Computers, Environment and Urban Systems 49 (2015) 136–147

Contents lists available at ScienceDirect

Computers, Environment and Urban Systems

journal homepage: www.elsevier.com/locate/compenvurbsys

Road network vulnerability analysis: Conceptualization, implementation and application

Erik Jenelius *, Lars-Göran Mattsson

KTH Royal Institute of Technology, Department of Transport Science, Teknikringen 72, SE-100 44 Stockholm, Sweden

ARTICLE INFO

Article history:
Available online 1 March 2014

Keywords:
Vulnerability
Robustness
Road network
Transport
Disruption
GIS

ABSTRACT

The paper describes a process for road network vulnerability analysis, from (i) the conceptual definition of vulnerability measures, through (ii) the derivation of practical indicators and models adapted to available data and their implementation in computational procedures, to (iii) the application of the methodology in case studies. In the first step, the vulnerability concept is defined and quantified formally, and distinct user and technological perspectives are highlighted. In the second step, the conceptual measures are adapted and calculated according to the conditions, requirements and goals of a particular analysis. The paper describes practical indicators and algorithms developed for large-scale vulnerability analyses. For the third step, the paper analyzes both single link closures and area-covering disruptions and the distribution of impacts among different regions in a case study on the Swedish road transport system. The spatial patterns are put in connection with the regional variations in location and travel patterns and network density. Finally, the implications for policy and possible approaches to vulnerability management are discussed.

1. Introduction

Modern society relies upon the collection of systems and institutions known as the infrastructure to support the welfare and living standard of people. A downside of this dependency is that sudden failures and disruptions in the systems may cause severe strains on the society. Road network disruptions can threaten the possibility for people to receive medical care and other critical services. More generally, they impair people's accessibility to daily activities such as commuting to work and doing the shopping. Furthermore, there may be large costs associated with remedies and restoration of the transport system to a fully operational state. It is thus of interest to study the magnitude and distribution of impacts due to disruptions in different parts of the network, so that resources for prevention, mitigation and restoration can be suitably allocated.

Disruptions can be caused by a wide range of events, some of which originate within the transport system, including traffic accidents and technical failures. Other events are external strains imposed on the system, often caused by nature, as with floods, landslides, heavy snowfall, storms, wildfires, earthquakes, etc. While accidents and technical failures may have limited extents, disruptions caused by nature may cover large areas in the road network.

Road network vulnerability analysis can be defined as the study of potential degradations of the road transport system and their impacts on society, modeling the road infrastructure as a network with links (road segments) and nodes (intersections). Research interest in the topic grew in the early 2000s as part of a broader focus on critical infrastructure protection. Several recent natural disasters and terrorist attacks raised awareness that society is vulnerable to disruptions in these infrastructure systems. It was recognized by some researchers that new quantitative methods for assessing the consequences of severe, albeit seemingly unlikely, disruptions of the road transport system were needed (Berdica, 2002; D'Este & Taylor, 2003).

The subsequent vulnerability research has embraced a rich exploration of perspectives, metrics and methods. A number of papers have proposed frameworks or metrics for evaluating road network vulnerability (Chen, Yang, Kongsomsaksakul, & Lee, 2007; Jenelius, Petersen, & Mattsson, 2006; Qiang & Nagurney, 2008; Sullivan, Novak, Aultman-Hall, & Scott, 2010; Taylor & Susilawati, 2012). Other studies focus on the modeling and computational aspects of the analysis (Erath, Birdsall, Axhausen, & Hajdin, 2009; Knoop, van Zuylen, & Hoogendoorn, 2008; Luathep, Sumalee, Ho, & Kurauchi, 2011). A third line of research develops mathematical

* Corresponding author. Tel.: +46 8 790 8032; fax: +46 8 212 899.
E-mail addresses: erik.jenelius@abe.kth.se (E. Jenelius), lars-goran.mattsson@abe.kth.se (L.-G. Mattsson).

http://dx.doi.org/10.1016/j.compenvurbsys.2014.02.003
0198-9715/

modeling and optimization techniques to identify worst-case scenarios and the impacts of intentional attacks, or best responses to such scenarios (Bell, Kanturska, Schmöcker, & Fonzone, 2008; Duan & Lu, 2013; Matisziw & Murray, 2009). Finally, many papers put most emphasis on the vulnerability evaluation itself (Bono & Gutiérrez, 2011; Dalziell & Nicholson, 2001; Tatano & Tsuchiya, 2008).

As the literature becomes more diverse and specialized, there is a growing need also for synthesis of various proposed methodologies into integrated analysis frameworks. The aim of this paper is thus to describe a process for large-scale road network vulnerability analysis: from (i) the conceptual definition of vulnerability measures, through (ii) the derivation of practical indicators and models adapted to available data and their implementation in computational procedures, to (iii) the application of the methodology in case studies. The intention is that such a comprehensive description will help researchers to identify parts of the process where additions and improvements can be made, and to see how contributions in one area can be connected to work in other parts of the process.

The task in the first step of the process is to formally define and quantify the concept of vulnerability, and to highlight different perspectives from which vulnerability can be viewed. This paper proposes that road network vulnerability is the societal risk of road infrastructure disruptions. The impacts of disruption scenarios for individuals are evaluated in economic terms. Two perspectives of vulnerability are distinguished: the first perspective focuses on the users and considers how different user groups are affected under various disruption scenarios. The second perspective focuses on the road network and considers how disruptions of different network elements affect the users and society overall.

In the second step, the conceptual measures are adapted and calculated according to the data, computational requirements and desired output of a particular analysis. This paper describes the derivation of one such set of practical indicators developed for large-scale vulnerability analyses using data from a travel demand forecasting model. A GIS-based approach and algorithms for computing the vulnerability indices for very large networks are presented.

In the third step the implemented measures are applied to generate useful information about the specific study area, or to draw more general conclusions regarding the factors contributing to vulnerability. This paper expands upon a series of studies of the Swedish road transport system (Jenelius, 2009, 2010; Jenelius & Mattsson, 2012). Both single link closures and area-covering disruptions are considered and the distribution of impacts among users in different regions is investigated. The spatial patterns that are found are explained in terms of the properties of the vulnerability metrics and models, and are put in connection with the regional variations in location and travel patterns and network density.

The remainder of the paper is organized as follows. A conceptual framework for vulnerability analysis is proposed in Section 2. The implementation of practical vulnerability indicators and computational methods and algorithms are described in Section 3. Section 4 presents results from large-scale applications of the vulnerability indicators to the Swedish road network. Section 5 concludes the paper.

2. Conceptualization: Perspectives and formal vulnerability measures

Transport system vulnerability is here seen as society's risk of transport system disruptions and degradations. Road network vulnerability analysis, in particular, focuses on the road transport system and models the physical infrastructure as a network of links (road segments) and nodes (intersections). The notion of risk is adopted from Kaplan and Garrick (1981), who propose that the results of a risk analysis can be represented as a list of "triplets", each consisting of a description of a particular scenario, the probability of that scenario occurring, and the impact of the scenario. The risk is then the set of all triplets. This definition of vulnerability is more general than the simplified notion that risk is the *product* of probability and consequence. Thus, a vulnerability analysis may well put particular focus on rare, extreme events. Furthermore, the focus is on the users of the road network, that is, people, businesses and services, rather than the network itself.

Consider a road network disruption scenario space Ω. Each dimension of Ω represents a relevant aspect of a network disruption, such as the element involved (the set of network links and nodes), the duration, the time of occurrence, and the levels of capacity reductions. With each scenario $\sigma \in \Omega$ is further associated a "null" scenario $\sigma_0(\sigma) \in \Omega$ that represents the baseline, normal level of operations during the time of the disruption had it not occurred, and against which the impact of the disruption is assessed.

Vulnerability analysis involves comparing and aggregating the various aspects of the disruption impacts for different users under different scenarios. The impacts must therefore be expressed in units such that interpersonal comparisons and aggregations are meaningful. For cost-benefit analyses of vulnerability-reducing investments, it is desirable to express the disruption impacts in economic terms. This allows prevention, repair and restoration costs to be added and compared to the disruption impacts, such as delayed goods deliveries and reduced accessibility to societal services.

With these aims it is reasonable to adopt a *micro-economic* approach and view users (i.e., individuals, businesses, etc.) as economic agents interacting with each other and the infrastructure. The individual is thus seen as a consumer of goods, activities, services and travel. Network disruptions often lead to increased travel times for travelers. An increase in travel time means that an individual may lose income, may have to sacrifice time from other activities, and may get reduced accessibility to societal services. The micro-economic framework postulates that individuals make decisions in order to maximize their obtained utility, while businesses or firms seek to maximize their profits, under the prevailing circumstances. The *compensating variation*, or CV for short, represents the smallest amount that the individual should be willing to accept as compensation for the disruption (or in the case of an improvement, the largest amount that the user should be willing to pay for it) (Mas-Colell, Whinston, & Green, 1995). The compensating variation is used here as a formal measure of the impact of a disruption for individuals. For individual n and disruption scenario σ this quantity is denoted $\Delta C_n(\sigma)$. The framework is illustrated in Fig. 1.

2.1. Vulnerability and exposure

Vulnerability may be viewed from two different perspectives. The first perspective is to focus on the *societal* side of the system. For a particular individual one may ask: Under various conceivable disruption scenarios, how would the individual be affected, and what is the probability of each scenario occurring? One may also ask: What would be the impacts of the worst-case plausible scenario, and what are the long-run expected impacts of system disruptions?

Following Jenelius et al. (2006), the impact for a single user under a certain disruption scenario is referred to as the *exposure* of the user to that scenario (Taylor and Susilawati (2012) use the term "vulnerability" for essentially the same concept as exposure). Combining the exposure with the probability of the scenario gives