ARTICLE IN PRESS

Transportation Research Part C xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Transportation Research Part C

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

An optimization approach for deriving upper and lower bounds of transportation network vulnerability under simultaneous disruptions of multiple links ☆

Xiangdong Xu [a], Anthony Chen [b,a,*], Chao Yang [a]

[a] Key Laboratory of Road and Traffic Engineering of the Ministry of Education, Tongji University, Shanghai, China
[b] Department of Civil and Environmental Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 16 August 2017
Received in revised form 18 August 2017
Accepted 19 August 2017
Available online xxxx

Keywords:
Network vulnerability
Vulnerability envelope
Upper and lower bounds

ABSTRACT

This paper aims to develop an optimization approach for deriving the upper and lower bounds of transportation network vulnerability under simultaneous disruptions of multiple links without the need to evaluate all possible combinations as in the enumerative approach. Mathematically, we formulate the upper and lower bounds of network vulnerability as a binary integer bi-level program (BLP). The upper-level subprogram maximizes or minimizes the remaining network throughput under a given number of disrupted links, which corresponds to the upper and lower vulnerability bounds. The lower-level subprogram checks the connectivity of each origin-destination (O-D) pair under a network disruption scenario without path enumeration. Two alternative modeling approaches are provided for the lower-level subprogram: the virtual link capacity-based maximum flow problem formulation and the virtual link cost-based shortest path problem formulation. Computationally, the BLP model can be equivalently reformulated as a single-level mixed integer linear program by making use of the optimality conditions of the lower-level subprograms and linearization techniques for the complementarity conditions and bilinear terms. Numerical examples are also provided to systematically demonstrate the validity, capability, and flexibility of the proposed optimization model. The vulnerability envelope constructed by the upper and lower bounds is able to effectively consider all possible combinations without the need to perform a full network scan, thus avoiding the combinatorial complexity of enumerating multi-disruption scenarios. Using the vulnerability envelope as a network performance assessment tool, planners and managers can more cost-effectively plan for system protection against disruptions, and prioritize system improvements to minimize disruption risks with limited resources.

1. Introduction

Vulnerability is the susceptibility of a system to threats and incidents that results in operational degradation. The core of transportation network vulnerability analysis is to identify the critical/vulnerable/important components (e.g., links and nodes), whose disruptions could have a significant impact on travelers' behaviors and network performance. This topic

☆ This article belongs to the Virtual Special Issue on "ISTTT22".

* Corresponding author at: Department of Civil and Environmental Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong.
E-mail addresses: xiangdongxu@tongji.edu.cn (X. Xu), anthony.chen@polyu.edu.hk (A. Chen), tongjiyc@tongji.edu.cn (C. Yang).

http://dx.doi.org/10.1016/j.trc.2017.08.015
0968-090X/

has received a great deal of attention in the past decade (see, e.g., Berdica, 2002; Chen et al., 2007a,c; Murray and Grubesic, 2007; Nagurney and Qiang, 2010; Chen et al., 2012; Ho et al., 2013; Zhao et al., 2013; Jenelius and Mattsson, 2015; Bell et al., 2017). Identification of critical components in a network has many potential applications in both the pre-disaster planning and post-disaster management (e.g., targeted protection or retrofitting, strategic location of rapid response and repair stations to facilitate the network recovery and mitigation, evacuation routes planning, and evacuation network monitoring) to ensure that the critical components are adequately monitored (Murray-Tuite and Wolshon, 2013; He et al., 2015; Wang et al., 2016b).

In the literature, the majority of existing methodologies for transportation network vulnerability analysis belong to the *disruption scenario enumeration approach* (via enumeration without or with pre-scanning, or random simulation schemes). At each enumerated scenario, *one link/node is removed or degraded at a time*, and the impact of each individual link/nodal removal or degradation is evaluated and ranked according to different indictors. Interested readers are directed to a comprehensive review by Mattsson and Jenelius (2015) on the evaluation methods and indictors. With the increase of the number of enumerated scenarios, this type of approach is able to consider a range of potential disruption scenarios. However, the *enumeration* approach has a combinatorial complexity especially when considering the simultaneous disruption of multiple links/nodes at the same time. Let m and n denote the total number of links and the number of simultaneously disrupted links, respectively. Then, the number of potential scenarios with n disrupted links is C_n^m. One can envision the computational burden when applying it to large-scale networks with simultaneous disruptions. Although many well connected networks could be resilient enough to a single-link (or node) failure, **simultaneous disruptions** can be very problematic, resulting in disruption propagations and widespread disruptions. On the other hand, the *simulation* scheme may miss some important scenarios (e.g., the best or the worst case) due to the limited number of samples. Also, it may miss some hidden/phantom vulnerability scenarios (see, e.g., Jenelius, 2010) that are not apparent to analysts due to the large scale and complex network structure. These issues render an incomplete understanding of all potential disruption scenarios and their associated impacts. Recently, Wang et al. (2016a) recognized the combinatorial complexity of considering multiple disruptions, and provided a global optimization approach to identifying critical links for multiple disruptions, without the need to perform a complete network scan. However, only the worst case situation was considered, which may not provide a useable or cost-effective strategy for managing/protecting the identified critical links.

On a different line of research, the *game theoretic approach* has been developed to assess the transportation network vulnerability, such as Bell (2000) of considering a two-player zero-sum non-cooperative game, Bell and Cassir (2002) of considering a multiplayer game, and Szeto et al. (2007) of considering multiple network-specific demons. In this approach, the evil entity or demon seeks to maximize the total network cost by damaging links in the network, while network users seek a route to minimize their travel costs. The critical links in the network are likely to be destroyed by the demon as a consequence of the game. Since the demon is allowed to destroy any link in the network, the game theoretic approach also only considers the worst-case scenario, and therefore provides a pessimistic evaluation of network performance.

In addition, *sensitivity and uncertainty analyses* have also been used to identify critical links that affect the system performance the most (e.g., Nicholson and Du, 1997; Chen et al., 2002; Luathep et al., 2011; Yang et al., 2013). A weak link with higher capacity variability may not necessarily be a critical link. Instead, a critical link must be one that is both important (i.e., substantial impact on system performance) and weak (i.e., large capacity variability). The critical links should be the prime candidates for strengthening, rather than those that are merely weak. The critical index of a link indicates the proportion of the overall uncertainty of performance measure contributed by the uncertainty of its link capacity. This approach is able to consider simultaneous link degradations. However, since sensitivity analysis is only valid locally for minor perturbations of inputs and parameters, this approach may not be applicable to large perturbations in some disruption scenarios.

When considering multiple simultaneous disruptions (e.g., n links disrupted), there may have a large number of possible scenarios corresponding to different location combinations, and each scenario has an *unknown* occurrence possibility. Hence, a way to avoid the unknown occurrence possibility of disruption scenarios is to consider the *range* of all potential disruption scenarios and their associated impacts. To the best of our knowledge, there is no analytical approach of transportation network vulnerability with a systematic consideration and quantification of all possible simultaneous disruptions. This study attempts to develop an optimization approach for deriving the upper and lower bounds of transportation network vulnerability – a vulnerability envelope, while circumventing the need of enumerating all possible disruption scenarios. This is different from the conservative (or pessimistic) consideration of the worst-case scenario in Wang et al. (2016a) or the *game theoretic approach* in Bell (2000), Bell and Cassir (2002), and Szeto et al. (2007). The upper and lower bounds provide the most optimistic and pessimistic quantification of network vulnerability range (i.e., the least to the most disruptive cases). The single consideration of either the least or the most disruptive cases may lead to biased (overestimated or underestimated) network performance assessment. Instead, with the vulnerability envelope, network planners and managers can more cost-effectively plan for system protection against disruptions, and prioritize system improvements to minimize disruption risks with limited resources. Particularly, those links appeared in both the upper-bound and lower-bound scenarios deserve more resources and actions to protect in the pre-disaster network planning stage. A large range between the upper and lower bounds indicates that the network is more susceptible or less resilient against disruptions, and a substantial percentage of trips can be affected by these different combinations of multiple simultaneous disruptions. On the other hand, a small range could mean that the network is very vulnerable as it could be easily disconnected (i.e., both upper and lower bounds are quite small and similar), or it is not vulnerable at all as it could be highly connected (i.e., both bounds are quite large and similar).

Please cite this article in press as: Xu, X., et al. An optimization approach for deriving upper and lower bounds of transportation network vulnerability under simultaneous disruptions of multiple links. Transport. Res. Part C (2017), http://dx.doi.org/10.1016/j.trc.2017.08.015