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/

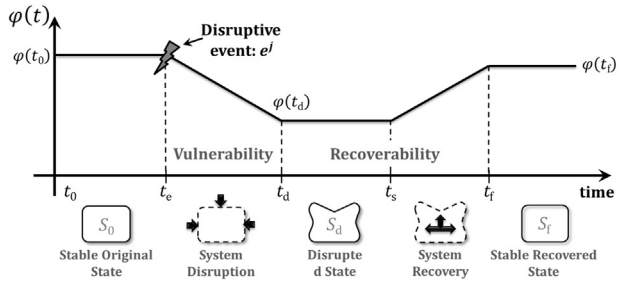

Fig. 1. Graphical depiction of network performance, $\varphi(t)$, across several state transitions over time.

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.