Reliability Engineering and System Safety 176 (2018) 154–161

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A bi-objective formulation for robust defense strategies in multi-commodity networks

Matthew McCarter[a], Kash Barker[a,*], Jonas Johansson[b], Jose E. Ramirez-Marquez[c,d]

[a] School of Industrial and Systems Engineering, University of Oklahoma, USA
[b] Division of Risk Management and Societal Safety, Lund University, Sweden
[c] School of Systems and Enterprises, Stevens Institute of Technology, USA
[d] Tec de Monterrey, School of Science and Engineering, Zapopan, Guadalajara, Mexico

ARTICLE INFO

Keywords:
Vulnerability
Resilience
Multi-commodity network flow
Max flow
Rail transportation

ABSTRACT

Characterizing system performance under disruption is a growing area of research, particularly for describing a system's resilience to disruptive events. Within the framework of system resilience, this study approaches the minimization of a multiple-commodity system's vulnerability to multiple disruptions. The vulnerability of a system is defined by the degree to which commodities can no longer flow through the system to satisfy demand given a disruptive event. A multi-objective formulation is developed to find defense strategies at minimal cost that maintain a high level of demand satisfaction across all commodities. A solution method involving an estimation of the Pareto frontier via the Non-dominated Sorted Genetic Algorithm II (NSGA-II) is also proposed. A decision support environment is proposed and supported by application of the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). The proposed formulation and solution method are illustrated with an example generated from the multi-commodity Swedish rail network.

1. Introduction and motivation

Characterizing the performance of a critical infrastructure following a disruptive event is an increasingly important area of research, given (i) the frequency of possible disruptions, and (ii) the scale of their implications. The US government emphasizes resilience planning for critical infrastructure, suggesting that they "must be secure and able to withstand and rapidly recover from all hazards" [36]. The ability to withstand, to adapt to, and to recover from a disruption is generally referred to as *resilience* [37].

A number of qualitative and quantitative approaches for characterizing resilience have been offered in the recent literature [19]. One such approach is depicted graphically in Fig. 1 [5,17,31]. This approach describes system performance before, during, and after a disruption with function $\varphi(t)$. Note two dimensions of resilience in Fig. 1. The lack of ability of the network to maintain performance immediately following disruptive event e^k is referred to as its *vulnerability*, an area receiving attention in the network literature for several years [18,21]. The ability of the network to return to an acceptable level of performance in a timely manner is referred to as its *recoverability*, a burgeoning area of study in the network field [12,29,3]. Moreover, recoverability has garnered attention earlier within specific fields of research (e.g., power system reliability [38]).

This work focuses on the vulnerability dimension of resilience. The evaluation and quantification of vulnerability is possible in a way that is generalizable across many problem instances. Graph encoding and network formulation are often relied upon for applying optimization approaches to a particular system, and it is assumed that networks of interest in this study lend themselves to such modeling paradigms. In previous research, efforts to quantify network vulnerability characteristics were directed towards graph-theoretic measures (e.g., edge betweenness, centrality, network diameter) [9,21,27]. However, performance-driven measures may be of more practical use in network defense and vulnerability reduction planning [22,28]. These metrics connect the idea of vulnerability with network flow as a proxy of system performance. As such, node and/or arc importance is a function of the degree to which overall network performance depends on the existence of, capacity of, and flow along that node/arc.

Various research has explored network defense strategies from a number of resource allocation [6], game theoretic [13], and bi- or tri-level optimization [2,34] perspectives. A review of such attack and defense strategy models is provided by Hausken and Levitin [16]. There exist many attack and defense strategy studies focusing on for example single-commodity networks, such as the interdiction of lines in a power transmission system based on a greedy algorithm that optimizes

[*] Correspondence to: School of Industrial and Systems Engineering, University of Oklahoma, 202 W. Boyd St., Room 124, Norman, OK 73019, USA.
E-mail address: kashbarker@ou.edu (K. Barker).

https://doi.org/10.1016/j.ress.2018.04.011
Received 22 June 2017; Received in revised form 15 November 2017; Accepted 18 April 2018
Available online 20 April 2018

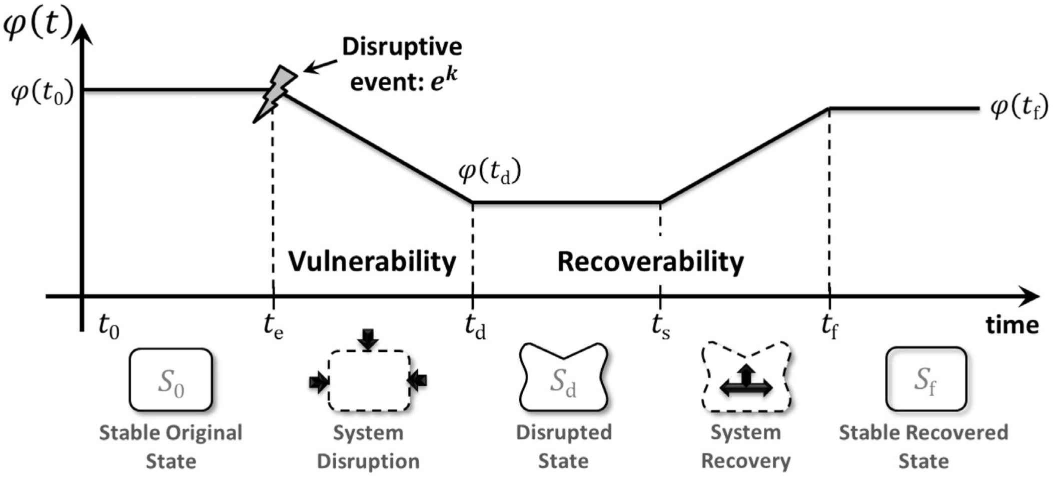

Fig. 1. Illustration of network performance, $\varphi(t)$, across different transition states.

the interdiction of maximum flow [7], a method for active and passive defense strategies against multiple attacks on single system elements [25], and a study of interdependent critical infrastructure vulnerability response to targeted attacks [40]. In comparison, this study focuses on single multi-commodity networks and robust decisions to a set of single attacks applicable to the study of real-life infrastructure networks. We are further emphasizing on the degree to which vulnerability (in terms of performance loss) can be mitigated in a robust way by employing an effective defense strategy against probable disruptions with known parameters. The research within this specific field is further addressed in the methodology section.

Given that a planner has some prior knowledge that a network faces a disruptive event with uncertainty, it is assumed that the planner will attempt to insulate, fortify, or otherwise harden the network in a way that minimizes the extent of the disruption (vulnerability reduction). It is assumed that the planner seeks to maintain the flow of commodities—or economic entities flowing through the network—in some way that is equitable or otherwise prioritized. Such a defense strategy would incur some cost to implement. The general approach for this study is to employ a defense strategy at a minimal cost that also minimizes network vulnerability. Prior effort has formalized this multi-objective problem [32], taking into account discrete, diverse "attack" scenarios and offering a solution approach for approximating Pareto-optimality to define an overall robust defense strategy. This study makes use of this approach, extending it for multi-commodity networks. The Pareto-optimal defense strategies are specific to a particular attack (hereafter more generally referred to as "disruption"). To explore strategies that are robust to multiple disruptions, the Pareto-optimal frontiers could be consolidated based on stakeholder opinions of the trade-offs between several criteria, including vulnerability reduction across several disruptions and cost. This study uses a multicriteria decision analysis technique, the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), to address these trade-offs, especially given the possibility of a large, high-dimensional Pareto set to consider.

The goal of this paper is to propose a methodology for making robust decisions for reducing vulnerability in multi-commodity networks under uncertain disruptions. The remainder of this paper is as follows. Section 2 describes the proposed methodology. Section 3 illustrates the methodology with a Swedish rail case study, and Section 4 offers concluding remarks.

2. Proposed methodology

This section discusses the proposed methodology for making robust decisions for reducing vulnerability in multi-commodity networks under uncertain disruptions.

2.1. Single commodity formulation

The network vulnerability reduction formulation proposed here extends that which was given previously for a single commodity [32], described as follows.

Let a network be represented by $G = (N, A)$, where N represents the set of nodes (with source node s and sink node t), and A represents the set of links (or edges) between nodes. The capacity of link (i, j) directed from node i to node j is $q_{ij}(a_{ij})$, where a_{ij} is a binary indicator of disruption equal to 1 if the link is disrupted and 0 if the link is not disrupted. It is assumed that if link (i, j) experiences a disruption, $q_{ij}(1) \le q_{ij}(0)$. The set of (disrupted) capacities across all links is noted as the vector $\mathbf{q}$.

The original formulation considers a set of resources belonging to an adversary divided amongst disruptive events $\mathbf{e}^k \in D$, which further divide those resources so that e^k_{ij} refers to the amount of resources dedicated to disrupt link (i, j) for event k. The set of all disruptive events is D. The network defender is assumed to be aware of possible disruption scenarios, D, but not aware of the specific components and their locality. The defender employs defense strategy $\mathbf{h}^l$ to minimize the vulnerability of the network to disruption $\mathbf{e}^k$, where h^l_{ij} denotes the resources dedicated to mitigate damage to link (i, j) for strategy l.

Linking disruption and defense strategies with the notion of vulnerability is a contest function found in Eq. (1) based on work by Skaperdas [33] and supported by the competing resource strategy by Levitin and Hausken [23]. That is, given disruption k and defense strategy l, the disruptive threat to link (i, j) is the probability that the link's capacity is reduced to zero, represented with $u_{ij}(\mathbf{e}^k, \mathbf{h}^l)$. The exponent m describes contest intensity (which defaults to a value of 1). Note that this contest function is particularly used for attacker/defender scenarios, though it is considered more generally here for disruptions beyond only malevolent attacks where e^k_{ij} could broadly be interpreted as the strength of disruption to link (i, j) and where h^l_{ij} could be a similarly scaled measure of the strength of defense of link (i, j).

$$u_{ij}\left(\mathbf{e}^k,\ \mathbf{h}^l\right) = \begin{cases} \frac{\left(e^k_{ij}\right)^m}{\left(e^k_{ij}\right)^m + \left(h^l_{ij}\right)^m} & \text{if } \left(e^k_{ij}\right)^m > 0 \\ 0 & \text{if } \left(e^k_{ij}\right)^m = 0 \end{cases} \tag{1}$$

When $\mathbf{e}^k$ and $\mathbf{h}^l$ are known, each link's survival probability is assumed to be a random variable with probabilities given by Eq. (2).

$$P\left(q_{ij}\left(a_{ij}\right)\right) = \begin{cases} 1 - u_{ij}\left(\mathbf{e}^k,\ \mathbf{h}^l\right)\ if\ a_{ij} = 1 \\ 1\ if\ a_{ij} = 0 \end{cases} \tag{2}$$

Expected network performance, where φ is defined as source-to-sink flow, can be described as $\varepsilon(h^l,\ e^k) = E[\varphi(\mathbf{q})|\mathbf{e}^k,\ \mathbf{h}^l]$, and network performance is a function of link flow, $f(i, j) \in (0, q_{ij}(0))$. From these definitions, the original formulation is defined as follows. The objectives in