ANALYZING VULNERABILITIES OF THE GERMAN HIGH-SPEED TRAIN NETWORK USING QUANTITATIVE GRAPH THEORY

ZHONGLIN WANG, MARTIN ZSIFKOVITS & STEFAN W. PICKL
Institute for Theoretical Computer Science, Mathematics and Operations Research,
Universität der Bundeswehr München, Germany.

ABSTRACT

The German high-speed train system (ICE) as one of the critical infrastructures is mapped into a distance-weighted undirected network. The aim of the analysis is to make full use of quantitative graph theory in order to analyze the vulnerabilities of the network and to detect the centers and hubs of the system. When conducting network analysis of railways, there is a tradition of such an analysis that the betweenness centrality measure and the efficiency measure would be applied; however, based on these two measures, we offer a new promising one that we call betweenness-efficiency vulnerability measure, which can be used to detect the most vulnerable nodes on an aggregated level. By analyzing and comparing the results of these three measures, highly vulnerable stations are identified, which therefore have more potential to harm the overall system in case of disruption. This can help decision-makers to understand the structure, behavior and vulnerabilities of the network more directly from the point of view of quantitative graph theory. Finally, the problem of adapting a new vulnerability measure to this kind of system is discussed.

Keywords: Betweenness centrality, efficiency, quantitative graph theory, vulnerability analysis.

1 INTRODUCTION

Our daily lives are so dependent on the functioning of critical infrastructures [1] that they became a major target of terroristic attacks. In addition, well-planned assaults to the most critical and vulnerable hubs or spots can damage a system very heavily. Therefore, the protection of such infrastructures is a key challenge and essential. As one of the critical infrastructures, public transport plays a very important role in our society. One example of such a vulnerable public transport system is the German high-speed train network (ICE) [2] on which the study of this paper mainly focuses. In the future, many advanced security technologies can be applied to keep the ICE network safer. However, economic boundaries demand for highly efficient resource use. Thus, before deploying the security measures, decision makers need to deeply understand the vulnerabilities of the ICE network.

In this paper, we analyze the vulnerabilities of the ICE network using quantitative graph methodologies [3, 4]. First, we map the ICE network into an undirected distance-weighted graph. It is known that the betweenness centrality measure [5] can be used to detect the most transferable nodes in the network. The network efficiency measure [6] can be applied to identify the most efficient nodes. Based on these two measures, we propose a new vulnerability measure which we call betweenness-efficiency vulnerability measure, which merges the two approaches.

The reminder of this paper is structured as follows. In Section 2, the ICE network is mapped into a graph; the betweenness centrality measure and efficiency measure are introduced in detail. More importantly, the new proposed vulnerability measure is presented. In Section 3, the network analysis on the ICE network is carried out using the described measures. Moreover, a vulnerability analysis is conducted in this section for comparing these three

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N1-59-64

measures. In the last section, important conclusions are drawn and the paper ends with further discussions.

2 GRAPH MODEL AND QUANTITATIVE GRAPH

This section mainly introduces the Germany high-speed train system (ICE) in detail, the quantitative graph measures betweenness centrality and network efficiency, as well as the new proposed vulnerability measure. Firstly, the ICE network is mapped into an undirected distance-weighted graph.

2.1 Graph model

Similar to any other railway transportation system, the ICE train network consists of stations (nodes) and their connections (edges). Based on its map [2], the ICE network has 121 nodes and 168 edges. In this paper, an undirected distance-weighted graph $G(V,E)$, which is illustrated in Fig. 1, is abstracted from this network by mapping the stations on this network into nodes and the connections (train lines) between stations into edges whose weights are the real length (unit 100 km) between them. Here, $V=\{v_i \mid i=1,2,3,\ldots,n\}$ represents the set of nodes and $E=\{e_{ij} \mid v_i, v_j \in V\}$ denotes the set of edges of the network. $A=\left[a_{ij}\right]_{n\times n}$ is the distance-weighted adjacency matrix, where $a_{ij}=\omega_{ij}$ when $(v_i,v_j)\in E$, otherwise $a_{ij}=0$. Here, n means the number of nodes in a graph and ω_{ij} is the length between every pair of adjacent nodes with the unit of 100 km.

2.2 Quantitative graph methodology

Centrality measures can be used to identify the most central nodes in a graph. So far, many centrality measures have been developed and applied in network analysis. In this paper, we

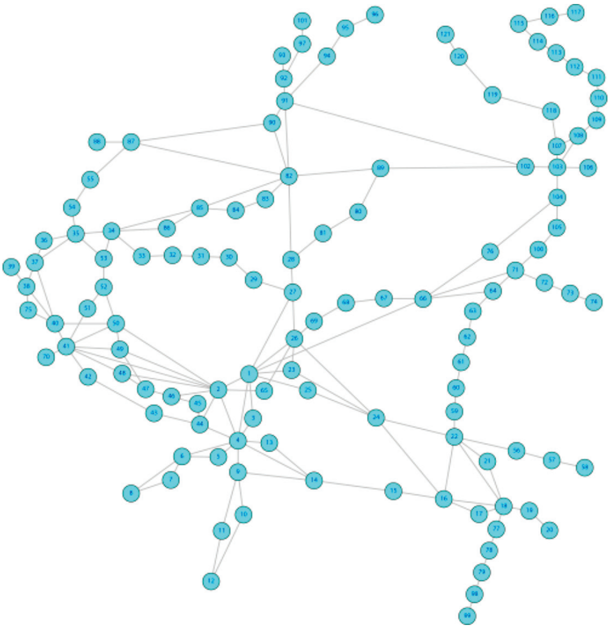

Figure 1: Graph model $G(V,E)$ of ICE train network.

mainly focus on the betweenness centrality measure which can be implemented to detect the most critical and transferable nodes. Besides this, the network efficiency measure can not only characterize the efficiency of the information exchange from one node to all other nodes in a network, but it can also be a tool to discern the most vulnerable nodes. Combining these two measures, a new vulnerability measure is proposed.

2.2.1 Betweenness centrality measure

The betweenness centrality measure quantifies how often one node would lie on the shortest paths between all other pairs of nodes in a graph. A node can be seen as the most crucial one in a graph if it has the highest value of betweenness centrality. The formula of the betweenness centrality $C_b\left(v_k\right)$ [5] for a node v_k is defined by:

$$C_b\left(v_k\right)=\frac{2}{(n-1)(n-2)}\sum_{i\neq k}^{n}\sum_{j\neq i,\, j\neq k}^{n}\frac{\sigma_{ij}\left(v_k\right)}{\sigma_{ij}}. \tag{1}$$

where, $n>2$, σ_{ij} denotes the total number of shortest paths between nodes i and j, and $\sigma_{ij}\left(v_k\right)$ represents the number of the shortest paths between nodes i and j passing through node k.

2.2.2 Efficiency measure

Based on [6, 7], the nodal efficiency measure is applied by calculating the length of the shortest paths from one node to all the others in the network. Its formula $E_{V(G)}\left(v_i\right)$ [6, 7] for one node v_i in the network G is defined by:

$$E_{V(G)}\left(v_i\right)=\frac{2}{n-1}\sum_{j\neq i}^{n}\frac{1}{d\left(v_i,v_j\right)}. \tag{2}$$

where, $n>1$, $d\left(v_i,v_j\right)$ denotes the length of the shortest path between node i and node j. The average efficiency measure $E_{Avg}\left(G\right)$ [6, 7] of a network G is defined by:

$$E_{Avg}\left(G\right)=\frac{2}{n(n-1)}\sum_{i}^{n}\sum_{j\neq i}^{n}\frac{1}{d\left(v_i,v_j\right)}. \tag{3}$$

2.2.3 Betweenness-efficiency vulnerability measure

Accordingly, based on the betweenness centrality and the efficiency measures, we propose a new vulnerability measure: the betweenness-efficiency vulnerability measure. This measure is defined by:

$$BEV\left(v_m\right)=\frac{\left|BEV^*\left(G\right)-BEV^*\left(v_m\right)\right|}{BEV^*\left(G\right)}. \tag{4}$$

where, $m=\left\{1,2,\ldots,n\right\}$, $BEV^*\left(G\right)$ denotes the original network value without removing any nodes, the network value after removing the m^{th} node from the original network is defined as:

$$BEV^*\left(v_m\right)=\frac{2}{(n-1)(n-2)}\sum_{k=1}^{n-1}BEV_m^*\left(v_k\right). \tag{5}$$

where, $n > 2$. Here, $BEV_m^*(v_k)$ is defined by:

$$BEV_m^*\left(v_k\right) = \sum_{i \neq k}^{n-1} \sum_{j \neq i, j = k}^{n-1} \left(\frac{1}{2^{d_m\left(v_i, v_j\right)}} - \frac{1}{2^{d_{m\_k}\left(v_i, v_j\right)}} \right).. \tag{6}$$

where, $d_m\left(v_i, v_j\right)$ denotes the length of the shortest path between nodes i and j after removing the m^{th} node from the original network, $d_{m\_k}\left(v_i, v_j\right)$ represents the length of the shortest path between nodes i and j passing thrgh node k after removing the m^{th} node from the original network. By choosing $2^{d_x\left(v_i, v_j\right)}$ cases where node i and node j are the same and so nullity are avoided. In general, the measure is used for choosing individual nodes for artificial attacks to the network with the highest possible effect.

Since the proposed measure is used to quantify the effect on the remaining network of removing a node from it, it is clear that the corresponding node needs to be removed for the calculation. However, the value of the measure at each node is independent of the order in which nodes are removed.

3 RESULTS

In this section, the aforementioned measures are applied to detect the most critical nodes. To compare which measure is more efficient for discerning the most critical nodes, the vulnerability analysis is also conducted. In order not to spread sensitive information, we have indexed the stations randomly and do not mention the station's names.

3.1 Network analysis

Table 1 presents the top five critical nodes of the ICE network based on the nodal betweenness centrality, nodal efficiency and the proposed betweenness-efficiency vulnerability.

According to the betweenness centrality measure in Table 1, the station *with ID 1* is detected as the most transmissible station based on how often a given station would be passed through by the shortest paths between all other pairs of stations. Furthermore, we found that station *1* is also identified as one of the top five critical nodes by the betweenness-efficiency vulnerability. It is interesting to observe that the station *103* ranked 2 in Table 1 is discerned as the most important node by nodal efficiency measure and the betweenness-efficiency vulnerability measure.

On the basis of the nodal efficiency measure, the station *103* is identified as the most efficient station of the ICE network based on the shortest paths from the given station to all other stations, as it is detected by the nodal betweenness centrality measure.

Table 1: The top five critical nodes of the ICE network.

Station ID	**Betweenness**	**Station ID**	**Efficiency**	**Station ID**	**Betweenness-efficiency**
1	0.284033613	103	1.007819958	103	0.101247186
103	0.280392157	106	0.850841497	4	0.100842476
22	0.201960784	41	0.829973494	34	0.086379072
2	0.196778711	50	0.827538527	1	0.08595542
82	0.181652661	91	0.811661689	35	0.059023728

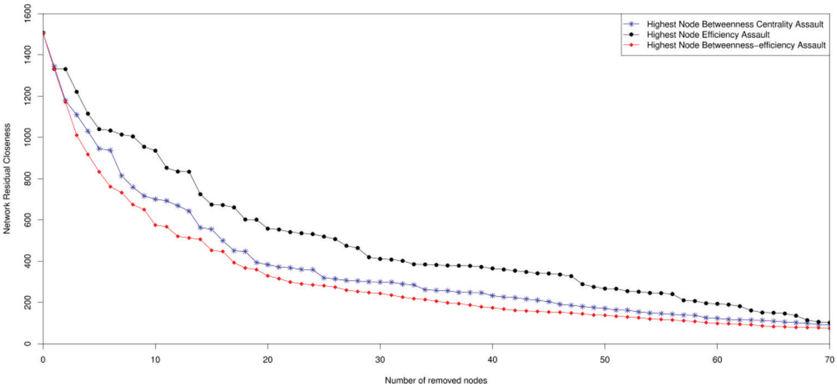

Figure 2: Network residual closeness of ICE network under various malicious assaults.

3.2 Vulnerability analysis

Before carrying out the vulnerability analysis of the ICE network, we introduce the vulnerability index network residual closeness [7]. This measure is based on how the closeness of a network would change after the removal of nodes or edges. It is demonstrated that the network residual closeness is more sensitive than other vulnerability indexes and can so detect even very insignificant network disturbances. Moreover, the network residual closeness is monotonous. It is defined by

$$RC = min_k \{C_k\} \qquad [7],$$

where $C_k = \sum_i \sum_{j \neq i} 1/2^{d_k(v_i, v_j)}$, $d_k(v_i, v_j)$ is the length of shortest path between nodes i and j after deleting node k and its corresponding edges from the original network.

Figure 2 shows the residual closeness of the ICE network under three kinds of malicious assaults. We can observe that the malicious assaults based on the strategy of betweenness-efficiency vulnerability can always lead to larger damages to the ICE network.

4 CONCLUSIONS AND DISCUSSIONS

In this paper, we extend the traditional approaches and propose a novel vulnerability measure. Through quantitative network analysis stations are identified as being critical. Based on the artificial attacker strategies derived from the three different measures applied, the novel betweenness-efficiency measure introduced in this article shows the highest impact on the overall network, as it aggregates two individual measures based on their residual closeness. Thus, we conclude that this novel measure seems to be promising for further research in this field. However, one measure cannot account for all factors when conducting network and vulnerability analysis. In further research, more aspects need to be taken into account. The idea of a network of networks [8, 9] might be a good approach, since it can combine more factors for network and vulnerability analysis.

ACKNOWLEDGEMENTS

The support from the German Federal Ministry of Education and Research (BMBF) (project RE(H)STRAIN) is gratefully acknowledged.

REFERENCES

[1] Rinaldi, S.M., Modeling and simulating critical infrastructures and their interdependencies. In: *Proceedings of the 37th annual Hawaii international conference on System sciences*, pp. 1–8, 2004.
https://doi.org/10.1109/hicss.2004.1265180

[2] ICE-Netz. *Deutsche Bahn*, 2016, available at https://www.bahn.de/p/view/service/fahrplaene/streckennetz.shtml (accessed 07 March, 2017).

[3] Dehmer, M. & Emmert-Streib, F., *Quantitative Graph Theory: Mathematical Foundations and Applications*. CRC Press, 2014.

[4] Dehmer, M., Emmert-Streib, F. & Pickl, S., *Computational Network Theory: Theoretical foundations and applications*. Wiley-VCH Verlang GmbH & Co. KGaA, Weinheim, 2015.

[5] Freeman, L.C., Centrality in social networks conceptual clarification. *Social Networks*, **1**, pp. 215–239, 1978.
https://doi.org/10.1016/0378-8733(78)90021-7

[6] Latora, V. & Marchiori, M., Economic small-world behavior in weighted networks. *The European Physical Journal B-Condensed Matter and Complex Systems*, **32**(2), pp. 249–263, 2003.
https://doi.org/10.1140/epjb/e2003-00095-5

[7] Nistor, M.S., Pickl, S., Raap, M. & Zsifkovits, M., Network efficiency and vulnerability analysis using the flow-weighted efficiency measure. *International Transactions in Operational Research*, 2017.
https://doi.org/10.1111/itor.12384

[8] Dangalchev, C., Residual closeness in networks. *Physica A: Statistical Mechanics and its Applications*, **365**, pp. 556–564, 2006.
https://doi.org/10.1016/j.physa.2005.12.020

[9] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H.E. & Havlin, S., Catastrophic cascade of failures in interdependent networks. *Nature*, **464**, pp. 1025–1028, 2010.
https://doi.org/10.1038/nature08932

[10] Gao, J., Buldyrev, S.V., Havlin, S. & Stanley, H.E., Robustness of a network of networks. *Physical Review Letters*, **107**(19), 2011.
https://doi.org/10.1103/physrevlett.107.195701