in Fig. 1._

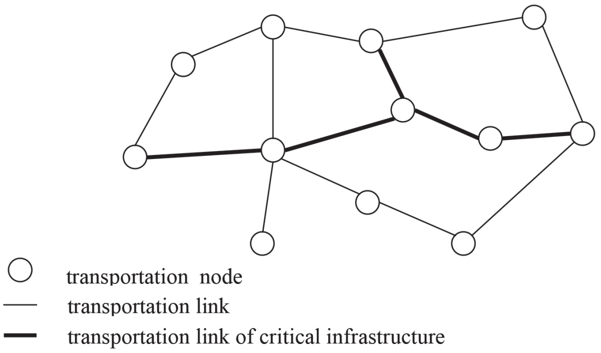


Fig. 1 Simple example of transportation network

To provide practical value of the vulnerability analysis it is important to identify to what type of events or threats TN's element is vulnerable. In general, the TN can be vulnerable to a wide range of influences and disruptions that can lead to an operational degradation. They can be the results of changes in environmental conditions or qualities pertaining to the network characteristics. One applicable categorisation of influences to TN is offered by Brathen and Laegran [11]: *structure*, *nature*, *traffic*, and *malevolence*.

Structure-related influences pertain to the way the infrastructure is built, and attributes of the network itself - in terms of topology, and connectivity. It also captures factors such as the physical body of the road, geometry, width, curvature, gradient, tunnels, bridges, access restrictions for certain vehicle types, etc. Nature-related influences relate to adverse natural processes, such as flash floods, avalanches, falling rocks, snow and ice, fog, earthquakes, tsunamis, etc. Traffic-related influences pertain to attributes describing the generic flow of traffic such as traffic accidents, maintenance operations, construction works and civil emergencies [11]. Malevolence related influences pertain to the intentional man-induced disruption of the traffic – examples include terrorist attacks and acts of sabotage.

To undertake a risks assessment (even if it is limited to geophysical aspect only) throughout the whole TN is not practical and cost-effective, according to Taylor and D´Este [6]. It is simply because the cost of such thorough assessment that would result in any practically useful results for the whole spectrum of risks would be too high. However, the vulnerability analysis provides a different approach to this problem. It could be used to find structural weaknesses which make the network more sensitive to the consequences of any failures or degradation of its parts without the need to perform a complete thorough risk assessment for the whole TN. This is why we argue to focus the analysis on a subset of TN, namely the critical infrastructure, which can be identified by the experts or through simulations. The process should start with identification of key threats and corresponding probabilities as well as specifying the elements of TN for which serviceability could be affected. Then the collected information would be used for suggesting or realising appropriate strategies to reduce risk of occurring of the identified threats and means to enhance resilience of the elements of TN. In this way we could combine vulnerability, risk, hazardous events and serviceability. Understanding of relation between them could result in improved framework for risk and vulnerability assessment as well as of vulnerability modelling. Relation of these terms is shown in Fig. 2. According to Berdica [2] reducing vulnerability can result in reducing risk of various events, which can enhance serviceability of the TN.

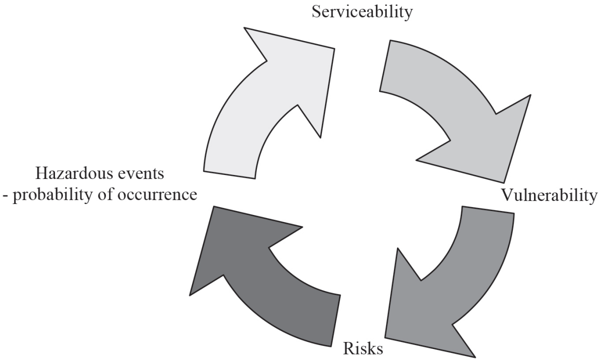


Fig. 2 Vulnerability of transportation network in wheel of concepts (by Berdica)

There are several possible strategies for the identifying threats and perceived risk that can lead to vulnerability reduction. One option is to make the transportation infrastructure more resilient. It can be achieved, for instance, by raising it above expected maximum flood levels. Another strategy would be to introduce additional links to the network – in such a way that the resulting TN would become more robust. Normally, such links may be redundant but in the cases of emergency provide alternative routes for traffic. These examples of strategies could make the TN more resilient (less vulnerable) in the context of specific risks and threats. But before one decides to adopt appropriate measures he or she needs to understand vulnerability. In this work we propose an outline of a simple methodology to quantify vulnerability by means for IDs.

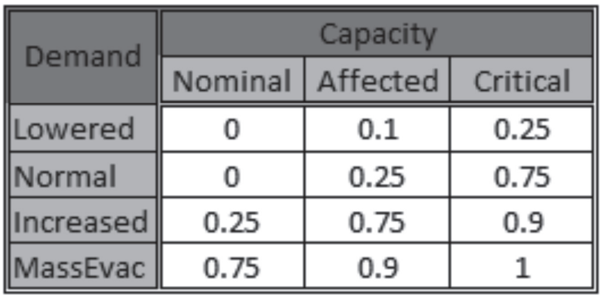
Modelling Vulnerability using Influence Diagrams

In this work we are concerned with defining a vulnerability index (VI) for a single element of the transportation network – either a link or a node. Earlier we argued that in practical context this would be done only for a part of whole transportation network, specifically the critical part of the infrastructure. The purpose is to produce a numeric measure that would quantify the notion of vulnerability.

The influence diagram [12] is a probabilistic decision model that is a more compact representation of a decision problem than decision tree. Unlike the probability or decision trees, the ID does not explicitly specify every single path through the problem; instead, it captures dependencies between variables in the modelled domain. This property allows for more compact and efficient (especially in terms of knowledge elicitation) representation of the problem, implying that it is suitable for larger scale decision problems. There are three types of variables in ID: (1) *chance nodes* that capture unknown events and relevant probabilities including probabilistic dependencies (by means of conditional probabilities), (2) *utility nodes* that encode utilities (which can be costs, profits, etc.) that define user's preferences over the set of outcomes, and (3) *decision nodes* that define elements of the domain over which the decision maker has complete control.

To model vulnerability we propose to define a measure of vulnerability which we further call *vulnerability* index (VI). In order to define VI we propose a structured approach based on IDs: in the first step we would ask subject matter experts (SMEs) familiar with given TN to produce a list of possible threats to a particular network element. The SMEs are expected to be practicing mid-level managers from institutions that are involved in TN maintenance and should be familiar with the concept of risk assessment. The elicitation process can be done using specialized computer-based elicitation tool, where the SMEs would identify relevant threats from a pre-defined list of possible threats. For each of the relevant threats, the SME would need to specify if the threat has a potential to affect the capacity of the network element (i.e. to block, damage or destroy road surface) and provide corresponding probabilities which are expected to be subjective or in less likely scenario based on risk assessment studies). Next, the SME would need to define if the threat has potential to result in decreased or increased traffic, or to cause a mass evacuation – in other words, if it can affect demand on the network element, and again provide corresponding probabilities.

We assume a fixed three-layer network structure of an ID. In the top layer nodes that correspond to threats are placed. They are assumed to be binary (threat can be *present* or *absent*) and quantified by asking the SME to provide probability of the threat occurring – we propose to use two scales, depending on frequency: for likely threats such as traffic incidents, snow storms, floods, etc. we propose to use the average number of days per year. For less likely threats, such as hazardous chemical releases, terrorist attacks, etc., the qualitative scale would be used such as *unlikely, highly unlikely, and extremely unlikely*. These would be translated into specific probabilities. We argue that as long as the scale is used consistently for all threats (and all network nodes) the actual values of probabilities do not matter that much, as the VI is intended to rank different elements of the transportation network relatively to each other rather than to provide interpretation of particular values of VI. The middle layer of the network always includes two nodes: *Demand* and *Capacity*. They are intended to model two factors: each threat can produce demand on network (cause people to use transportation network) and/or affect the capacity of the TN. The states of the nodes would be: *Lowered*, *Normal*, *Increased*, *Mass Evacuation* for the *Demand* node and *Nominal*, *Decreased,* and *Critical* for the *Capacity* node. In the lowest layer a single utility node would be placed that would combine the effects of *Demand* and *Capacity*. An example of definition for the *Vulnerability* node is shown in Fig. 3. A simple example of the ID model is shown in Fig. 4.



Demand	Capacity		
	Nominal	Affected	Critical
Lowered	0	0.1	0.25
Normal	0	0.25	0.75
Increased	0.25	0.75	0.9
MassEvac	0.75	0.9	1

Fig. 3 An example of definition for the Vulnerability node

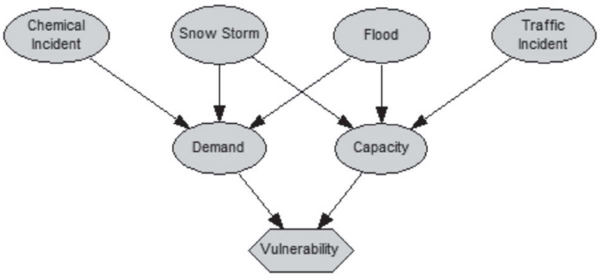


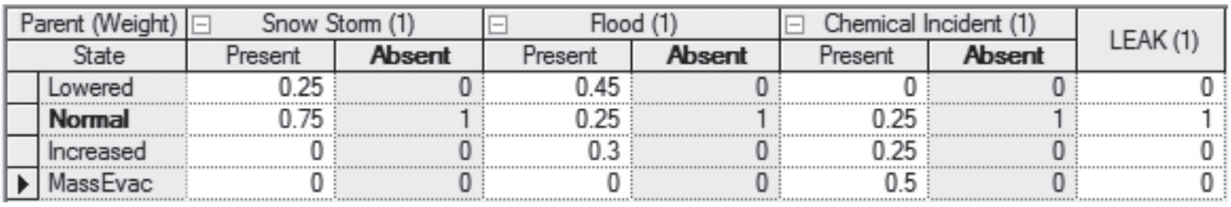
Fig. 4 A simple example of the ID model

For the sake of example, we assumed only 4 threats: *Traffic Incident*, *Snow Storm*, *Flood*, and *Chemical Release*, with the corresponding probabilities of occurrence: 0.01, 0.005, 0.0002, 10^{-6}. In order to understand the working of the approach we analyze the HAZMAT scenario. The HAZMAT scenario would be denoted in the model as *Chemical Release* and it would produce demand on network – it is because a HAZMAT incident is likely to be followed by some form of evacuation and resulting with people forced to leave the threatened area and incur heavy load on the network. On the other hand, *Chemical Release* has no direct impact on capacity of the TN, as we assume that the infrastructure is able to withstand the HAZMAT incident effects with no noticeable effects. A *Traffic Incident* does not directly produce demand on the system, but it has a potential to affect capacity of network element (i.e. to totally block traffic). In the cases when the threats such as *Snow Storm* or *Flood* are occurring they can produce demand on network and affect the capacity of TN because there is a chance that a mass evacuation could be required and also some transportation links could be impossible to use or damaged.

One of particular limitations of IDs is the number of numerical probabilities required to quantify a model. In particular nodes with large numbers of incoming links (often referred and nodes with a large number of parent nodes) should be quantified with a number of probability distributions that is exponential in the number of parent nodes in the graphical part. This implies that if there are 10 incoming links to a node and assuming that all variables are binary (have two states), an SME would be required to provide $2^{10} = 1024$ probability distributions, which would be unrealistic in practice.

In order to reduce the number of parameters required to specify the ID model, we decided to use the noisy-average model [13] for local probability distributions that is available in GeNIe software. The noisy-average model shown in Fig. 5 is suitable for the modelled interactions between variables where there are following conditions required: (1) both the parent variables have a state that describes the 'normal' state of the world (no snowstorm, no flood, etc.), (2) the child variable has as well the 'normal' state (corresponding to typical traffic patterns or the level of traffic flow for which the road was designed), (3) for the child variable the deviation from the 'normal' state can be in both increased and decreased values, and (4) the way the influences are combined is achieved by averaging (hence the name of the model), which means that no single parent variable is assumed to have stronger influence on the state of the child variable than the other parent variables. We believe the noisy-average model is suitable for the task we want to achieve with creating the VI index. Finally, the application of the noisy-average allows to substantially reduce the elicitation task on the SME – it allows reducing the number of parameters required to quantify the model from exponential to linear in the number of parent nodes.

The defined VI ranges from 0 to 1, with increasing values indicating increasing vulnerability. Its values have no strict interpretation, but if the model definition and elicitation process are used consistently for all the network elements, the values for different network elements can be interpreted in the context of all VIs produced from the network. This approach allows for identifying vulnerability areas. There is additional benefit resulting from using IDs – this approach allows for dynamic calculation of VI, under assumption that some of the events are observed (we say that some nodes are instantiated in ID) – for example, if there is snow storm in some area, the model can result with increased VI for some nodes, allowing for implementing tools that would provide situational awareness based on the proposed VI.



Parent (Weight)	⊟ Snow Storm (1)		⊟ Flood (1)		⊟ Chemical Incident (1)		LEAK (1)
State	Present	**Absent**	Present	**Absent**	Present	**Absent**	
Lowered	0.25	0	0.45	0	0	0	0
Normal	0.75	1	0.25	1	0.25	1	1
Increased	0	0	0.3	0	0.25	0	0
▶ MassEvac	0	0	0	0	0.5	0	0

Fig. 5 An example of model definition for the node Demand using the noisy-averege model

4. Conclusions

The concept of vulnerability in the context of TN is a subject of active interest from both practitioners' and academic communities. In particular, the understanding of distribution of vulnerabilities in the TN may help to identify critical components of transportation infrastructure. As discussed, the proposed methodology is intended to be applied to this critical infrastructure element, rather than to the TN as whole. This is dictated by practical considerations – to define models is necessary knowledge of experts on which should be placed the limited burden of elicitation.

In this paper we proposed a method for the assessment of TN's vulnerability using the concepts of "demand" and "capacity" that are consequently combined to produce a numeric vulnerability index. We provided a simple example to illustrate the proposed approach and to demonstrate the way how to model TN's vulnerability using IDs. We presented how the noisy-average model is used to take advantage of independence of causal influences in order to reduce the knowledge elicitation effort and to make the proposed method more practical. Our approach to vulnerability modelling does not take into consideration socio-economic impacts of TN's link failure – it is focused on capturing TN's sensitivity to combination of the specific adverse events directly related to transportation functions.

We believe that the contribution of the paper is two-fold: (1) we proposed to develop a method of vulnerability assessment based on a decision-theoretic framework of IDs, which allows for exploiting well established body of experience with creating this type of models in a new application, (2) we proposed use of the noisy-average model for local probability distributions as a tool to improve and streamline knowledge elicitation processes.

Determining actual TN's vulnerability is important to identify weak links in the network. It can be used to identify and implement appropriate risk reduction strategies for the identified threats. If once can develop a useful way to quantify vulnerability it can potentially be used to improve TN safety. It can be useful not only in the crisis management context, but as well in planning and as a tool to inform future developments and expansion.

We want to emphasise that the proposed approach is at an early stage of development and that this paper only outlines the proposed approach. Further work is needed to validate the approach on an actual example of transportation network, and this is our intention to do so.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-0471-10.

References

[1] ZANICKA-HOLLA, K., RISTVEJ, J., SIMAK, L.: *Systematic Method of Risk Assessment in Industrial Processes*, Risk analysis VII: simulation and hazard mitigation - Southampton : WIT Press, 2010. ISBN 9781845644747 - WIT transaction on information and communication technologies; v. 43. ISSN 1746-4463. DOI: 10.2495/RISK100111

[2] BERDICA, K.: An Introduction to Road Vulnerability: What has been Done, is Done and should be Done. *Transport Policy*, vol. 9, No. 2, 2002, pp. 117-127.

[3] JONSSON, H., JOHANSSON, J., JOHANSSON, H.: Identifying Critical Components in Technical Infrastructure Networks. Proc. of the Institution of Mechanical Engineers, Part O: *J. of Risk and Reliability*. vol. 222, No. 2, 2008. pp. 235-243.

[4] DILLEY, M., BOUDREAU, T. E.: *Coming to Terms with Vulnerability: A Critique of the Food Security Definition*. Food Policy, 2001, 26, pp. 229-247.

[5] WISNER, B., BLAIKIE, P., CANNON, T., DAVIS, I.: *At Risk: Natural Hazards, People's Vulnerability and Disasters.* 2nd ed. Routledge, London, 2004.

[6] TAYLOR, M. A. P., D'ESTE, G. M.: *Concepts of Network Vulnerability and Applications to the Identification of Critical Elements of Transport Infrastructure.* 26th Australasian Transport Research Forum Wellington New Zeland, 2003.

[7] YANG, L., QIAN, D.: Vulnerability Analysis of Road Networks. *J. of Transportation Systems Engineering and Information Technology*, vol. 12, No. 1, 2012, pp. 105-110.

[8] JENELIUS, E., PETEMEN, T., MATTSSON, L. G.: Importance and Exposure in Road Network Vulnerability Analysis. *Transportation Research Part A: Policy and Practice*, vol. 40, No.7, 2006, pp. 537-560.

[9] HUSDAL, J.: *Reliability and Vulnerability Versus Cost and Benefits*. The 2nd Intern. Symposium on Transportation Network Reliability. Queenstown and Christchurch, New Zealand, 2004, pp. 180-186.

[10] SLIVONE, M.: Several Approaches to Identification of Critical Links in Transport Network. *Perner's Contacts*, vol. 3, No. 5, 2008, pp. 261-275.

[11] BRATHEN, S., LAEGRAN, S.: *Bottlenecks in Cargo Transport in Norway.* Molde Research Institute/SWECO Groner, Norway, 2004.

[12] HOWARD, R. A., MATHESON, J. E.: *Influence Diagrams.* Howard and Matheson (eds.) The Principles and Applications of Decision Analysis, vol. II., Strategic Decisions Group, Menlo Park, CA pp. 721-762.

[13] ZAGORECKI, A. DRUZDZEL, M. *The Noisy-average Model for Local Probability Distributions*. Technical report, Decision Systems Laboratory, University of Pittsburgh.