Reliability Engineering and System Safety 145 (2016) 62–73

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Flow-based vulnerability measures for network component importance: Experimentation with preparedness planning

Charles D. Nicholson [a], Kash Barker [a,*], Jose E. Ramirez-Marquez [b,c]

[a] School of Industrial and Systems Engineering, University of Oklahoma, USA
[b] School of Systems and Enterprises, Stevens Institute of Technology, USA
[c] Tec de Monterrey, School of Science and Engineering, Zapopan, Guadalajara, Mexico

ARTICLE INFO

Article history:
Received 30 October 2014
Received in revised form
21 August 2015
Accepted 28 August 2015
Available online 5 September 2015

Keywords:
Resilience
Vulnerability
Networks
Flow

ABSTRACT

This work develops and compares several flow-based vulnerability measures to prioritize important network edges for the implementation of preparedness options. These network vulnerability measures quantify different characteristics and perspectives on enabling maximum flow, creating bottlenecks, and partitioning into cutsets, among others. The efficacy of these vulnerability measures to motivate preparedness options against experimental geographically located disruption simulations is measured. Results suggest that a weighted flow capacity rate, which accounts for both (i) the contribution of an edge to maximum network flow and (ii) the extent to which the edge is a bottleneck in the network, shows most promise across four instances of varying network sizes and densities.

1. Introduction and motivation

The notion of resilience, broadly defined as the ability to withstand the effects of a disruption and subsequently return to a desired state, has been studied across a number of fields, including ecology [11,21,22], social sciences [48,6], engineering [13,16,23,36,44], and risk contexts [19,3,47], to name a few. *Resilience* has increasingly been seen in the literature [43], owing to the need to prepare for the inevitability of disruptions. For example, the US Department of Homeland Security through its National Infrastructure Protection Plan (2013) [14] shifts from solely focusing on disruption prevention and protection of infrastructure systems to risk management strategies that "strengthen national preparedness, timely response, and rapid recovery in the event" of an attack or disaster.

Fig. 1 illustrates two primary dimensions of resilience: vulnerability and recoverability. The network performance function $\varphi(t)$ describes the behavior of the network at time t (e.g., $\varphi(t)$ could describe traffic flow or delay for a highway network) [20,4,41,5]. Emphasis in this paper is placed on the *vulnerability* dimension of resilience. The ability of e^j to impact network performance in an adverse manner is a function of the network's *vulnerability* [34,52,53], similar in concept to a lack of *robustness* in the "resilience triangle" literature in civil infrastructure [10]. Jonsson et al. [30] define vulnerability as the magnitude of damage given the occurrence of a particular disruptive event, noting that the vulnerability of a network is highly dependent upon the type and extent of disruption e^j. We measure vulnerability as network performance after the removal of a set of nodes or links based only on topological features (i.e., without load redistribution leading to potential cascading failures).

There are two common approaches to quantifying the vulnerability of a network to a disruption [8]: (i) probabilistic models from reliability theory, and (ii) graph invariants as deterministic measures. Such graph invariants often include graph theoretic measures (e.g., centrality, diameter) [1,25,26,28,29,51]. This paper makes use of a tangible variation on the second type of approaches, wherein we use a network performance measure (e.g., network flow) rather than a graph theoretic measure. Recent studies have compared strictly topological models to flow-based or hybrid models for electric power networks [37,40], showing similarities in the results of both model types, though Ouyang et al. [38] offer caution on using topological models to quantify the real vulnerability of power networks.

Several works have explored the identification of important components in a network with respect to vulnerability. Nagurney and Qiang [32,33] develop a measure of network efficiency to describe the performance of a network when disrupted or congested, as well as an identification of the individual components

* Correspondence to: School of Industrial and Systems Engineering University of Oklahoma, 202W. Boyd St., Room 124, Norman, OK 73019, USA.
Tel.: +1 405 325 3721; fax: +1 405 325 7555.
E-mail address: kashbarker@ou.edu (K. Barker).

http://dx.doi.org/10.1016/j.ress.2015.08.014
0951-8320/

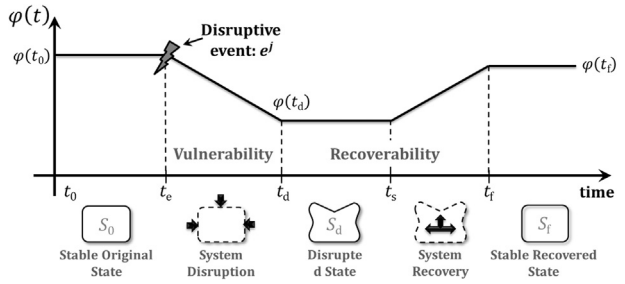


Fig. 1. Graphical depiction of network performance, $\varphi(t)$, across several state transitions over time.

that lead to adverse network performance, with mention given to applications in network vulnerability and robustness. Rodriguez-Nunez and Garcia-Palomares [46] develop vulnerability component importance measures for transportation networks based on travel time, while others have considered cost of travel time [27,49] and accessibility, or the ease of reaching components of the network [12,50]. Park et al. [42] offer a flow-based performance measure for setting rehabilitation investment priorities for the component of a water distribution network, while Ouyang et al. [39] examine the flow-based vulnerability of train networks.

While several works have dealt with definitions, paradigms, and methodological approaches to quantify network vulnerability, work in the broader characterization of network resilience is still in its infancy. With this paper, we look to first contribute to modeling and decision making for network vulnerability, a first step in a larger integrated resilience framework. Section 2 provides several importance measures, both existing in the literature and developed in this paper, many of which emphasize network performance and not solely network topology. Section 3 illustrates with several network instances, and concluding remarks are given in Section 4.

2. Quantifying network vulnerability and component importance

We opt for a flow-based performance function, $\varphi(t)$. Network performance could be defined in number of ways, including network connectivity or flow across the shortest path. For this work, we choose *all node pairs average maximum flow* for φ, calculated by finding the maximum flow from a source node s to a sink node t, then exhausting all (s,t) pairs across the network and averaging the maximum flow for each (s,t) pair. Implicitly this assumes max flows among s–t pairs are independent. This assumption allows for the computation of an upper bound on system flow performance.

Max flow problems can be solved by several algorithms. In this study we employ a minimum cost network flow formulation and solve the resulting linear program (LP) using a concurrent solver technique (a parallel processing approach in which each processor initializes a different algorithm) which includes the well-known and practically efficient simplex and dual simplex methods. Polynomially bounded algorithms exist for solving LP problems (e.g., the interior point method [31], and for a graph with n nodes, the number of max flow problems to be solved is a function in $O(n^2)$ making the all node pairs problem a polynomially bounded problem.

This work considers geographic based physical networks with capacitated and directed arcs. Examples include transportation networks in which traffic per hour on a roadway or bridges with weight restrictions constrain traffic flow. We consider a class of disruptive events that impair the capacity of one or more edges in the network. To prioritize preemptive efforts to reduce network-wide vulnerability, we develop a variety of edge-specific, flow-based metrics to identify the most important edges. Edges deemed as the most important can be reinforced or otherwise protected prior to any event to reduce network vulnerability or can be candidates for expedited recovery (though we focus on the vulnerability, and not recoverability, aspect of network resilience in this work). In this section we provide details concerning various candidate edge importance measures relating to network vulnerability.

2.1. Definitions and notation

Let $G=(V,E)$ denote a directed graph where V is a set of n vertices (also called nodes) and $E \subseteq V \times V$ is a set of m directed edges (also called arcs or links). For $(i,j) \in E$, the initial vertex i is called the tail and the terminal vertex j is called the head. Let c_{ij} and x_{ij} denote the capacity and flow on edge $(i,j) \in E$, respectively.

A *directed path* P from a source node s to a target node t is a finite, alternating sequence of vertices and one or more edges starting at node s and ending at node t, $P=\{s,(s,v_1),v_1,(v_1,v_2),v_2,\ \ldots,(v_k,t),t\}$ where all of the odd elements are distinct nodes in V and the even elements are directed edges in E. All nodes other than s and t are referred to as *internal* nodes. The length of path P is the number of edges it contains. The *capacity of a path* is equal to the minimum capacity of all edges in the path. That is, the capacity of path P equals $\min_{(i,j) \in P} c_{ij}$.

The *s–t max flow problem* utilizes a subset of all possible paths between s and t to route a maximum amount of a commodity from s to t without exceeding the capacity of any edge. The s–t max flow problem can be formulated as the linear programming problem in Eqs. (1)–(3).

$$max\ v_{st} \tag{1}$$

$$\text{s.t.} \sum_{(i,j) \in E} x_{ij} - \sum_{(j,i) \in E} x_{ji} = \begin{cases} \omega_{st} & \text{for } i=s \\ 0 & \forall\ i \in V\{s,t\} \\ -\omega_{st} & \text{for } i=t \end{cases} \tag{2}$$

$$0 \le x_{ij} \le c_{ij} \tag{3}$$

In objective function from Eq. (1), ω_{st} denotes the maximum feasible flow from s to t for any source and sink node pair $s,t \in V$ where $s \neq t$. Note if $s=t$, we assign $\omega_{st}=0$. The flow-conservation constraints in Eq. (2) require that the flow into and out of any internal node $i \in Vs,t$ to be equal, whereas the total flow out of s and the total flow into t must equal ω_{st}. The constraints in Eq. (3) ensure that edge flow does not exceed edge capacity.

2.2. Edge importance measures

Significant effort has been made in the literature on defining importance measures for components of graphs. A frequent theme in these measures is the notion of *centrality* [2,17]. *Edge betweenness,* for example, of $(i,j) \epsilon E$ is a function of the number of shortest paths between nodes s and t which include edge (i,j). The *edge betweenness centrality* of (i,j) is the sum of its edge betweenness for all s–$t$pairs. There are numerous modifications of both node and edge centrality measures, primarily based on shortest-paths within a graph (e.g., [9] for a sampling of such variants). Newman [35] introduced a modified edge centrality that does not restrict the metric to only shortest paths between s and t but stochastically includes other paths. In our work we introduce or otherwise consider multiple flow-based and topological measures relating to max flow paths within a graph, as described subsequently.

2.2.1. All pairs max flow edge count

The first edge importance measure we will consider is inspired by the basic edge betweenness centrality concept. However instead of shortest paths, we consider max flow paths. The *all pairs max flow edge count* is equal to the total number of times a given edge is utilized in all s–t pairs max flow problems. The intuition is that if an edge is used more often than others in contributing to maximum flow, then a disruption that impacts its capacity is likely to have a significant impact on network performance φ.

Let $\mu_{st}(i,j)=1$ if edge (i,j) is used in a given s–t max flow problem and 0 otherwise. We define the first candidate for edge importance based on the raw max flow edge tally divided by the total number of s–$t$pairs, as shown in Eq. (4).

$$I_{(i,j)}^{\text{MFcount}} = \frac{1}{n(n-1)}\sum_{s,t\in V}\mu_{st}(i,j) \tag{4}$$

If multiple paths share a minimally capacitated edge, there will be multiple paths that contribute the same value to a given s–t max flow problem. We arbitrarily choose among the shortest of these paths. For example, in Fig. 2, there are two example graphs with five nodes and edge capacities as listed. In both cases the max flow from node 1 to 5 is 1. In Fig. 2a, there are two paths from 1 to 5 with the same capacity: $\{1,(1,2),\ 2,(2,4),4,\ (4,5),5\}$ and $\{1,(1,3),\ 3,(3,4),4,(4,5),5\}$. Since these have the same length, we randomly choose a path to have flow. In Fig. 2b, the path $\{1,(1,4),\ 4,\ (4,5),5\}$ is the shortest, therefore only edges $(1,4)$ and $(4,5)$ are included as part of the max flow path tally.

2.2.2. Min cutset count

An s–t *cut* on a graph is a partitioning of nodes into two disjoint sets S and T such that $s\in S$ and $t\in T$. The s–t *cutset* is the set of edges which have a tail in S but terminate in T. The capacity of an s–t cut is equal to the sum of the capacity of the s–t cutset. The *min cut* of a graph is the s–t cut with minimal capacity. According to the max-flow min-cut theorem [15], the s–t max flow is equal to its min cut. If an edge (i,j) is a member of the min cutset for an s–t pair, then it is a bottleneck for the corresponding max flow problem, thus the intuition for this measure. Furthermore, if (i,j) is damaged and its capacity reduced, then the max flow value is also reduced. The edge importance measure $I_{(i,j)}^{\text{cutset}}$ is the total number of times edge (i,j) is a member of the min cutset for all s–t pairs. This is represented arithmetically in Eq. (5), where $\delta_{st}(i,j)=1$ if edge (i,j) is a member of the s–t min cutset and 0 otherwise.

$$I_{(i,j)}^{\text{cutset}} = \frac{1}{n(n-1)}\sum_{s,t\in V}\delta_{st}(i,j) \tag{5}$$

If multiple equivalent minimum cutsets exist, we choose one arbitrarily.

2.2.3. Edge flow centrality

Another variation on component importance from the literature useful for the current work is a node centrality measure based on max flow introduced by Freeman et al. [18]. Freeman's measure is derived from the total flow passing through node i when max flow ω_{st} is routed from s to t for all $s,t\in V$. A simple revision of the metric provides an importance based on the total volume of flow on an edge. Specifically, the *edge flow centrality* of $(i,j)\epsilon E$ is defined as the sum of flow on (i,j) for all possible s–t pair max flow problems divided by the sum of all pairs max flows, shown in Eq. (6), where $\omega_{st}(i,j)$ is the flow on (i,j) when the max flow ω_{st} is routed from s to t.

$$I_{(i,j)}^{\text{flow}} = \frac{\sum_{s,t\in V}\omega_{st}(i,j)}{\sum_{s,t\in V}\omega_{st}} \tag{6}$$

If more than one path have the same capacity for a given s–t max flow problem, then we employ the same strategy as with the all pairs max flow edge count.

2.2.4. Flow capacity rate and weighted flow capacity rate

The min cutset count from Eq. (5) addresses whether or not an edge is a bottleneck. and the edge flow centrality from Eq. (6) addresses the contribution of a given edge to max flow. The *flow capacity rate* (FCR) quantifies how close a given edge is to becoming a potential bottleneck based on flow amount and capacity. If an edge is significantly underutilized with respect to its capacity, then it is inherently robust to disruptions that reduce capacity. Whereas if $\omega_{st}(i,j)\approx c_{ij}$ then damage to (i,j) is more likely to affect network performance.

The edge flow capacity rate is the sum of the percentages of edge flows to edge capacity for all s–t pair max flow problems, shown in Eq. (7).

$$I_{(i,j)}^{\text{FCR}} = \frac{1}{n(n-1)}\sum_{s,t\in V}\frac{\omega_{st}(i,j)}{c_{ij}} \tag{7}$$

An edge with a high flow capacity rate is more likely to become a bottleneck than an edge with a lower value, but the expected impact to the overall network performance should also be a function of the expected contribution of the given edge provided by Eq. (6). A *weighted flow capacity rate* (WFCR) can be computed by weighting each term in Eq. (7) by the edge flow volume, as shown in Eq. (8).

$$I_{(i,j)}^{\text{WFCR}} = \frac{1}{n(n-1)}\sum_{s,t\in V}\left(I_{(i,j)}^{\text{flow}}\right)\frac{\omega_{st}(i,j)}{c_{ij}} = \frac{1}{n(n-1)\sum_{s,t\in V}\omega_{st}}\sum_{s,t\in V}\frac{[\omega_{st}(i,j)]^2}{c_{ij}} \tag{8}$$

2.2.5. One-at-a-time damage impact

The last edge importance measure we consider is an empirical one based on a direct computation of the impact to network performance when a given edge is damaged. The *one-at-a-time damage impact* importance measure is the average percent change across all s–t max flow problems when (i,j) has its capacity reduced by 50%. This is shown in Eq. (9), where $\omega'_{st,ij}$ is the max

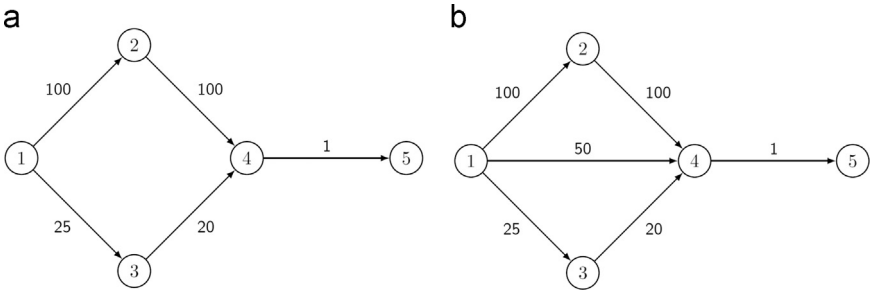
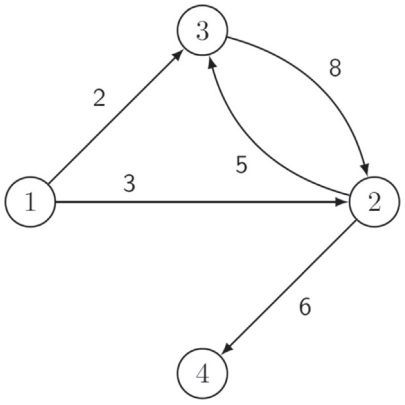


Fig. 2. Shortest path max flow edge count example.



All ***s*-*t*** pairs max flows

		Sink node			
		1	2	3	4
Source node	1	-	5	5	5
	2	0	-	5	6
	3	0	8	-	6
	4	0	0	0	-

Fig. 3. Example network to demonstrate importance measures.

flow from s to t when the capacity of (i,j) is set equal to $0.5c_{ij}$.

$$I_{(i,j)}^{\text{impact}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \frac{\omega_{st} - \omega'_{st'ij}}{\omega_{st}} \tag{9}$$

Eq. (9) is a specific application of the α-at-a-time flow importance measure by Rocco et al. [45] though considering a fractional capacity reduction rather than complete edge incapacitation. These measures are inspired by the Birnbaum [7] importance measure from reliability engineering.

2.3. Example network with performance and edge importance measures

We demonstrate the edge importance measures on the four node network depicted in Fig. 3. The edges are labeled according to their capacities. The s–t max flow table in Fig. 3 shows the max flows from every possible source to every possible sink node. The performance measure for this network is 3.33.

Table 1 reports the capacity, the all pairs max flow usage count, min cutset count, edge flow centrality, flow capacity rate, weighted flow capacity rate, and the one-at-a-time 50% capacity reduction damage impact importance measures for each edge. The values for the metric corresponding to the most important edge(s) are in bold. While the rank ordering is different by importance measures, there is some agreement as to the most important edge: $I_{(i,j)}^{\text{MFcount}}$ and $I_{(i,j)}^{\text{flow}}$ identify $(3,2)$ as the most important; $I_{(i,j)}^{\text{cutset}}$ and $I_{(i,j)}^{\text{FCR}}$ rank $(1,2)$ and $(1,3)$ as a tie for the most important edge; and $I_{(i,j)}^{\text{WFCR}}$ and $I_{(i,j)}^{\text{impact}}$ agree on $(2,4)$ as the most important.

In the following section we describe larger scale network problems and a simulated disruption scenario. The importance metrics will be used to make a priori decisions to reduce the vulnerability of the network.

3. Illustrative examples and empirical analysis

To evaluate the usefulness of the six edge importance measures under investigation we will simulate disruptions to large networks. The edge importance measures will be used to prioritize a simulated resource allocation process for reinforcing components of the network infrastructure. Assuming limited funding, for example, it is possible that only a small fraction of edges in a network (e.g., roadways, bridges, power lines) may be improved.

An importance ranking of edges with respect to overall network performance will allow for a more effective usage of such limited resources. As such, we will choose the top $k < m$ edges for a given importance metric and simulate the strengthening of the k edges. In a series of disruptive event simulations we quantify the quality of the *a priori* strengthening policies based on Eqs (5)–(9). We then simulate a recovery of the overall network to complete the analysis of the importance measures.

Table 1
Results of the importance measures for the edges of the example network in Fig. 3.

(i,j)	c_{ij}	$I_{(ij)}^{\text{MFcount}}$	$I_{(ij)}^{\text{cutset}}$	$I_{(ij)}^{\text{flow}}$	$I_{(ij)}^{\text{FCR}}$	$I_{(ij)}^{\text{WFCR}}$	$I_{(ij)}^{\text{impact}}$
(1, 2)	3	0.250	**0.250**	0.225	**0.250**	0.056	0.075
(1, 3)	2	0.250	**0.250**	0.150	**0.250**	0.038	0.050
(2, 3)	5	0.167	0.083	0.200	0.133	0.027	0.050
(2, 4)	6	0.250	0.083	0.425	0.236	**0.100**	**0.117**
(3, 2)	8	**0.333**	0.167	**0.450**	0.188	0.084	0.069

Note that the importance measures capture different perspectives on vulnerability. While the illustrative examples demonstrate how different these perspectives are for different network instances of varying size and density, the choice of an appropriate importance measure may depend on a particular application at hand. The empirical analysis in this section assumes no particular application area, as we are illustrating the differences in the measures.

3.1. Network instances with their disruption and recovery

The network instances in our empirical analysis are generated from a random geometric graph structure with bi-directional and capacitated edges. A bi-directional edge is modeled as two symmetric directed arcs. The symmetry implies that the capacity is equal for both arcs. The random geometric graph algorithm randomly positions nodes within a two dimensional area, and edges are added between all nodes that are within a specified distance. To create a network that is connected, after the algorithm terminates, if two or more disconnected components exists, two nodes are selected at random, each from a different disconnected component, and an edge is added between the two nodes. This process continues until the network is connected. All edges are then randomly assigned capacities according to a continuous uniform distribution on $[100, 1000]$. Each edge is then modified to become bi-directional. That is, for each edge (i,j) the edge (j,i) is added with $c_{ji} = c_{ij}$.

We simulate two sizes of networks, small and large, and a low-density and high-density version of each. The four network instances are depicted in Fig. 4. Fig. 4a and b depict the lower and higher density instances of the smaller network which both contain 20 nodes. The Small Graph with Lower Density (SGLD) instance has 20 bi-directional edges. The Small Graph with Higher Density (SGHD) contains 53 bi-directional edges. Fig. 4c and d portray the larger network size which consists of 70 nodes. The

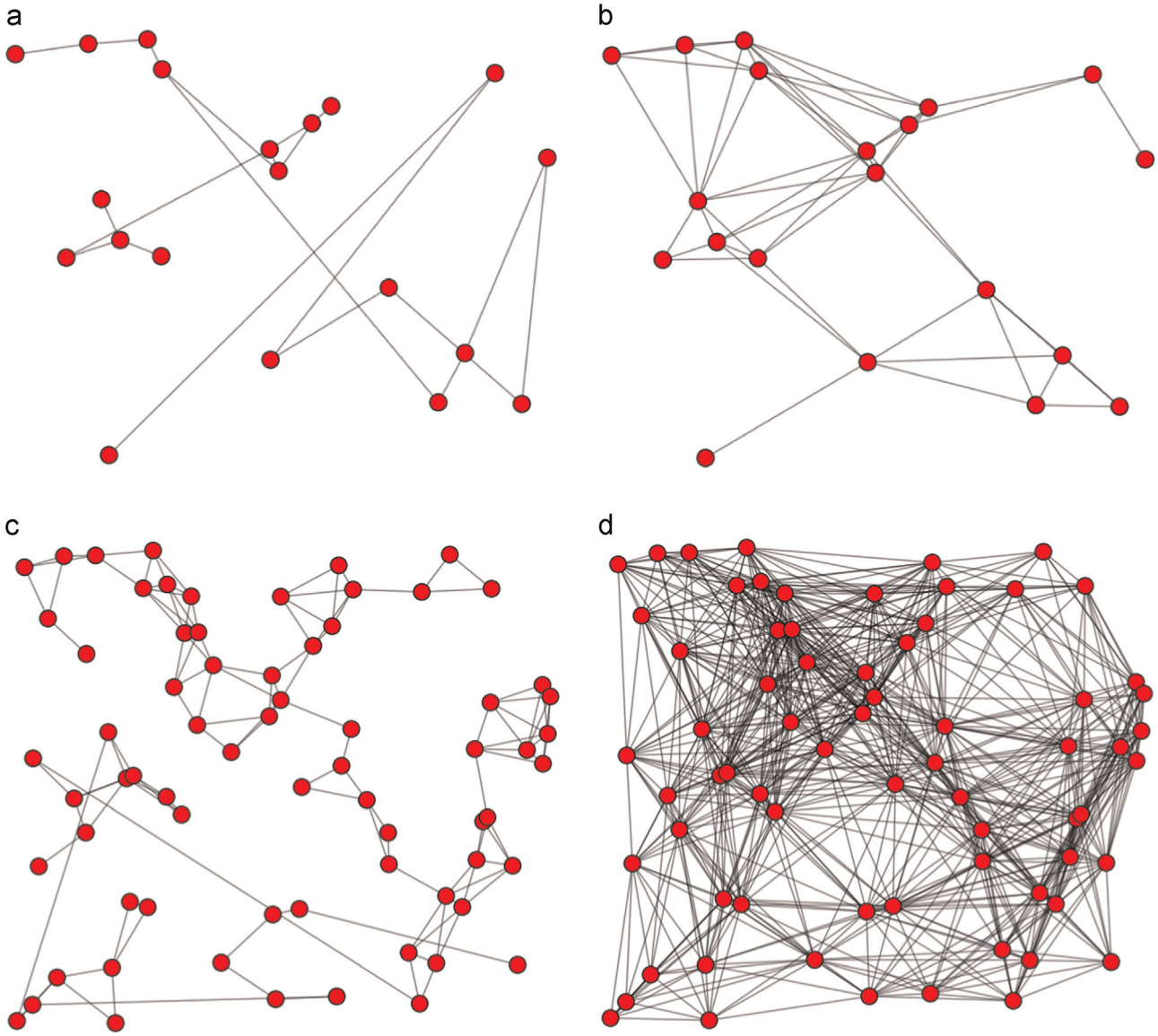


Fig. 4. Four network design instances for vulnerability analysis. (a) Small graph, lower density (SGLD), (b) Small graph, higher density (SGHD), (c) Large graph, lower density (LGLD) and (d) Large graph, higher density (LGHD).

low density (LGLD) instance has 128 bi-directional edges and the higher density (LGHD) instance contains 791. Lower density graphs have less inherent redundancy and may be more vulnerable to disruptions.

The simulated disruptions impact capacities of edges depending on the distance from the epicenter of the disruptive event. Four concentric circles of discrete damage levels are centered about the epicenter. The four damage levels reduce edge capacities by 80%, 60%, 40%, and 20%, with the most damage located at the smallest circle at the epicenter. Any edge that intersects one of these disruptive event circles sustains damage, and the damage sustained will be associated with the smallest of the concentric circles intersected (i.e., the largest related damage value). The circles, from smallest to largest, cover 10%, 20%, 30%, and 40% of the network region such that an individual damage level corresponds to 10% of the total area. Fig. 5 depicts an example of the four damage circles (not to scale) superimposed on one network instance. This approach to disrupting the network is similar to what could be expected with an explosion or possibly an earthquake (depending on the geographical scale).

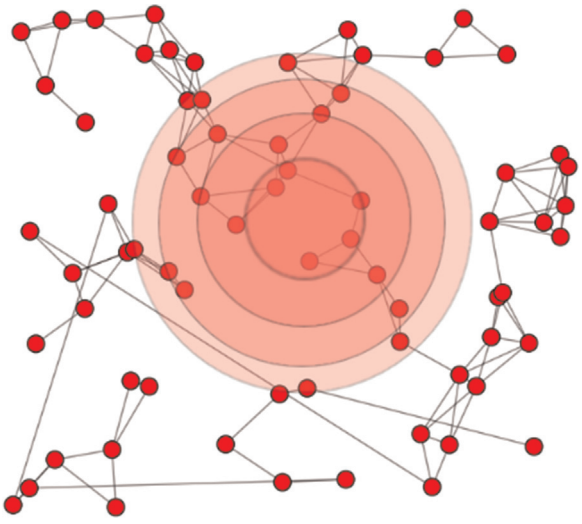


Fig. 5. Concentric circles of damage from a simulated disruptive event.

We perform 100 independent simulations on all four network instances. In each simulation the epicenter of the disruptive event is randomly located. Network performance φ is computed at the time of maximum disruption (time t_d from Fig. 1) to evaluate the vulnerability of the network without any preventive measures. Naturally, the approach to disrupting the network (in this case, concentric circles of varying capacity damage effects) will affect vulnerability results. However, as we are simulating several such disruptions, we feel that vulnerability results will be somewhat general.

For each candidate importance measure, we employ an associated improvement policy to strengthen certain edges. The top 15% of edges, ranked according to importance, are selected for strengthening. To evaluate the effectiveness of the rankings, we compare the average disrupted network performance across all simulated disruptions for each of the improvement policies as well as a "random selection" improvement policy, where 15% of edges are randomly selected for hardening.

An improved edge does not sustain as much damage as it would otherwise if affected in a disruption. Specifically, an edge that would suffer an 80% reduction in capacity would incur only 40% reduction if hardened; an edge which would sustain 60% damage would only experience 20%. The lower damage impact zones do not affect strengthened edges. Table 2 summarizes the disruptive event simulation scenario.

Finally, we expect policies based on the importance measures will also affect recoverability. To depict this we construct a highly simplified recovery procedure: each edge is recovered in parallel at a fixed rate (8% of their original edge capacity) per time unit. Since the most damaged edges must recover 80% of their capacity, there will a total of 10 time steps per simulated disruption. Networks will be recovered to their original performance level at t_0. The performance will be computed at every time step during the recovery to compare how the strengthening measures impact the recovery curve. Note that the focus of this work is how different edge prioritization policies can impact vulnerability and subsequently resilience. To understand resilience, recovery must be accounted for, but it is done so in a general way here. Combining the vulnerability-related policies with a study of more realistic recovery policies is considered future work.

Table 2
Disruptive event scenario damage details.

Damage circle	Total area	Edge damage (no hardening)	Edge damage (hardening)
Circle 1 (epicenter)	5%	80%	40%
Circle 2	10%	60%	20%
Circle 3	15%	40%	0%
Circle 4	20%	20%	0%

Table 3
Network instance descriptions and baseline performance metric, $\varphi(t_0)$.

Network instance	Nodes	Bi-directional edges	Density	Edges to be improved	$\varphi(t_0)$
SGLD	20	20	10.5%	3	285.0
SGHD	20	53	38.4%	8	1532.5
LGSD	70	128	6.0%	19	433.5
LGHD	70	791	32.8%	119	10,027.3

3.2. Edge importance associations

Summary information for the four network instances, including baseline network performance without disruption, $\varphi(t_0)$, is presented in Table 3.

A series of scatter plots for each edge importance measure plotted against the others is shown in Figs. 6–9 for the four network instances. The axes are scaled for comparison such that a point in the far upper right of a plot represents an edge that is listed as highly important for both associated ranking policies. A linear trend line with confidence intervals is superimposed.

Some measures display moderately positive linear correlations in all four instances (e.g., max flow count and edge flow centrality or flow capacity rate), suggesting that two measures draw similar conclusions as to edge vulnerability. Certain trend lines, however, are impacted more by outliers than by strong linear relationship (e.g., cutset count and flow capacity rate in Figs. 7 and 8). For decision-making purposes, the rankings of the importance measures may be more important than the values themselves. For example, given limited resources for mitigation, which edges are

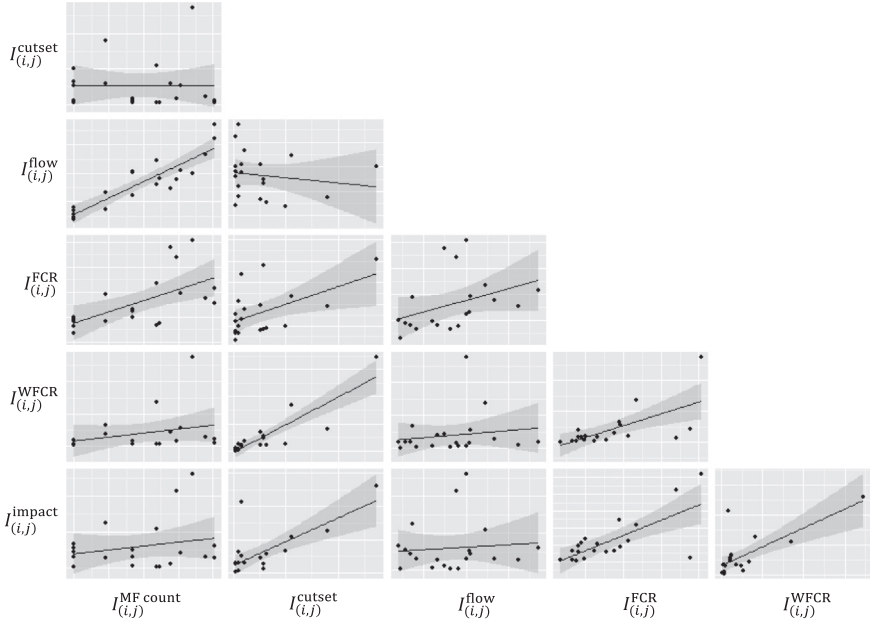


Fig. 6. Edge importance measure relationships for the Small Graph, Low Density instance.

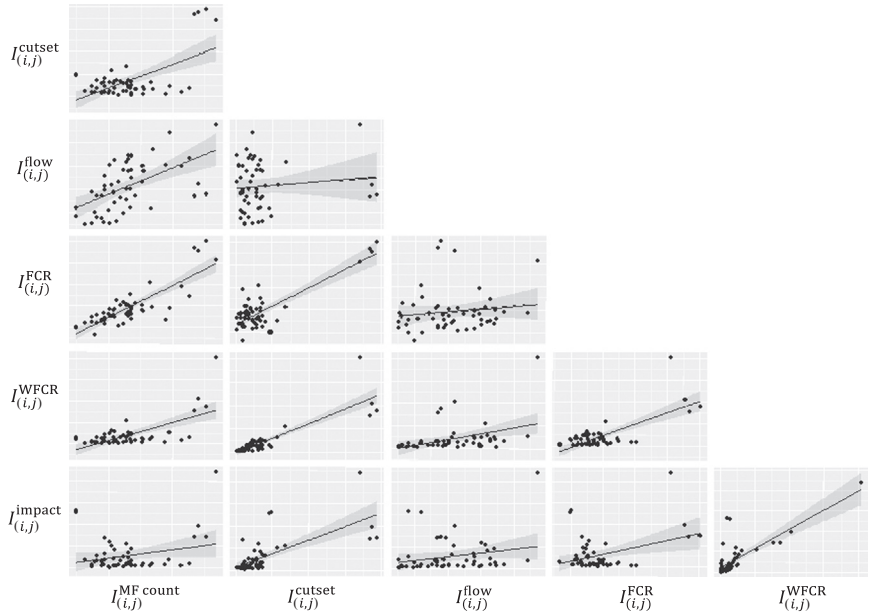


Fig. 7. Edge importance measure relationships for the Small Graph, High Density instance.

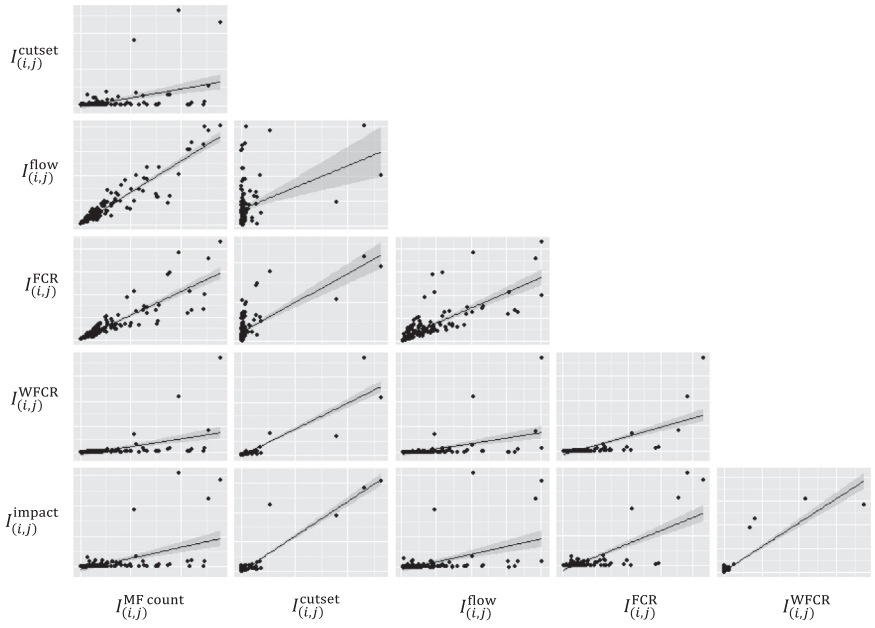


Fig. 8. Edge importance measure relationships for the Large Graph, Low Density instance.

the most critical. The Kendall-tau metric quantifies the strength of the monotonic relationship between two importance measures and is reported in Table 4.

For the large network instances and the higher density instances, the weighted flow capacity rate measure has the strongest association with the impact measure. Two importance measures with low association may provide different dimensions of information about the network. It is possible such discordance could be exploited to better inform improvement decisions. Edge flow centrality and cutset count on the High Density instances, for example, appear to provide independent information. Future research will explore the generality of such associations.

Given that the implementation strategy to reduce vulnerability is to select and improve the top ranked important edges, the lack of vulnerability in the network, or the network's robustness, after disruption will vary only if there are differences in the top ranked edges. Table 5 reports a measure of agreement among the most critical edges for the importance measures in these network instances. The agreement between two measures is evaluated based on the percentage of edges that are classified as within the top 15% of importance by both calculations. For example, max flow count and FCR both agree that a certain set of 16 edges should be in the top 19 of the LGLD instance; the percent agreement is reported as 84%. Max flow count and FCR are in good agreement across instances except the smallest instance (overall agreement of 110 out of 149 top ranks). Note that the top 15% of the SGLD instance is only three edges, thus explaining the behavior of the percent agreement for this instance. The empirical impact importance measure and WFCR have the second highest overall agreement (95 of 149 top ranks).

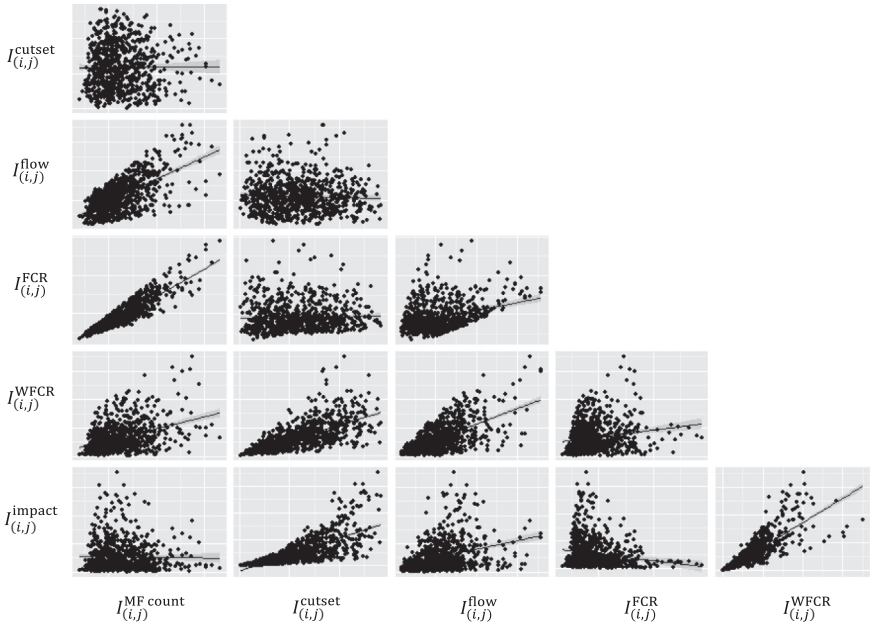


Fig. 9. Edge importance measure relationships for the Large Graph, High Density instance.

Table 4
Kendall-tau measure of association for edge importance measures.

	Small Graph, Low Density instance					**Small Graph, High Density instance**				
	$I^{\text{MFcount}}_{(i,j)}$	$I^{\text{cutset}}_{(i,j)}$	$I^{\text{flow}}_{(i,j)}$	$I^{\text{FCR}}_{(i,j)}$	$I^{\text{WFCR}}_{(i,j)}$	$I^{\text{MFcount}}_{(i,j)}$	$I^{\text{cutset}}_{(i,j)}$	$I^{\text{flow}}_{(i,j)}$	$I^{\text{FCR}}_{(i,j)}$	$I^{\text{WFCR}}_{(i,j)}$
$I^{\text{cutset}}_{(i,j)}$	−0.10	–	–	–	–	0.03	–	–	–	–
$I^{\text{flow}}_{(i,j)}$	0.73	−0.15	–	–	–	0.43	−0.01	–	–	–
$I^{\text{FCR}}_{(i,j)}$	0.47	0.40	0.36	–	–	0.56	0.17	0.10	–	–
$I^{\text{WFCR}}_{(i,j)}$	0.19	0.71	0.17	0.58	–	0.28	0.62	0.38	0.21	–
$I^{\text{impact}}_{(i,j)}$	0.02	0.56	0.01	0.46	0.44	−0.01	0.50	0.20	−0.13	0.57
	Large Graph, Low Density instance					**Large Graph, High Density instance**				
	$I^{\text{MFcount}}_{(i,j)}$	$I^{\text{cutset}}_{(i,j)}$	$I^{\text{flow}}_{(i,j)}$	$I^{\text{FCR}}_{(i,j)}$	$I^{\text{WFCR}}_{(i,j)}$	$I^{\text{MFcount}}_{(i,j)}$	$I^{\text{cutset}}_{(i,j)}$	$I^{\text{flow}}_{(i,j)}$	$I^{\text{FCR}}_{(i,j)}$	$I^{\text{WFCR}}_{(i,j)}$
$I^{\text{cutset}}_{(i,j)}$	0.22	–	–	–	–	0.01	–	–	–	–
$I^{\text{flow}}_{(i,j)}$	0.78	0.19	–	–	–	0.40	−0.03	–	–	–
$I^{\text{FCR}}_{(i,j)}$	0.78	0.35	0.64	–	–	0.74	0.05	0.18	–	–
$I^{\text{WFCR}}_{(i,j)}$	0.56	0.63	0.57	0.62	–	0.25	0.54	0.43	0.13	–
$I^{\text{impact}}_{(i,j)}$	0.38	0.41	0.41	0.35	0.51	0.01	0.60	0.28	−0.09	0.74

3.3. Network vulnerability and recovery by preparedness policy

The six preparedness policies, as well as “do nothing” and random policies, are tested for 100 simulated disruptive events. The first policy, the “do nothing” policy referred to as “none” in the subsequent figures, selects no edges for hardening. The second policy randomly selects 15% of edges to harden. The third through the eighth polices are based on the importance measures max flow count, cutset count, edge flow centrality, flow capacity rate, weighted flow capacity rate, and one-at-a-time impact, respectively.

Boxplots depicting network vulnerability by policy and network instance are presented in Fig. 10. The vertical axis represents the percent performance loss at time of greatest disruption, t_d, with respect to the baseline performance. That is, $1-\frac{\varphi(t_d)}{\varphi(t_0)} \times 100\%$. As expected there is notable variation in the vulnerability from the simulated disruptions. Some disruptions do not affect many edges, whereas others occur in more dense areas of the network and cause severe shock to the network. The interquartile range, as well as the “whiskers” of the boxplots which depict the upper and lower inner fences of the data, reveal notable differences between the small and large networks. The smaller graphs have a wider spread of vulnerability due to the fact that (i) a smaller graph with fewer edges is naturally less likely to be impacted by the simulated disruptions, but (ii) when they are impacted, there is a higher probability that important components are affected and the damage is more severe.

Mean network vulnerability percentages at time t_d are listed in Table 6. Possibly more important than expected vulnerability at disruption is the “worst case” vulnerability disruption scenario. Maximum vulnerabilities occurring during the most disruptive of

Table 5
Percent agreement among top ranked importance measures.

	Small Graph, Low Density instance					**Small Graph, High Density instance**				
	$I_{(i,j)}^{\text{MFcount}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$	$I_{(i,j)}^{\text{MFcount}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	0%	–	–	–	–	50%	–	–	–	
$I_{(i,j)}^{\text{flow}}$	100%	0%	–	–	–	38%	13%	–	–	–
$I_{(i,j)}^{\text{FCR}}$	0%	33%	0%	–	–	75%	50%	25%	–	–
$I_{(i,j)}^{\text{WFCR}}$	0%	100%	0%	33%	–	63%	75%	25%	50%	–
$I_{(i,j)}^{\text{impact}}$	0%	67%	0%	67%	67%	50%	75%	13%	50%	50%
	Large Graph, Low Density instance					**Large Graph, High Density instance**				
	$I_{(i,j)}^{\text{MFcount}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$	$I_{(i,j)}^{\text{MFcount}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	32%	–	–	–	–	13%	–	–	–	–
$I_{(i,j)}^{\text{flow}}$	74%	32%	–	–	–	55%	14%	–	–	–
$I_{(i,j)}^{\text{FCR}}$	84%	42%	74%	–	–	74%	17%	31%	–	–
$I_{(i,j)}^{\text{WFCR}}$	53%	79%	53%	63%	–	29%	49%	47%	19%	–
$I_{(i,j)}^{\text{impact}}$	37%	63%	47%	47%	63%	11%	59%	28%	6%	65%

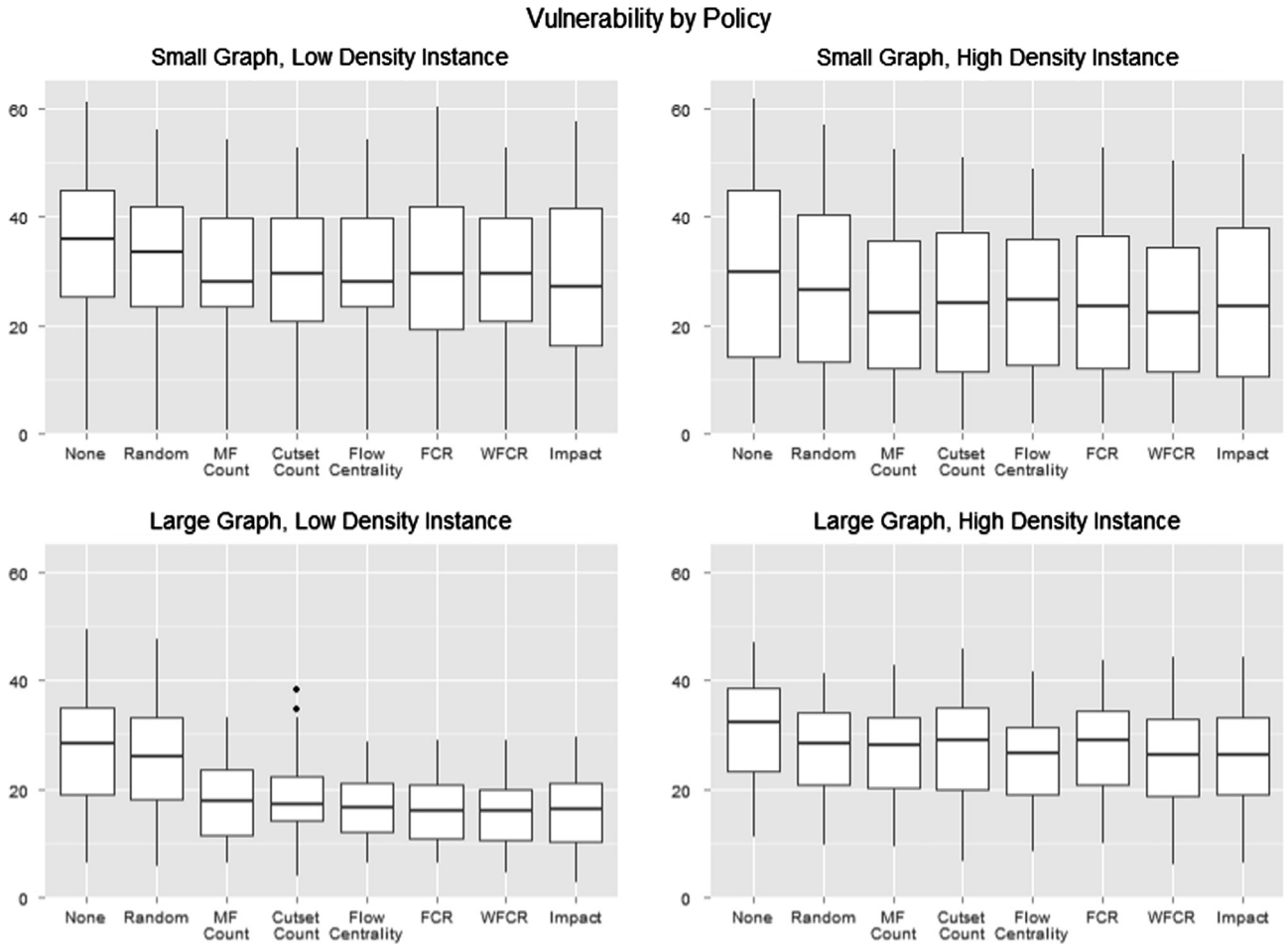


Fig. 10. Network robustness for each network instance and preparedness policy.

the 100 simulated events is also listed in Table 6. The least vulnerable network performance means and worst-case disruptions are in bold.

The network types prove to exhibit different inherent strengths with regard to vulnerability to disruptions. The two larger graphs have more edges and thus a higher likelihood of redundant paths. The worst case vulnerability without edge hardening for the larger graphs is less than 50%, whereas the two smaller instances have maximum vulnerabilities observations exceeding 60% performance drops. The percentage point range of maximum vulnerability varies considerably by instance type: 8.5%, 13.0%, 20.9%, and 5.5% for SGLD, SGHD, LGLD, and LGHD, respectively. The graph

type which benefits most from an improvement policy is the LGLD instance, whereas the graph which benefits the least is the LGHD instance.

Accordingly the most effective preparedness policies on average (and for the worst case disruptions) change based on network type. The cutset count ranking policy is a top performer in the SGLD instance but the weakest among the competing importance metrics in the LGLD instance. The WFCR importance ranking generates the most consistently effective improvement strategy, yielding the least vulnerable network on average in all four instances.

To determine statistically valid vulnerability differences between ranking policies, given that the performance measurements are not independent (i.e., a given disrupted event is replicated for each improvement policy), the familywise error rate should be controlled. As such Holm [24] adjusted *p*-values for multiple comparisons of repeated measures tests are recorded in Table 7.

All policies, including random improvements, statistically outperform (with 95% confidence) the "do nothing" strategy (not shown). Four cases exist in which the importance ranked policies do not statistically outperform random: FCR on SGLD (no difference) and LGHD (underperforms); max flow count and cutset count on LGHD (no difference).

Table 6
Network vulnerability by preparedness policy.

Policy	SGLD		SGHD		LGLD		LGHD	
	Mean	Max	Mean	Max	Mean	Max	Mean	Max
None	34.6%	61.2%	30.0%	61.7%	27.6%	49.5%	31.1%	46.9%
Random	32.4%	55.9%	27.2%	56.8%	26.0%	47.6%	27.7%	**41.4%**
MF count	29.6%	54.3%	24.3%	52.4%	17.7%	33.2%	27.5%	42.7%
Cutset count	**28.9%**	**52.7%**	24.3%	51.1%	18.1%	38.1%	27.9%	45.8%
Flow centrality	29.6%	54.3%	24.8%	**48.7%**	16.8%	**28.6%**	**26.0%**	**41.4%**
FCR	31.3%	60.2%	24.8%	52.7%	15.9%	28.8%	28.4%	43.8%
WFCR	**28.9%**	**52.7%**	**23.6%**	50.4%	**15.6%**	28.9%	**26.0%**	44.4%
Impact	29.6%	57.6%	24.2%	51.4%	**15.6%**	29.6%	26.2%	44.4%

The average network recovery curves for the 100 simulations are presented in Fig. 11. Due to the similarity of the recovery process, only a subset of the policies is represented. Specifically, the "do nothing," cutset count, edge flow centrality, and WFCR based improvement policies are plotted for the 10 time periods until full network recovery. Note that in the SGLD plot, the cutset count and WCFR performances are perfectly aligned and cannot be distinguished.

Predominantly, the average recoveries for all improvement policies occur at similar rates such that the network performance lines do not intersect until the final time step. However, the edge flow centrality importance policy in particular has a recovery curve that behaves differently than the others. For example, in the LGLD plot, the flow centrality policy outperforms the cutset count in terms of reducing vulnerability, but during the recovery process it soon lags in performance. This underperforming trend is clearly seen in the SGLD network recovery where edge flow centrality does not stimulate as aggressive of a recovery as the other metrics. Evidently, the importance measures affect both the initial impact vulnerability from a disruption as well as the efficiency of the recovery efforts. These two facets of resilience should be considered jointly when evaluating a network improvement strategy and will be explored further in future efforts.

4. Concluding remarks

Many previous network disruption studies focus on graph theoretic measures to identify network components that may have an adverse impact on network connectivity if they are disrupted. Alternatively, this work focuses on network performance-driven measures of vulnerability to develop component importance measures that provide a more tangible representation of how network flows are disrupted. And we address disrupted flow in the broader context of network resilience, combining vulnerability and recoverability.

Of six measures compared in this paper, initial results suggest that adopting a preparedness policy based on the weighted flow capacity rate importance measure results in networks with the least vulnerability across network instances. This measure

Table 7
Adjusted *p*-values for repeated measures significance testing of preparedness policies.

Instance		Random	MF count	Cutset count	Flow centrality	FCR	WFCR
SGLD	MF count	$<10^{-3}$	–	–	–	–	–
	Cutset count	$<10^{-3}$	1	–	–	–	–
	Flow centrality	$<10^{-3}$	–	1	–	–	–
	FCR	0.166	0.015	$<10^{-3}$	0.015	–	–
	WFCR	$<10^{-3}$	1	–	1	$<10^{-3}$	–
	Impact	$<10^{-3}$	1	1	1	$<10^{-3}$	1
SGHD	MF count	$<10^{-3}$	–	–	–	–	–
	Cutset count	$<10^{-3}$	1	–	–	–	–
	Flow centrality	$<10^{-3}$	0.116	0.112	–	–	–
	FCR	$<10^{-3}$	$<10^{-3}$	0.001	1	–	–
	WFCR	$<10^{-3}$	$<10^{-3}$	0.001	$<10^{-3}$	$<10^{-3}$	–
	Impact	$<10^{-3}$	1	0.604	0.116	0.001	0.116
LGLD	MF count	$<10^{-3}$	–	–	–	–	–
	Cutset count	$<10^{-3}$	0.616	–	–	–	–
	Flow centrality	$<10^{-3}$	$<10^{-3}$	0.003	–	–	–
	FCR	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	–	–
	WFCR	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	0.163	–
	Impact	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	0.146	0.866
LGHD	MF count	0.139	–	–	–	–	
	Cutset count	1	0.174	–	–	–	
	Flow centrality	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	–	–	
	FCR	$<10^{-3}$	$<10^{-3}$	0.005	$<10^{-3}$	–	
	WFCR	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	1	$<10^{-3}$	–
	Impact	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	0.414	$<10^{-3}$	$<10^{-3}$

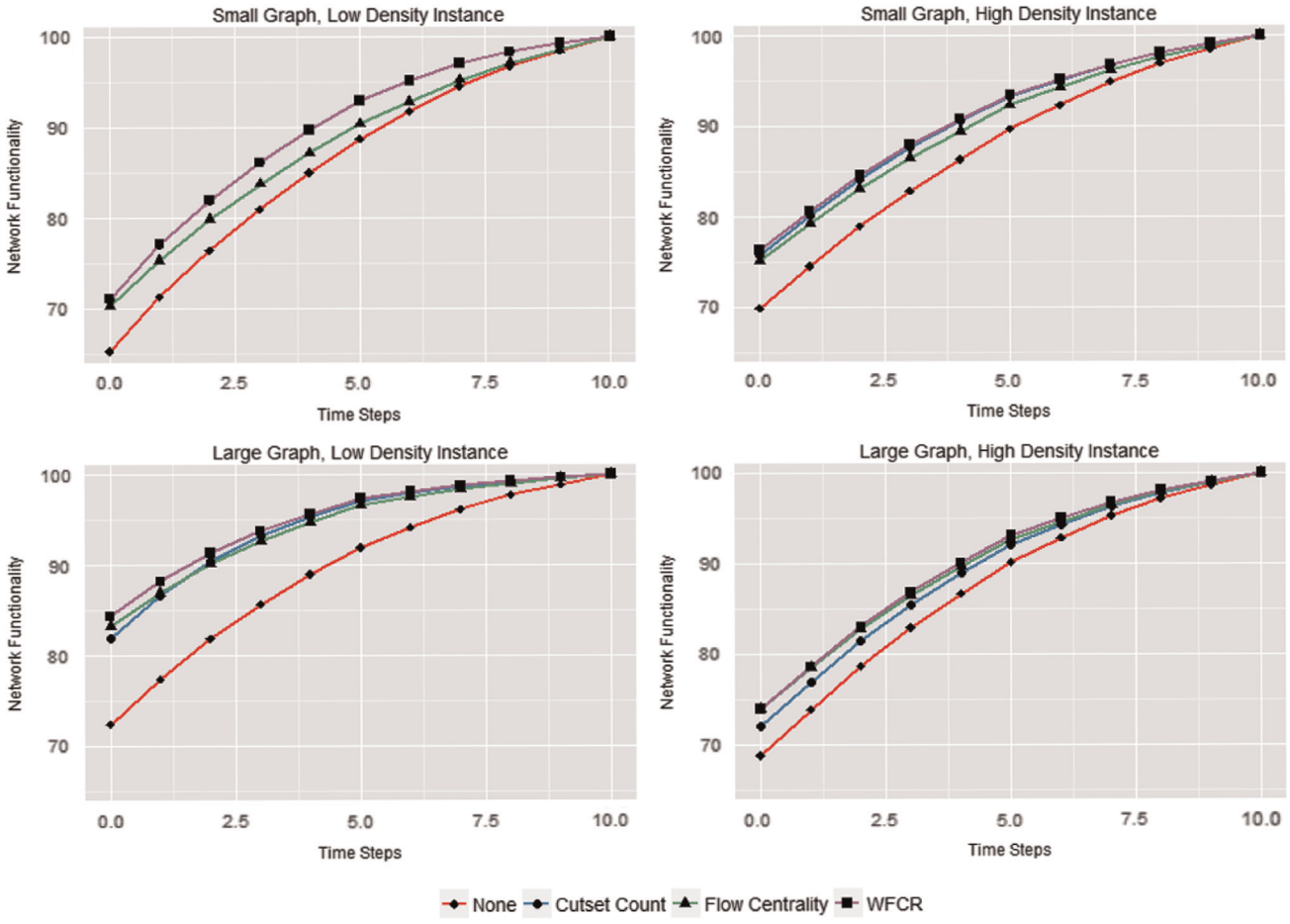


Fig. 11. Recovery curves for selected preparedness policies.

accounts for (i) the amount of flow across an edge relative to the network max flow as well as (ii) the capacity of the arc, accounting for both criticality to max flow as well as capacity. Perhaps these two dimensions combine to identify edges that produce a robust network, particularly for those generated in the empirical analysis provided in this paper. However, as the different flow-based vulnerability importance measures discussed in this paper offer different perspectives of network vulnerability, the efficacy of the importance measure may differ depending on the network application.

Future work remains in drawing broader conclusions about relationships among the importance measures across a larger variety and larger generation of network instances. Initial results suggest that measures may complement each other in terms of identifying edges for hardening. And this is not surprising, as some of the measures focus more on network topology (e.g., cutset) while others are focused almost entirely on network performance (e.g., max flow edge count). Further, Fig. 11 suggests that there could be some interaction between vulnerability and recoverability for certain preparedness policies. We will explore this possible interaction with more realistic recovery policies (e.g., optimal recovery crew assignment). The damage model used to generate the disruptive event can impact results, and accordingly future work will explore how the importance measures are robust to the damage model and network configuration, particularly in the context of tactical (recovery) and strategic (design) decision making. Finally, the implicit assumption regarding the independence of max flows among s–t pairs will be addressed using a multi-commodity flow formulation as well as incorporating a probabilistic factor relating to concurrent node-pair flows. More realistic upper bounds on network performance are particularly valuable in the context of tactical (recovery) and strategic (design) decision making.

References

[1] Albert R, Albert I, Nakarado GL. Structural vulnerability of the North American power grid. Phys Rev E 2004;69(2):025103.
[2] Anthonisse JM. The rush in a directed graph (Technical report BN 9/71). Stichting Mathematisch Centrum. Amsterdam; 1971.
[3] Aven T. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Anal 2011;31(4):515–22.
[4] Barker K, Ramirez-Marquez JE, Rocco CM. Resilience-based network component importance measures. Reliab Eng Syst Saf 2013;117(1):89–97.
[5] Baroud H, Ramirez-Marquez JE, Barker K, Rocco CM. Stochastic measures of network resilience: applications to waterway commodity flows. Risk Anal 2014;34(7):1317–35.
[6] Baruth KE, Carroll JJ. A formal assessment of resilience: the Baruth protective factors inventory. J Individ Psychol 2002;58(3):235–44.
[7] Birnbaum ZW. On the importance of different component in a multicomponent system. In: Krishnaiah PR, editor. Multivariate analysis, 11. New York (NY): Academic Press; 1969.
[8] Boesch FT, Satyanarayana A, Suffel CL. A survey of some network reliability analysis and synthesis results. Networks 2009;54(2):99–107.
[9] Brandes U. On variants of shortest-path betweenness centrality and their generic computation. Soc Netw 2008;30(2):136–45.
[10] Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, von Winterfeldt D. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq. Spectra 2003;19(4):733–52.
[11] Carpenter S, Walker B, Anderies JM, Abel N. From metaphor to measurement: resilience of what to what? Ecosystems 2001;4(8):765–81.
[12] Chen A, Yang C, Kongsomsaksakul S, Lee M. Network-based accessibility measures for vulnerability analysis of degradable transportation networks. Netw Spat Econ 2007;7(3):241–56.

[13] Cimellaro G, Reinhorn A, Bruneau M. Seismic resilience of a hospital system. Struct Infrastruct Eng 2010;6(1):127–44.
[14] National Infrastructure Protection Plan. Department of homeland security. Washington, DC: Office of the Secretary of Homeland Security; 2013.
[15] Ford LR, Fulkerson DR. Maximal flow through a network. Can J Math 1956;8:399–404.
[16] Francis R, Bekera B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 2014;121(1):90–103.
[17] Freeman LC. A set of measures of centrality based upon betweenness. Sociometry 1977;40:35–41.
[18] Freeman LC, Borgatti SP, White DR. Centrality in valued graphs: a measure of betweenness based on network flow. Soc Netw 1991;13(2):141–54.
[19] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Anal 2006;26(2):293–6.
[20] Henry D, Ramirez-Marquez JE. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 2012;99:114–22.
[21] Holling CS. Resilience and stability of ecological systems. Annu Rev Ecol Syst 1973;4(1):1–23.
[22] Holling CS. Engineering resilience versus ecological resilience. In: Schulze PC, editor. Engineering with ecological constraints. Washington (DC): National Academy Press; 1996. p. 31–44.
[23] Resilience engineering: concepts and precepts. In: Hollnagel E, Woods DD, Leveson N, editors. Aldershot, UK: Ashgate Press; 2006.
[24] Holm S. A simple sequentially rejective multiple test procedure. Scand J Stat 1979;6(2):65–70.
[25] Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex Networks. Phys Rev E 2002;65(5):056109.
[26] Holmgren AJ. Using graph models to analyze the vulnerability of electric power networks. Risk Anal 2006;26(4):955–69.
[27] Jenelius E, Petersen T, Mattsson L-G. Importance and exposure in road network vulnerability analysis. Transp Res Part A: Policy Pract 2006;40(7):537–60.
[28] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Saf 2010;95(12):1335–44.
[29] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems. Reliab Eng Syst Saf 2013;120:27–38.
[30] Jonsson H, Johansson J, Johansson H. Identifying critical components in technical infrastructure networks. J Risk Reliab 2008;222(2):235–43.
[31] Karmarkar N. A new polynomial time algorithm for linear programming. Combinatorica 1984;4(4):373–95.
[32] Nagurney A, Qiang Q. A network efficiency measure for congested networks. Europhys Lett 2007;79:38005.
[33] Nagurney A, Qiang Q. Robustness of transportation networks subject to degradable links. Europhys Lett 2007;80:68001.
[34] Nagurney A, Qiang Q. A network efficiency measure with application to critical infrastructure networks. J Glob Optim 2008;40(1–3):261–75.
[35] Newman M. A measure of betweenness centrality based on random walks. Soc Netw 2004;26(2):175–88.
[36] Ouyang M, Duenas-Osorio L. Time-dependent resilience assessment and improvement of urban infrastructure systems. Chaos 2012;22(3):033122.
[37] Ouyang M, Zhao L, Pan Z, Hong L. Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks. Phys A: Stat Mech Appl 2014;403(1):45–53.
[38] Ouyang M, Pan Z, Hong L, Zhao L. Correlation analysis of different vulnerability metrics on power grids. Phys A: Stat Mech Appl 2014;396(15):204–11.
[39] Ouyang M, Zhao L, Hong L, Pan Z. Comparisons of complex network based models and real train flow model to analyze chinese railway vulnerability. Reliab Eng Syst Saf 2014;123:38–46.
[40] Ouyang M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos 2013;23:023114.
[41] Pant R, Barker K, Ramirez-Marquez JE, Rocco S. CM. Stochastic measures of resilience and their application to container terminals. Comput Ind Eng 2014;70(1):183–94.
[42] Park JI, Lambert JH, Haimes YY. Hydraulic power capacity of water distribution networks in uncertain conditions of deterioration. Water Resour Res 1998;34(12):3605–14.
[43] Park J, Seager TP, Rao PSC, Convertino M, Linkov I. Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 2013;33(3):356–67.
[44] Reed DA, Kapur KC, Christie RD. Methodology for assessing the resilience of networked infrastructure. IEEE Syst J 2009;3(2):174–80.
[45] Rocco CM, Ramirez-Marquez JE, Salazar DE, Zio E. A flow importance measure with application to an Italian transmission power system. Int J Perform Eng 2010;6(1):53–61.
[46] Rodriguez-Nunez E, Garcia-Palomares JC. Measuring the vulnerability of public transport networks. J Transp Geography 2014;35(1):50–63.
[47] Rose AZ, Dixon PB, Giesecke J, Avetisyan M. Economic consequences of and resilience to terrorism. (Current research project synopsis). National Center for Risk and Economic Analysis of Terrorism Events; 2012.
[48] Smith BW, Dalen J, Wiggins K, Tooley E, Christopher P, Bernard J. The brief resilience scale: assessing the ability to bounce back. Int J Behav Med 2008;15(3):194–200.
[49] Sullivan JL, Novak DC, Aultman-Halla L, Scott DM. Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: a link-based capacity-reduction approach. Transp Res Part A: Policy Pract 2010;44(5):323–36.
[50] Taylor MAP, Sekhar SVC, D'Este GM. Application of accessibility based methods for vulnerability analysis of strategic road networks. Netw Spat Econ 2006;6(3-4):267–91.
[51] Wu J, Barahona M, Tan Y-J, Deng H-Z. Spectral measure of structural robustness in complex networks. IEEE Trans Syst Man Cybernetics Part A: Syst Hum 2011;41(6):1244–52.
[52] Zhang C, Ramirez-Marquez JE, Rocco C. A new holistic method for reliability performance assessment and critical components detection in complex networks. IIE Trans 2011;43(9):661–75.
[53] Zio E, Sansavini G, Maja R, Marchionni G. An analytical approach to the safety of road networks. Int J Reliab Qual Saf Eng 2008;15(1):67–76.