Physica A 515 (2019) 288–298

Contents lists available at ScienceDirect

Physica A

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

# Detecting critical links of urban networks using cluster detection methods

Meisam Akbarzadeh [a,*], Sayed Farzin Salehi Reihani [a], Keivan Aghababaei Samani [b]

[a] Department of Transportation Eng., Isfahan University of Technology, Isfahan, 8115683111, Iran
[b] Department of Physics, Isfahan University of Technology, Isfahan, Iran

## HIGHLIGHTS

- We show that links connecting neighboring clusters of an urban road network are the most critical links of the network.
- We defined a link as critical if its failure significantly diminishes the integrity or functionality of the network.
- We measured the integrity by the size of the giant component and the functionality of the network is measured by the temporal network efficiency.
- Second most important metric is found to be betweenness of links. Flow, and congestion are third and fourth, respectively.
- Infomap was found to be the most suitable cluster detection method for the urban network under study.

## ARTICLE INFO

*Article history:*
Received 21 May 2018
Available online xxxx

*Keywords:*
Criticality
Infomap
Functionality
Integrity
Urban road networks

## ABSTRACT

Clusters of a network are sets of nodes that are strongly connected to each other but weakly connected to the rest of the network. A network link is considered critical if loss of it significantly diminishes the integrity or functionality of the network. Therefore, networks are most vulnerable to losing their critical links. Integrity of the network is measured by the relative size of the giant component. The functionality of the network is measured by the temporal network efficiency. Temporal network efficiency is the sum of reciprocal of the time it takes to traverse between node pairs of the network and is more suitable in transportation networks than the well-known network efficiency which is based on the distance. It is shown in this paper that links connecting neighboring clusters are the most critical links of the network in comparison to links with highest congestion, flows, or betweennesses. Second most important metric is found to be betweenness of links. Flow, and congestion (ratio of link flow and its capacity) are third and fourth, respectively. It was also found that the links located on the borders of communities are not those with highest values of flows, congestion, or betweenness. Infomap was found to be the most suitable cluster detection method for the urban network under study.



## 1. Introduction

Modern societies are highly dependent on power, transportation, water, sewage, and data networks. Near-capacity performance, intricate relations between different infrastructures and complexities within each system have led to the increase of the sensitivity of these systems [1].

* Corresponding author.
*E-mail address:* makbarzadeh@cc.iut.ac.ir (M. Akbarzadeh).

https://doi.org/10.1016/j.physa.2018.09.170
0378-4371/

Transportation networks consist of road, rail, naval and air networks. In many countries, road networks are more important than the others due to their wider coverage and higher accessibility. In addition to the economic role of road networks, they can be used as the principal infrastructure for evacuation and rescue during tentative crisis. Therefore, guarantying the road network performance under different possible conditions is of utmost importance. A network link is considered critical if loss of it significantly diminishes the integrity or functionality of the network. Thus, networks are most vulnerable to losing their critical links.

Vulnerability of systems has been defined in various ways. In a pioneer paper, Berdica [2] defined the vulnerability of a transportation system based upon how its performance would be influenced by possible incidents. D'Este and Taylor [3] put their focus on network's accessibility, and defined vulnerability as a significant reduction in the accessibility of roads. These two definitions are used as base definitions of vulnerability. Mattsson and Jenelius [1] defined vulnerability as the risk of disruptions in a transportation network and its surrounding areas. A notable point in these definitions is that, unlike the risk analysis, the probability of incidents is not explicitly considered. Therefore, rare incidents with high destructive effects are very well addressed.

Two main approaches employed for analyzing the vulnerability of networks include the topological approach and the system-based approach [4]. The first approach focuses on the structure and configuration of a network and therefore graph theory and complex network concepts play a vital role in it. Network disruptions are modeled by modifying the links and nodes of the graph (link and node removal/addition) and network metrics e.g. clustering coefficient, average path length, and relative size of the giant component are updated accordingly. System-based approach focuses on the interaction of the demand and supply and adopts the famous four-step (trip generation, distribution, mode choice, and route choice) procedure. Besides network elements, disruptions and crisis would modify the origin–destination (OD) matrix. This is because under critical situation, the travel patterns are different from ordinary days and also highly scenario-dependent.

Studies adopting the topological approach have come up with several indices for explaining the integrity of the network and identifying the critical links of a network. These indices include the relative size of the giant component [5–7], network efficiency measure [8], and the largest eigenvalue [9]. On the other hand, studies adopting the system-based approach have come up with a variety of indices for explaining the functioning of the network and identifying the critical links of a network. These indices include but are not limited to the change in generalized cost measure [10], importance measure [11], Network Robustness Index [12], and network vulnerability index [13]. Knoop et al. [14] analyzed nine link-based indicators developed by Tampère et al. [15], Li [16], and Tamminga et al. [17]. These indices were based upon concepts including traffic queue rate, blocking, and the spillback. Knoop et al. [14] compared the vulnerability of links of a network based on each criterion. They concluded that results were not well correlated i.e. each criterion yielded different set of vulnerable links. A linear model combining the criteria could not predict the right vulnerability of links. Therefore, link-based indicators were suitable to for indicating the vulnerability of the traffic flow on each specific link but insufficient to capture all network effects. El-Rashidy and Grant-Muller [18] developed a technique based on fuzzy logic and exhaustive search optimization to combine six vulnerability attributes with different weights into a single vulnerability index for network links.

Recently, Bell et al. [19] investigated network vulnerable links using capacity weighted spectral analysis. They identified the network cut with least capacity which would take into account the relative sizes of the sub-networks on both sides of the cut.

This paper aims to test the hypothesis that the borders of the clusters of a network are the most critical links.

### *1.1. Cluster: definition and detection methods*

Cluster (also known as community or module) is a set of nodes which have relatively strong connections within themselves, but weak connections with the other parts of the network [20]. Fig. 1 illustrates an example of a network (on the left) and its clusters colored and encircled (on right). The example network consists of three clusters which are colored blue, orange, and green. Connections in border regions between clusters are not as strong as connections within a cluster. Weakness of these connections means that separation of the network into two distinct subsections is easier by cutting the borders of the clusters. Therefore, networks are vulnerable in these areas. If links' throughput becomes disrupted for some reasons, alternative routes are relatively hard to find and connections between clusters will reduce.

Several approaches for detecting clusters of a network are proposed in the literature such as partitioning, hierarchical, spectral, and kernel-based [9]. Spectral analysis examines networks' cluster structure by considering eigenvalues of the Laplacian and adjacency matrix. Modularity methods define a modularity function, and optimize it with regards to every possible cluster of network's nodes [21]. Techniques based on information theory cluster nodes in a way that every node can be named with minimum data bits [22].

Yang et al. [23] tested eight commonly used cluster detection algorithms including Infomap (IM), Label Propagation (LP), Multilevel (ML), Walktrap (WT), Spinglass (SP), and Edge Betweenness (EB) on Lancichinetti–Fortunato–Radicchi benchmark to examine them in terms of accuracy and computing time. They concluded that the most suitable method of clustering could be determined according to the network size and its structure. Number of nodes represents the network size and a mixing parameter ($\mu$) quantified the network structure as shown in Eq. (1).

$$\mu = \frac{\sum_i K_i^{ext}}{\sum_i K_i^{tot}} \tag{1}$$