Vulnerability Importance Measures Toward Resilience-Based Network Design

Kash Barker
Assistant Professor, Industrial and Systems Engineering, University of Oklahoma, Norman, OK, USA

Charles D. Nicholson
Assistant Professor, Industrial and Systems Engineering, University of Oklahoma, Norman, OK, USA

Jose E. Ramirez-Marquez
Associate Professor, Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ, USA

ABSTRACT: Network resilience to a disruption is generally considered to be a function of the initial impact of the disruption (the network's vulnerability) and the trajectory of recovery after the disruption (the network's recoverability). In the context of network resilience, this work develops and compares several flow-based importance measures to prioritize network edges for the implementation of preparedness options. For a particular preparedness option and particular geographically located disruption, we compare the different importance measures in their resulting network vulnerability, as well as network resilience for a general recovery strategy. 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.

Resilience, broadly defined as the ability to stave off the effects of a disruption and subsequently return to a desired state, has been studied across a number of fields, including engineering (Hollnagel et al. 2006, Ouyang and Duenas-Osorio 2012) and risk contexts (Haimes 2009, Aven 2011), to name a few. *Resilience* has increasingly been seen in the literature (Park et al. 2013), recognizing the need to prepare for the inevitability of disruptions.

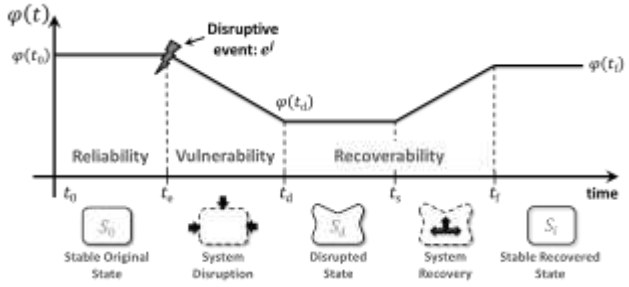


Figure 1: Graphical depiction of network performance, $\varphi(t)$, over time (adapted from Henry and Ramirez-Marquez (2012)).

Figure 1 illustrates three dimensions of resilience: reliability, vulnerability, and recoverability. The network service function $\varphi(t)$ describes the behavior or performance of the network at time t (e.g., $\varphi(t)$ could describe traffic flow or delay for a highway network). Prior to disruption e^j, the ability of the network to meet performance expectations is described by its *reliability*, often considered to the likelihood of connectivity of a network. Research in the area of *recoverability* is related to understanding the ability and speed of networks to recover after a disruptive event, similar in concept to *rapidity* in the "resilience triangle" literature in civil infrastructure (Bruneau et al. 2003).

Emphasis in this paper is placed on the *vulnerability* dimension, or the ability of e^j to impact network performance in an adverse manner is a function of the network's *vulnerability* (Nagurney and Qiang 2008, Zio et al. 2008, Zhang et al. 2011), similar in concept to

robustness in the "resilience triangle" literature. Haimes (2006) broadly offers that that the states of the system are described by a state vector, suggesting that vulnerability is multifaceted (i.e., certain aspects of a system may be adversely affected by certain events and not others). Our work adopts this qualitative perspective, though we assume that the vulnerabilities found in the different aspects of the network can still be measured by changes in a single network service function $\varphi(t)$. As such, Jonsson et al. (2008) define vulnerability appropriately for our work as the magnitude of damage given the occurrence of a particular disruptive event.

Networks have been characterized in two broad categories with respect to how their vulnerability is analyzed (Mishkovski et al. 2011): (i) those that involve "structural robustness," or how networks behave after the removal of a set of nodes or links based only on topological features, and (ii) those that involve "dynamic robustness," or how networks behave after the removal of a set of nodes or links given load redistribution leading to potential cascading failures. With respect to Figure 1, in networks that are primarily described by structural robustness (e.g., inland waterway, railway), t_e and t_d would coincide with each other such that network performance drops immediately as disruption e^j occurs. The performance of networks exhibiting dynamic robustness would dissipate over time after a disruption due to cascading effects (e.g., electric power networks), such that t_d is subsequent to t_e. This paper focuses on networks described by structural robustness.

Emphasis is placed on vulnerability in the larger context of network resilience. Resilience is defined here as the time dependent ratio of recovery over loss, noting the notation for resilience, $\mathit{Я}$ (Whitson and Ramirez-Marquez 2009) as *R* is commonly reserved for *reliability*. Similar in concept to the *resilience triangle*, we make use of the resilience paradigm provided in Figure 1, and we quantify resilience with Eq. (1) (Pant et al. 2014, Baroud et al. 2014, Barker et al. 2013, Henry and Ramirez-Marquez 2012). $\varphi(t_0)$ is the "as-planned" performance level of the network, t_d is the point in time after the disruption where network performance is at its most disrupted level, and recovery of the network occurs between times t_s and t_f.

$$\mathit{Я}_\varphi\left(t|e^j\right) = \frac{\varphi(t|e^j)-\varphi(t_\mathrm{d}|e^j)}{\varphi(t_0)-\varphi(t_\mathrm{d}|e^j)} \quad (1)$$

1. QUANTIFYING NETWORK VULNERABILITY

A common approach to quantifying network vulnerability is with graph invariants (e.g., connectivity, diameter, betweenness centrality) as deterministic measures (Boesch et al. 2009). We focus on tangible metrics of network behavior in the form of a flow-based service function, $\varphi(t)$, rather than graph theoretic measures of performance. 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.

This work considers geographic based physical networks with capacitated and symmetric 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.

1.1. 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, $P = \{s, (s, v_1), v_1, (v_1, v_2), v_2, \dots, (v_k, t), t\}$ 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 *maximum capacity of a path* is equal to the minimum capacity of all edges in the path. That is, the max 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.

1.2. Proposed Importance Measures

Several importance measures for components of graphs have previously been offered. A frequent theme in these measures is the notion of *centrality* [Anthonisse 1971, Freeman 1977]. *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. Newman [2004] 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 several flow-based and topological measures relating to max flow paths within a graph.

1.2.1. All Pairs Max Flow Edge Count

The first importance measure 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 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. (2). 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 otherwise equally capacitated paths.

$$I_{(i,j)}^{\text{MF count}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \mu_{st}(i, j) \qquad (2)$$

1.2.2. 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, 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. 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. (3), where $\delta_{st}(i, j) = 1$ if edge (i, j) is a member of the s-t min cutset and 0 otherwise. If multiple

equivalent minimum cutsets exist, we choose one arbitrarily.

$$I_{(i,j)}^{\text{cutset}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \delta_{st}(i,j) \quad (3)$$

1.2.3. Edge Flow Centrality

Another variation from the literature useful for this work is a node centrality measure based on max flow introduced by Freeman [1991]. 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. (4), where $\omega_{st}(i,j)$ is the flow on (i,j) when the max flow ω_{st} is routed from s to t.

$$I_{(i,j)}^{\text{flow}} = \frac{\sum_{s,t \in V} \omega_{st}(i,j)}{\sum_{s,t \in V} \omega_{st}} \quad (4)$$

1.2.4. Flow Capacity Rate and Weighted Flow Capacity Rate

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. (5).

$$I_{(i,j)}^{\text{FCR}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \frac{\omega_{st}(i,j)}{c_{ij}} \quad (5)$$

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. A *weighted flow capacity rate* (WFCR) can be computed by weighting each term in Eq. (5) by the edge flow volume.

$$I_{(i,j)}^{\text{WFCR}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \left(I_{(i,j)}^{\text{flow}}\right) \frac{\omega_{st}(i,j)}{c_{ij}} \quad (6)$$

1.2.5. One-at-a-Time Damage Impact

We consider a baseline empirical measure 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. (7), where $\omega'_{st,ij}$ is the max flow from s to t when the capacity of (i,j) is set equal to $0.5c_{ij}$.

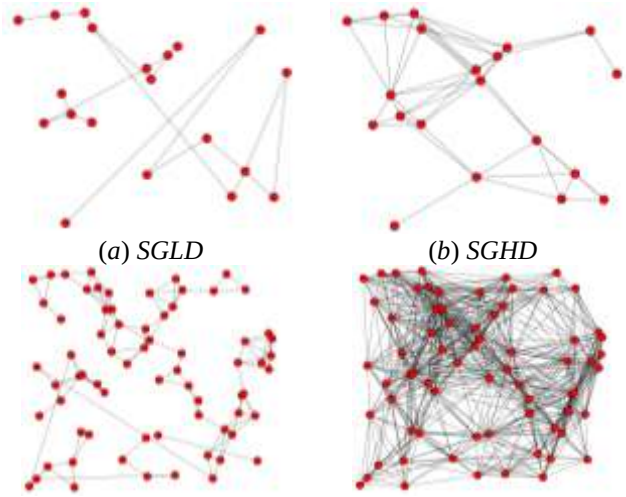
$$I_{(i,j)}^{\text{impact}} = \frac{1}{n(n-1)} \sum_{s,t \in V} \frac{\omega_{st} - \omega'_{st,ij}}{\omega_{st}} \quad (7)$$

2. ILLUSTRATIVE EXAMPLES

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 composed of two symmetric directed 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 component 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].

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 Figure 2. Figure 2a and 2b 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. Figure 2c and 2d portray the larger network size which consists of 70 nodes. The 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.



(*a*) *SGLD* (*b*) *SGHD*

(*c*) *LGLD* (*d*) *LGHD*

Figure 2: Four network design instances for vulnerability analysis.

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 correspond to 10% of the total area. Figure 3 depicts an example of the four damage circles 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).

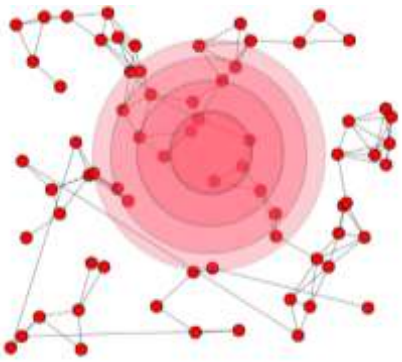


Figure 3: Concentric circles of damage from a simulated disruptive event.

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 to evaluate the vulnerability of the network without any preventive measures. The approach to disrupting the network 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 1 summarizes the disruptive event simulation scenario.

To recover the network we assume a straightforward process in which the capacities of all links are recovered in parallel at 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 are recovered to their original performance level. 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 is done so in a general way here.

Table 1: Disruptive event scenario damage details.

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

2.1. Initial Results

Some measures displayed 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 drew similar conclusions as to edge vulnerability. For the purposes of this study, the priority rankings of the importance measures are more important than the values themselves. The Kendall-tau metric quantifies the strength of the monotonic relationship between two importance measures and is reported in Tables 2 through 5.

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 without a strong correlation provide different dimensions of information about the network. It is possible such orthogonality 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.

Table 2: Kendall-tau measure of association for edge importance measures: SGLD instance.

	$I_{(i,j)}^{\text{MF count}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	-0.10	-	-	-	-
$I_{(i,j)}^{\text{flow}}$	0.73	-0.15	-	-	-
$I_{(i,j)}^{\text{FCR}}$	0.47	0.40	0.36	-	-
$I_{(i,j)}^{\text{WFCR}}$	0.19	0.71	0.17	0.58	-
$I_{(i,j)}^{\text{impact}}$	0.02	0.56	0.01	0.46	0.44

Table 3: Kendall-tau measure of association for edge importance measures: SGHD instance.

	$I_{(i,j)}^{\text{MF count}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	0.03	-	-	-	-
$I_{(i,j)}^{\text{flow}}$	0.43	-0.01	-	-	-
$I_{(i,j)}^{\text{FCR}}$	0.56	0.17	0.10	-	-
$I_{(i,j)}^{\text{WFCR}}$	0.28	0.62	0.38	0.21	-
$I_{(i,j)}^{\text{impact}}$	-0.01	0.50	0.20	-0.13	0.57

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

	$I_{(i,j)}^{\text{MF count}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	0.22	-	-	-	-
$I_{(i,j)}^{\text{flow}}$	0.78	0.19	-	-	-
$I_{(i,j)}^{\text{FCR}}$	0.78	0.35	0.64	-	-
$I_{(i,j)}^{\text{WFCR}}$	0.56	0.63	0.57	0.62	-
$I_{(i,j)}^{\text{impact}}$	0.38	0.41	0.41	0.35	0.51

Table 5: Kendall-tau measure of association for edge importance measures: LGHD instance.

	$I_{(i,j)}^{\text{MF count}}$	$I_{(i,j)}^{\text{cutset}}$	$I_{(i,j)}^{\text{flow}}$	$I_{(i,j)}^{\text{FCR}}$	$I_{(i,j)}^{\text{WFCR}}$
$I_{(i,j)}^{\text{cutset}}$	0.01	-	-	-	-
$I_{(i,j)}^{\text{flow}}$	0.40	-0.03	-	-	-
$I_{(i,j)}^{\text{FCR}}$	0.74	0.05	0.18	-	-
$I_{(i,j)}^{\text{WFCR}}$	0.25	0.54	0.43	0.13	-
$I_{(i,j)}^{\text{impact}}$	0.01	0.60	0.28	-0.09	0.74

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. Mean network vulnerability percentages at time t_d are listed in Table 6. Maximum vulnerabilities occurring during the most disruptive of the 100 simulated events is also listed. The least vulnerable network performance means and worst-case disruptions are in bold.

Table 6: Vulnerability by preparedness policy.

	SGLD		**SGHD**	
Policy	Mean	Max	Mean	Max
None	34.6%	61.2%	30.0%	61.7%
Random	32.4%	55.9%	27.2%	56.8%
MF Count	29.6%	54.3%	24.3%	52.4%
Cutset Count	**28.9%**	**52.7%**	24.3%	51.1%
Flow Centrality	29.6%	54.3%	24.8%	**48.7%**
FCR	31.3%	60.2%	24.8%	52.7%
WFCR	**28.9%**	**52.7%**	**23.6%**	50.4%
Impact	29.6%	57.6%	24.2%	51.4%
	LGLD		**LGHD**	
Policy	Mean	Max	Mean	Max
None	27.6%	49.5%	27.6%	49.5%
Random	26.0%	47.6%	26.0%	47.6%
MF Count	17.7%	33.2%	17.7%	33.2%
Cutset Count	18.1%	38.1%	18.1%	38.1%
Flow Centrality	16.8%	**28.6%**	16.8%	**28.6%**
FCR	15.9%	28.8%	15.9%	28.8%
WFCR	**15.6%**	28.9%	**15.6%**	28.9%
Impact	**15.6%**	29.6%	**15.6%**	29.6%

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.

3. CONCLUSIONS

Many previous network disruption studies focus on graph theoretic, topological measures to identify network components that may have an adverse impact on network connectivity if they are disrupted. We focus directly on network performance and 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.

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 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.

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). Finally, 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.

4. REFERENCES

Aven, T. (2011). "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience." *Risk Analysis*, 31(4), 515-522.

Barker, K., Ramirez-Marquez, J.E., and Rocco, C.M. (2013). "Resilience-Based Network Component Importance Measures." *Reliability Engineering and System Safety*, 117(1), 89-97.

Baroud, H., Ramirez-Marquez, J.E., Barker, K., and Rocco, C.M. (2014). "Stochastic Measures of Network Resilience: Applications to Waterway Commodity Flows." *Risk Analysis*, 34(7), 1317-1335.

Boesch, F.T., Satyanarayana, A., and Suffel, C.L. (2009). "A Survey of Some Network Reliability Analysis and Synthesis Results." *Networks*, 54(2), 99-107.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., and von Winterfeldt, D. (2003). "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities." *Earthquake Spectra*, 19(4), 733-752.

Freeman, L.C., Borgatti, S.P., and White, D.R. (1991). "Centrality in Valued Graphs: A Measure of Betweenness Based on Network Flow." *Social Networks*, 13(2), 141-154.

Haimes, Y.Y. (2006). "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures." *Risk Analysis*, 26(2), 293-296.

Haimes, Y.Y. (2009). "On the Definition of Resilience in Systems." *Risk Analysis*, 29(4), 498-501.

Henry, D., and Ramirez-Marquez, J.E. (2012). "Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time." *Reliability Engineering and System Safety*, 99, 114-122.

Hollnagel, E., Woods, D.D., and Leveson, N. (eds). (2006). *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Press.

Jonsson, H., Johansson, J., and Johansson, H. (2008). "Identifying Critical Components in Technical Infrastructure Networks." *Journal of Risk and Reliability*, 222(2), 235-243.

Mishkovski, I., Biey, M., and Kocarev, L. (2011). "Vulnerability of Complex Networks." *Communication in Nonlinear Science and Numerical Simulations*, 16(1), 341-349.

Nagurney, A., and Qiang, Q. 2008. "A Network Efficiency Measure with Application to Critical Infrastructure Networks." *Journal of Global Optimization*, 40(1-3), 261-275.

Newman, M. (2004). "A Measure of Betweenness Centrality Based on Random Walks. *Social Networks*, 26(2), 175-188.

Ouyang, M., and Duenas-Osoro, L. (2012). "Time-dependent Resilience Assessment and Improvement of Urban Infrastructure Systems." *Chaos*, 22(3), 033122.

Pant, R., Barker, K., Ramirez-Marquez, J.E., and Rocco, C.M. (2014). "Stochastic Measures of Resilience and their Application to Container Terminals." *Computers and Industrial Engineering*, 70(1), 183-194.

Park, J., Seager, T.P., Rao, P.S.C., Convertino, M., and Linkov, I. (2013). "Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems." *Risk Analysis*, 33(3), 356–367.

Whitson, J., and Ramirez-Marquez, J.E. (2009). "Resiliency as a Component Importance Measure in Network Reliability." *Reliability Engineering and System Safety*, 94(10), 1685-1693.

Zhang, C., Ramirez-Marquez, J.E., and Rocco, C.M. (2011). "A New Holistic Method for Reliability Performance Assessment and Critical Components Detection in Complex Networks." *IIE Transactions*, 43(9), 661-675.

Zio, E., Sansavini, G., Maja, R., and Marchionni, G. (2008). "An Analytical Approach to the Safety of Road Networks." *International Journal of Reliability, Quality and Safety Engineering*, 15(1), 67-76.