Original Article

Institution of MECHANICAL ENGINEERS
Journal of RISK AND RELIABILITY

Proc IMechE Part O:
J Risk and Reliability
2021, Vol. 235(5) 798–813

DOI: 10.1177/1748006X21991038
journals.sagepub.com/home/pio
SAGE

Community vulnerability perspective on robust protection planning in interdependent infrastructure networks

Hannah Lobban[1], Yasser Almoghathawi[2], Nazanin Morshedlou[3] and Kash Barker[1]

Abstract

Critical infrastructure networks, including water, power, communication, and transportation, among others, are necessary to society's functionality. In recent years, the threat of different types of disruptions to such infrastructure networks has become an increasingly important problem to address. Due to existing interdependencies, damage to a small area of one of the networks could have far-reaching effects on the ability to meet demand across the entire system. Common disruption scenarios include, among others, intentional malevolent attacks, natural disasters, and random failures. Similar works have focused on only one type of scenario, but combining a variety of disruptions may lead to more realistic results. Additionally, the concept of social vulnerability, which describes an area's ability to prepare for and respond to a disruption, must be included. This should promote not only the protection of the most at-risk components but also ensure that socially vulnerable communities are given adequate resources. This work provides a decision making framework to determine the allocation of defensive resources that accounts for all these factors. Accordingly, we propose a multi-objective mathematical model with the objectives of: (i) minimizing the vulnerability of a system of interdependent infrastructure networks, and (ii) minimizing the total cost of the resource allocation strategy. Moreover, to account for uncertainty in the proposed model, this paper incorporates a means to address robustness in finding the most adaptable network protection plan to reduce the vulnerability of the system of interdependent networks to a variety of disruption scenarios. The proposed work is illustrated with an application to social vulnerability and interdependent power, gas, and water networks in Shelby County, Tennessee.

Keywords

Interdependent networks, robust allocation, vulnerability, optimization, multi-criteria decision analysis

Date received: 13 August 2019; accepted: 10 January 2021

Introduction

In the past few decades, regions across the world have been affected by numerous disruptions (i.e. natural disasters and human-made attacks) that result in direct and indirect costs. Many of these disruptions (e.g. the recent devastation of Hurricane Maria on Puerto Rico in 2017) not only cause severe physical damage but also impact society's perception of the government's ability to prepare for and respond to disruptions. An extensive analysis of the costs of such disruptions performed by Al Kazimi and Mackenzie[1] suggests that not only has the average cost risen in recent years but that these costs can reach up to hundreds of billions of dollars. For example, earthquakes are responsible for anywhere from $100 million to $100 billion in losses to both commercial and residential areas.[1] Terrorist attacks, while less common and more frequently localized in terms of target areas, can be just as costly, causing substantial damages.[1] Furthermore, in a recent report for the Department of Homeland Security (DHS), the

[1]School of Industrial and Systems Engineering, University of Oklahoma, Norman, OK, USA
[2]Systems Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
[3]Department of Industrial and Systems Engineering, Mississippi State University, Starkville, MS, USA

Corresponding author:
Kash Barker, School of Industrial and Systems Engineering, University of Oklahoma, 202 W Boyd St, Rm. 124, Norman, OK 73019, USA.
Email: kashbarker@ou.edu

National Consortium for the Study of Terrorism and Responses to Terrorism classifies attacks by target type and shows that 75% of attacks focus on critical infrastructure networks.[2]

From these reports, it is clear that disruptive events pose a significant risk to infrastructure in the U.S. and across the world. Critical infrastructure networks are defined as service and utility networks that are considered necessary for society to function.[3] Critical infrastructure networks include energy, water, transportation, and communication systems, among many others on which all aspects of our society – from the public to government and businesses – depend. With the growth of technology in recent years, the definition of critical infrastructure networks has expanded to include cyber-based systems. Examples of cyber-related advances in power grid networks include software installations in control centers, specialized hardware in substations, and smart elements transformers. While these advances, and the desire to make such networks more efficient, have improved overall functionality, they come at a cost and "have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches" to ensure that both the infrastructure itself and the population in potentially at-risk areas are protected.[3] This problem was stated in the Directive nearly 20 years ago, and it is even more pressing today due to higher levels of interaction and interdependency among different infrastructure networks.

Interdependency can be defined as a "bidirectional relationship between two infrastructure networks through which the state of each infrastructure influences or is correlated to the state of the other."[4] Such a relationship between components of different networks increases the complexity of the network system as a whole. Consequently, damage to a section of one infrastructure network could have far-reaching effects on other networks as high vulnerability in even a small number of components might have significant adverse potential. To combat this vulnerability, a defensive strategy (e.g. fortifying network components, constructing redundant components) that concentrates on susceptible components can be implemented. Such a strategy could help in increasing the overall strength of the infrastructure networks to adapt to the negative impacts of disruptions and recover from them in a timely manner (i.e. to become resilient infrastructure networks[5]).

However, these infrastructure networks do not exist on their own; they exist because society relies upon them to enable economic productivity, health, and a way of life. As such, understanding the broader societal impacts of infrastructure disruptions is important when determining the allocation of resources to reduce infrastructure vulnerability. This is particularly true when different members of the community may experience the same disruption to lifeline services in different ways based on their inability to cope, or their social vulnerability.[6,7]

Complementing recent work in managing and mitigating infrastructure risk,[8–10] this paper aims to provide a decision making framework that can be used to determine the allocation of defensive resources to a system of interdependent infrastructure networks that (i) is robust to a variety of disruption scenarios, and (ii) considers the impact to socially vulnerable groups of the disruption scenarios.

The objectives of the model are to (i) minimize the vulnerability of a system of interdependent infrastructure networks, and (ii) minimize the total cost of the resource allocation strategy (which is comprised of the amount of defensive resources selected to each component and the unit cost of the resource at each component). Moreover, uncertainty is an important consideration in the proposed model as the location and impact of the disruption are derived from a set of disruptive scenarios, thus this paper incorporates a means to address robustness in finding the most adaptable network protection plan to reduce the vulnerability of the interdependent networks.

The remainder of this paper is organized as follows. A background of the problem is presented in the following section with a discussion of relevant previous work. Next, the proposed model formulation is provided with an illustrative example of a real system of interdependent networks in Shelby County, TN. Finally, concluding remarks are given, including some insights for how decision makers might manage a protection plan for a system of interdependent infrastructure networks.

Methodological background

This section discusses some of the prior work in the literature related to our proposed decision making framework as well as how concepts of resilience and social vulnerability are incorporated.

Vulnerability and resilience

In the field of disaster planning and recovery, the term resilience can take on a variety of meanings.[11] Resilience is generally defined as the ability of an entity or system to withstand, adapt to, and recover from a disruptive event in a timely manner.[3] This research employs the framework adapted from Henry and Ramirez-Marquez,[12] depicted in Figure 1 to visualize and measure resilience. Figure 1 illustrates the performance $\varphi(t)$ of the system before, during, and after some disruptive event, noting that resilience is a function of a particular initiating disruptive event. Here, resilience is a function of vulnerability, or the amount that $\varphi(t)$ decreases in the disruption period,[13–15] and of recoverability, or for the trajectory of $\varphi(t)$ that the system takes on to return to acceptable performance.[16–18]

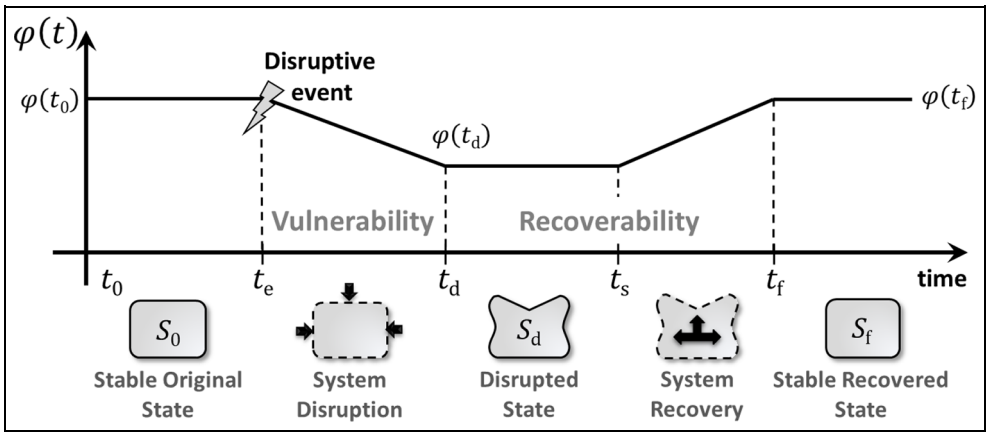

Figure 1. Network performance over time (adapted from Henry and Ramirez-Marquez[12]).

The model proposed here focuses on decreasing vulnerability by enacting preemptive defensive measures prior to the disruptive event (between t_0 and t_e) and is therefore independent of time.

Network protection allocation

Defensive resources refer to equipment and crews that secure and protect network components against malevolent attacks. In power networks, examples of defensive resources include equipment and crews that (i) replace existing transformers with transformers that have more interchangeability across the utility's service territory, (ii) harden transmission lines and towers, circuit breakers, and servers, (iii) restrict the physical accessibility to critical facilities by segregating them into protected zones, and (iv) expand visual barriers, such as tall and opaque defensive fences.[19] For gas networks, these defensive resources may fortify and secure gas pipelines by building redundant counterpart pipeline paths and increase the physical restriction of compressor stations. Finally, defensive resource examples in water networks includes hardening water purification facilities against disruptions, segregating water storage facilities (e.g. reservoirs, water tanks, and water towers), and building redundant water pipes.

A number of works have focused on the allocation of defense resources to reduce the vulnerability of networks. Qiao et al.[20] examine security budgets applied to a water supply network under intentional physical, cyber, or biological disruptions. Assuming the attacker has knowledge of the network and will target components whose disruption will cause the most damage, the defender allocates resources so that the attack will be costly to carry out. Bier et al.[21] propose a computational model to determine the optimal defense resource allocation plan which minimizes the adverse effects of malevolent attacks. Using the measures of target attractiveness (e.g. expected property damage, component criticality, and expected fatalities), their model prioritizes target valuations and allocates the security budget effectively. Mo et al.[22] introduce a dynamic resource allocation strategy that balances protecting existing components and building new ones to increase the redundancy with the goal of minimizing the total disruption to the network. To decrease the probability of network disruption, they consider the most probable attack time, uncertainties of attack time, and disruption probability to evaluate the ability of the network to survive the attack. Using game theory approaches, Zhang et al.[23] propose an analytical equilibrium to study how the risk preferences of the attacker and defender, particularly in allocating defense resources, affect a player's behavior in the equilibrium. In comparison with models that consider the attacker to be risk neutral, this model results in a lower expected disruption, specifically when the attacker is assumed to be risk seeking. Feng et al.[24] introduce a Bayesian game-theoretic method to model different types of attacks, allocate limited resources optimally, and consequently minimize the expected network performance loss. They demonstrate the applicability and efficiency of the model by comparing the expected loss of different defensive strategies. Ramirez-Marquez et al.[25] devise a multi-objective problem that balances network vulnerability and protection resources, finding a Pareto-optimal set of protection strategies for each of several attacks. They then evaluate the effectiveness of each strategy to all other attacks, ultimately ranking all strategies according to their robustness across attacks using a multi-criteria decision analysis technique. McCarter et al.[26] expand upon this idea for multi-commodity networks. Several other works have explored protection allocation models,[27–30] including a review of attack and defense strategy models is provided by Hausken and Levitin.[31]

Interdependent networks

As the importance of studying infrastructure resilience has grown, so too has the literature on the resilience of interdependent infrastructure networks (e.g. Buldyrev

et al.,[32] Buldyrev et al.,[33] Schneider et al.,[34] Holden et al.,[35] Garas,[36] Almoghathawi and Barker[37] and Ghorbani-Renani et al.[38]). Research has also focused on both dimensions of resilience (i.e. vulnerability and recoverability) that are highlighted in Figure 1.

With regard to measuring vulnerability in interdependent networks, as well as strategies to reduce vulnerability, Wang et al.[39] analyze interdependent network responses to different link disruption scenarios and propose a ranking method for protecting critical components. Wu et al.[40] assess the structural and functional vulnerability of interdependent networks with two types of interdependencies: physical and geographical. They demonstrate the applicability of their proposed methodology to a variety of infrastructure networks and disruption scenarios, as well as insights into vulnerability mitigation strategies (e.g. defense resource allocation). Using game theory approaches, Hausken[41] analyzes two interdependent systems to study how the failure of one or both systems may affect defense plans and subsequent attack strategies. Focusing on spatially localized attacks, Ouyang[42] proposed two strategies, including protecting vulnerable components and building new component to increase the redundancy of network, to enhance interdependent network resilience.

A number of recent works have focused on the recoverability dimension of resilience, primarily in modeling work crew assignment and scheduling for restoring interdependent networks.[43–46] As the recoverability dimension of resilience is not the focus of this paper, we highlight only Almoghathawi et al.,[47] as it serves as the foundation for the vulnerability model proposed here, which considers the same resilience quantification approach proposed by Henry and Ramirez-Marquez.[12] Almoghathawi et al.[47] describe a system of interdependent critical infrastructure networks subjected to a range of disruption scenarios, proposing a multi-objective model to determine a restoration strategy (order of disrupted components and schedule of work crews) to restore the networks. They use the ε-constraint method to balance cost and resilience objectives, the latter of which is based on concepts in Figure 1.

Social vulnerability

Measure of social vulnerability often depend on the characteristics of the community under study. Age, level of income, average level of education, population, housing structure, and geographical neighborhood are among the factors that affect the vulnerability of the corresponding community. For example, those with lower incomes often live in mobile homes and poorly constructed houses which are vulnerable to disruptions.[48]

The majority of the works in resilience from a community perspective present a qualitative analysis and the conceptual framework of the dynamics between physical infrastructure networks and the society.[49–52] The concept of community resilience is common among earthquake hazards research,[53–55] though more recent work has explored the difference among community characteristics in other settings.[56] In particular, we focus on resource allocation for protecting interdependent networks with vulnerable populations in mind.

Social vulnerability describes how social factors and inequalities (e.g. economic disparities, access to emergency services, and political representation), affect a community's ability to respond to and recover from some disruptive events.[57] In the context of critical infrastructure systems, socially vulnerable areas are those in which communities may be most negatively impacted by a lack of critical services and resources during times of disruption. Cutter et al.[57] developed a method to assign a quantitative Social Vulnerability Index (SoVI) score across the U.S. by county using 29 demographic, housing, and economic data that are publicly available through the U.S. Census. A simplification of the SoVI method, referred to as SoVI-Lite and developed for the U.S. Army Corps of Engineers, provides a quicker, less technical method for hazard planners.[58] SoVI-Lite also allows for the index to be more easily scaled down to determine scores within smaller geographical units for an individual county and uses a smaller set of variables determined to be the most relevant to the specific region of study.

With regard to the relationship among physical infrastructure networks and society, Cavalieri et al.[59] propose a multi-criteria decision analysis framework that measures the impact of interdependent physical infrastructure network disruptions on social losses, focusing on the displaced population level of that area. Franchin[60] developed a seismic vulnerability hazard to analyze multiple large interacting systems concurrently and their inherent uncertainty. However, the model adopts a fixed and predetermined evaluation sequence. Ellingwood et al.[61] present a virtual community testbed to relate infrastructure networks with a community network, defining natural hazards to which the infrastructure networks are exposed and the population demographics which are required for the assessment of potential post-disruption impacts.

This paper offers an integrated framework to analyze the vulnerability of interdependent physical networks from the perspective of the social vulnerability of the corresponding affected areas. Uncertainty is an important consideration in the model, as it can arise in the presence of a malevolent attack, which could be based on various (and unknown to the defender) motivations (e.g. surrounding population, connectivity of a component, the capacity of the component, random). Therefore, this paper incorporates a means to address robustness in finding the most adaptable network protection planning to reduce interdependent network vulnerability to a variety of disruption scenarios.

Proposed decision making framework

This section provides the variables and parameters for the interdependent networks, the optimization model that aims to minimize the effects of the disruption while

simultaneously minimizing costs, and the robust decision making approach that measures the efficacy of protection strategies for different disruption scenarios (i.e. natural disasters (spatial), random, intentional malevolent attacks (capacity-based and degree-based)). The optimization model of this paper is inspired by the interdependent restoration model proposed by Almoghathawi et al.[47].

Definitions and notation

The mathematical model deals with components in a set K of interdependent networks.N^k and A^k are the sets of nodes and links, respectively, in network $k \in K$. Subsets of N^k in network $k \in K$ include supply and demand nodes, N_s^k and N_d^k, respectively. In network $k \in K$, For node $i \in N_s^k$ in network $k \in K$, the available supply is b_i^k, and for node $i \in N_d^k$, the demand that must be met is b_i^k. Each link from node $i \in N^k$ to node $j \in N^k$ in network $k \in K$ has a capacity of c_{ij}^k. Within the sets of nodes and links, N'^k and A'^k are the subsets of disrupted nodes and links, respectively, in network $k \in K$. The performance of network $k \in K$ is measured by the maximum flow, $\sum_{i \in N_d^k} b_i^k$, that reaches demand nodes. For node $i \in N_d^k$ in network $k \in K$, the reduction from this maximum flow, or slack, is s_i^k and has an associated unit cost of p_i^k. When the flows into the demand node sum to b_i^k, $s_i^k = 0$. The unit cost of allocation resources for a node or a link in network $k \in K$ is q_i^k and r_{ij}^k, respectively. As some of the networks may be more critical to a community's functionality, the importance of network $k \in K$ is represented by μ^k. The importance of network $k \in K$ is defined based on three factors: (i) the number of networks that depend on network $k \in K$, (ii) the level of dependency among network $k \in K$ and other dependant networks (i.e. the number of components in other networks that depends on the operability of components in network $k \in K$), and (iii) the amount of demand that is covered by network $k \in K$ (e.g. total number of residential, commercial, and industrial customers). Moreover, the SoVI rank (i.e. 1, 2, or 3, as discussed in Section 4.1) for demand node $i \in N_d^k$ in network $k \in K$ is represented by v_i^k. Hence, the porposed model considers two weights, which are discussed in Section 3.3 and further in the case study: (i) the importance of network $k \in K$, μ^k and (ii) the social vulnerability of the location around demand node $i \in N_d^k$, v_i^k.

Contest function

As McCarter et al.[26] demonstrate, the vulnerability of a component in a network subjected to some disruption scenario can be found using a contest function. In general, contest functions are used when multiple players exert effort to win a prize. This can include events such as elections, sports games, and military combat.[62] The outcome $\rho \in (0, 1)$ of such a function can either represent the probability that a player wins the prize or the percentage of the prize a player wins, depending on the nature of the prize and event for which the function is employed.[63] Different contest functions have been developed to describe different contest situations. However, considering attacks, or disruptions in general, the two most common contest functions are the ratio form and difference form proposed by Levitin and Hausken.[64] Both forms take as input the amount of disruption and defense resources assigned to a given component. The value of the output is dependent on how the relation between the two amounts is defined in the function; it is either based on the ratio of the disruption and defense inputs or the magnitude of difference between them. The different form of contest functions, shown in equations (1) and (2), is commonly applied to scenarios in which a defender is determining resource amounts to combat an intentional attack but can be used in other defense allocation circumstances (e.g. guarding against natural disasters).

$$u_i^k\left(g_i^k, d_i^k\right) = \begin{cases} \frac{g_i^k - d_i^k}{g_i^k} & \text{if } g_i^k > 0 \\ 0 & \text{if } g_i^k = 0 \end{cases} \quad (1)$$

$$w_{ij}^k\left(h_{ij}^k, f_{ij}^k\right) = \begin{cases} \frac{h_{ij}^k - f_{ij}^k}{h_{ij}^k} & \text{if } h_{ij}^k > 0 \\ 0 & \text{if } h_{ij}^k = 0 \end{cases} \quad (2)$$

This paper considers a set of attack resources, $(\mathbf{g}, \mathbf{h})^{\bar{l}}$, associated with disruptive event $\bar{l} \in \{1, \ldots, \bar{L}\}$, where $\bar{L}$ is the total number of possible disruptive events. Each attack resource is assigned to network components to disrupt them intentionally. Examples of attack resources include the equipment and labor for (i) shooting transmission towers, (ii) sabotaging support bolts in high-power transmission lines, (iii) rupturing natural gas pipelines, and (iv) contaminating service reservoirs in water networks. Vector $\mathbf{g}$ consists of elements g_i^k that refer to the amount of resources assigned to disrupt node $i \in N^k$ in network $k \in K$, and vector $\mathbf{h}$ consists of elements h_{ij}^k that refer to the amount of resources assigned to disrupt link $(i,j) \in A^k$ in network $k \in K$. The defender employs the defense strategy $(\mathbf{d}, \mathbf{f})^l$ to minimize the vulnerability of the interdependence networks, where $l \in \{1, \ldots, L\}$ is the index of the L defense strategies. Similar to attack strategies, $\mathbf{d}$ consists of elements d_i^k that refer to the amounts of resources assigned to protect node $i \in N^k$ in network $k \in K$, and $\mathbf{f}$ consists of elements f_{ij}^k that refer to the amount of resources assigned to protect link $(i,j) \in A^k$ in network $k \in K$.

Shown in equation (1), for each disruptive event $\bar{l} \in \{1, \ldots, \bar{L}\}$, the vulnerability of a node in network $k \in K$, u_i^k, is calculated for some assumed attack (or disruption) resources g_i^k and allocation of defense resources d_i^k if the component is included in that disruption scenario (if the value for the disruption amount is greater than zero). If the node is not disrupted, its vulnerability is zero. Likewise, the vulnerability of a link in network $k \in K$, w_{ij}^k, is a function of attack

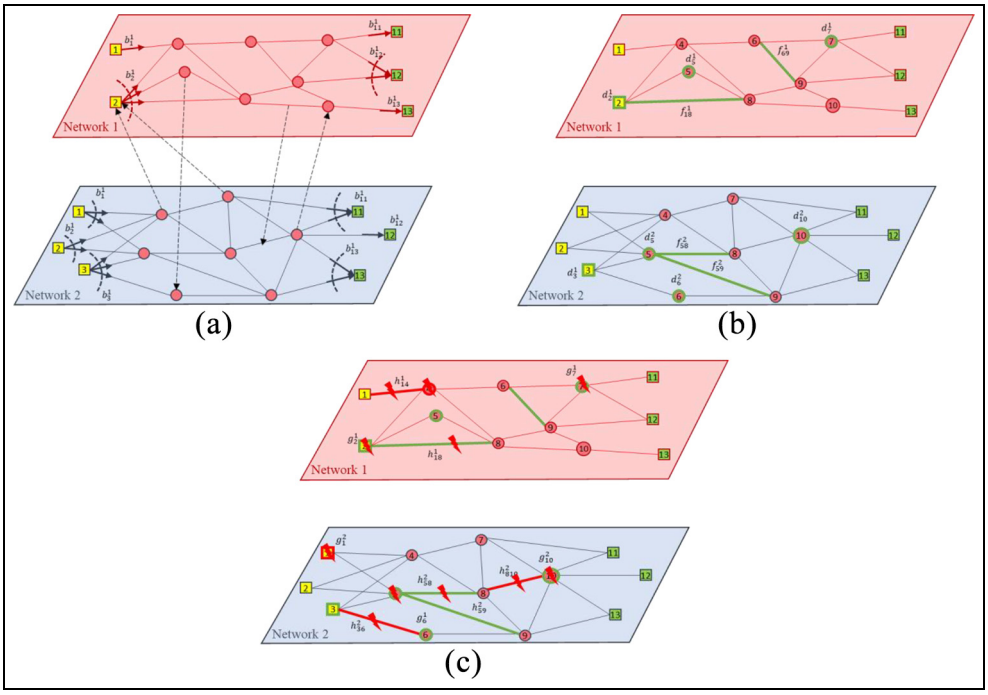

Figure 2. Graphic representation of two interdependent networks: (a) before disruptions, (b) after assigning defense resources, and (c) after attack resources are distributed throughout the networks.

resources h_{ij}^k and defense resources f_{ij}^k is calculated with the contest function in equation (2). If a defender does not allocate any resources to a component it is completely disrupted, and its capacity is reduced to zero. If equal amounts of disruption and defense resources are assigned to a component, the vulnerability is zero, and the component's capacity is unaffected. It is assumed that the defense allocation is no more than the attack allocation. The expected value for a component's functionality in a disruption scenario can be estimated by multiplying its pre-disruption supply by $1 - u_i^k$ for nodes and capacity by $1 - w_{ij}^k$ for links.

Figure 2 is the graphical representation of two interdependent networks before disruption, Figure 2(a), after assigning defense resources, Figure 2(b), and after attack resources are assigned to disrupt nodes and links, Figure 2(c). As Figure 2(a) indicates, in both networks 1 and 2, the flow starts from supply nodes (nodes 1, 2, and 3), distributes through the network, and reaches to demand nodes (nodes 11,12, and 13). The interdependencies among the components of the two networks are shown by the black dashed arrow. The node/link located at the end of the arrow is the one on which other node/link depends. In Figure 2(b), defense resources are distributed through each network to be assigned to nodes and links. For example, in network 1 the amount of defense resources d_2^1, d_5^1, and d_7^1 are assigned to nodes 2, 5, and 7, respectively, and the amount of defensive resources $f_{1,8}^1$ and $f_{6,9}^1$ are assigned to links $(1, 8)$ and $(6, 9)$. As we see in Figure 2(c), the attack resources are distributed through the network to disrupt nodes and links. For example, in network 2, attack resources of amounts g_3^2, g_6^2, and g_{10}^2 are assigned to nodes 1, 6, and 10, and the attack resources of $h_{3,6}^2$, $h_{5,8}^2$, $h_{5,9}^2$, and $h_{8,10}^2$ are assigned to links $(3, 6)$, $(5, 8)$, $(5, 9)$, and $(8, 10)$ to disable them. Mentioned previously in equations (1) and (2), if the amount of defense resources assigned to a node or link (e.g. d_7^1, $f_{5,8}^2$) is equal the amount of attack resources assigned to that corresponding node or link (e.g. g_7^1, $h_{5,8}^2$), that node or link remains unharmed.

Objective functions

There are multiple objective functions of the proposed model. The first objective of the model, shown in equation (3), minimizes the vulnerability in the system of interdependent infrastructure networks, as measured by the weighted unmet demand in the system. Slack s_i^k is weighted by (i) the social vulnerability v_i^k of the location around demand node $i \in N_d^k$ and by (ii) the importance μ^k of network k. The weights encourage defensive resources first to be allocated to susceptible components whose removal would cause the most harm, functionally and socially, in terms of unmet demand. The quantity S in the denominator represents the total amount of weighted demand that is met in the undisrupted scenario.

$$\min \left[\frac{\sum_{k \in K} \sum_{i \in N_d^k} \mu^k v_i^k s_i^k}{S} \right] \tag{3}$$

The competing objective shown in equation (4) minimizes the total cost of the resource allocation strategy

$(\mathbf{d}, \mathbf{f})$, which is comprised of: (i) the amount of defensive resources selected to each of the nodes and links in the disruption scenario, and (ii) the unit cost of the resource at each component.

$$\min\left[\sum_{k\in K}\sum_{i\in N^k} q_i^k d_i^k + \sum_{k\in K}\sum_{(i,j)\in L^k} r_{ij}^k f_{ij}^k\right] \tag{4}$$

Constraints

Constraints (5) through (7) are the flow conservation constraints at each node: the sum of flows out of supply node $i \in N_s^k$ cannot exceed b_i^k, the sum of the flows, x_{ij}^k, out of transition node $i \in N^k \backslash \{N_s^k, N_d^k\}$ must be equal to the sum of the flows, x_{ji}^k, into that corresponding node, and the sum of flows into a demand node $i \in N_d^k$, combined with the amount of slack, s_i^k, at that node must be equal to the demand (maximum performance), respectively. Constraint (8) ensures that the flow across any link is no more than the link capacity. Constraints (9) through (11) consider link capacity for disrupted components whose capacity has been reduced by a disruption, where the flow between nodes i and j cannot be greater than the disrupted performance level of either node, or the disrupted capacity of the link itself. The interdependency of the networks in the system is captured by Ψ as shown in constraint (12), where $\left((i,k),(\bar{i},\bar{k})\right) \in \Psi$ denotes that if node $\bar{i} \in N^{\bar{k}}$ in network $\bar{k} \in K$ depends physically on node $i \in N^k$ in network $k \in K$, then node $\bar{i} \in N^{\bar{k}}$ must be at least as vulnerable as node $i \in N^k$. Finally, constraints (13) through (18) represent the nature of the decision variables.

$$\sum_{(i,j)\in A^k} x_{ij}^k \leqslant b_i^k, \forall i \in N_s^k, k \in K \tag{5}$$

$$\sum_{(i,j)\in A^k} x_{ij}^k - \sum_{(j,i)\in A^k} x_{ji}^k = 0, \forall i \in N^k \backslash \{N_s^k, N_d^k\}, k \in K \tag{6}$$

$$\sum_{(i,j)\in A^k} x_{ji}^k + s_i^k = b_i^k, \forall i \in N_d^k, k \in K \tag{7}$$

$$x_{ij}^k - c_{ij}^k \leqslant 0, \forall (i,j) \in A^k, k \in K \tag{8}$$

$$x_{ij}^k - \left(1 - u_i^k\right) c_{ij}^k \leqslant 0, \forall (i,j) \in A^k, i \in N^k, k \in K \tag{9}$$

$$x_{ij}^k - \left(1 - u_j^k\right) c_{ij}^k \leqslant 0, \forall (i,j) \in A^k, j \in N^k, k \in K \tag{10}$$

$$x_{ij}^k - \left(1 - w_{ij}^k\right) c_{ij}^k \leqslant 0, \forall (i,j) \in A'^k, k \in K \tag{11}$$

$$u_i^k - u_{\bar{i}}^{\bar{k}} \leqslant 0, \forall \left((i,k),(\bar{i},\bar{k})\right) \in \Psi \tag{12}$$

$$s_i^k \geqslant 0, \forall i \in N_d^k, k \in K \tag{13}$$

$$x_{ij}^k \geqslant 0, \forall (i,j) \in L^k, k \in K \tag{14}$$

$$u_i^k \geqslant 0, \forall i \in N^k, k \in K \tag{15}$$

$$w_{ij}^k \geqslant 0, \forall (i,j) \in L^k, k \in K \tag{16}$$

$$d_i^k \geqslant 0, \forall i \in N^k, k \in K \tag{17}$$

$$f_{ij}^k \geqslant 0, \forall (i,j) \in L^k, k \in K \tag{18}$$

The ε-constraint method[65] is used to generate a Pareto set for the multi-objective problem by setting one of the objectives to be at most ε in a constraint, then generating different solutions to the remaining single objective problem by varying the value of ε. The first objective is constrained by a given value of ε representing the maximum allowable vulnerability, as seen in equation (19). While a number of approaches have been proposed to generate a Pareto set,[66] we make use of the ε-constraint method due to its popularity in the multi-objective optimization literature.[67,68] The ε-constraint method has shown to have advantages in generating efficient solutions relative to other approaches (e.g. the weighting method[69]). Further, note that ε represents a tangible value to decision makers, and such tangibility is not always available in other approaches for generating Pareto sets.[70]

$$\frac{\sum_{k\in K}\sum_{i\in N_d^k} \boldsymbol{\mu}^k v_i^k s_i^k}{S} \leqslant \varepsilon \tag{19}$$

Solution robustness

For each disruption scenario, $\bar{l}$, a Pareto set of defense strategies that balance the cost of defense resource allocation and network vulnerability reduction is generated. Once the set of Pareto-optimal solutions has been found for one disruption scenario, each solution is evaluated to determine which is the most robust with respect to all other scenarios regarding maximizing the weighted residual network flow (i.e. flow in the network after a disruption). To evaluate the effectiveness of solutions across the different disruption scenarios, a multi-criteria decision analysis technique is used.

The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS),[71] the multi-criteria decision analysis technique, ranks strategies across M weighted criteria. The TOPSIS formulation is based on the idea of a compromise solution, where strategies are ranked according to how close they are from the best case and how far they are from the worst case. In this implementation, $M = \bar{L} + 1$, representing the vulnerability associated with each attack scenario as well as the cost associated with implementing the strategy. Value y_{lm} represents the evaluation of defense strategy l for the criterion $m \in \{1, \ldots, M\}$.

Because the criteria have different units, the first step of TOPSIS is to standardize the evaluations with a standardization formula[72] like the one shown in equation (20). The standardized value is denoted by α_{lm}.

$$\alpha_{lm} = \frac{y_{lm} - \min_l y_{lm}}{\max_l y_{lm} - \min_l y_{lm}}, \forall m = 1, \ldots, M \tag{20}$$

Next, weights, ω_m, are applied to the standardized values, as shown in equation (21), such that more

important criteria have greater influence on the solution ranking.

$$\beta_{nm} = \omega_m \alpha_{nm} \tag{21}$$

After that, the minimum values of vulnerability and cost evaluations are sought based on the standardized and weighted values obtained by equation (21) Hence, the positive ideal solution (PIS) and negative ideal solution (NIS) are found as the best-case (minimum value in criteria performance) and the worst-case (maximum in criteria performance), respectively, across strategies for each criterion. The formulas for calculating these two values are shown in equations (22) and (23).

$$\begin{aligned} PIS &= \{\beta_1^+, \ldots, \beta_m^+, \ldots, \beta_M^+\} \\ &= \left\{\min_l \beta_{l1}^+, \ldots, \min_l \beta_{lm}^+, \ldots, \min_l \beta_{lM}^+\right\} \end{aligned} \tag{22}$$

$$\begin{aligned} NIS &= \{\beta_1^-, \ldots, \beta_m^-, \ldots, \beta_M^-\} \\ &= \left\{\max_l \beta_{l1}^-, \ldots, \max_l \beta_{lm}^-, \ldots, \max_l \beta_{lM}^-\right\} \end{aligned} \tag{23}$$

In next step, we compare the solutions to both PIS and NIS conditions and sort them according to their similarities to PIS. In other words, for each defense strategy, the best solution has the greatest Euclidean distance from the worst condition (γ_n^-) and the least distance from the best condition (γ_n^+).[73] The distances of each candidate solution to the PIS and NIS are found using the Euclidian distance function in equations (24) and (25).

$$\gamma_l^+ = \sqrt{\sum_{m=1}^{M} \left[\beta_{lm} - \beta_m^+\right]^2} \forall l = 1, \ldots, L \tag{24}$$

$$\gamma_l^- = \sqrt{\sum_{m=1}^{M} \left[\beta_{lm} - \beta_m^-\right]^2} \forall l = 1, \ldots, L \tag{25}$$

The two distance measures are then combined into a single closeness coefficient using equation (26). The coefficients are ranked, and larger coefficients (i.e. larger δ_l^+ values) represent strategies that are closer, based on Euclidean distance, to the PIS and furthest from the NIS. In this way, a compromise solution is sought.

$$\delta_l^+ = \frac{\gamma_l^-}{\gamma_l^+ + \gamma_l^-} \tag{26}$$

Case study: Interdependent networks, Shelby County, TN

This section details an application of the proposed framework on a system of critical infrastructure networks in Shelby County, TN. The interdependent water, gas, and power networks are found in González et al.[44] and illustrated in Figure 3. The set of networks contains a total of 125 nodes and 328 links, with other characteristics found in Table 1. From González

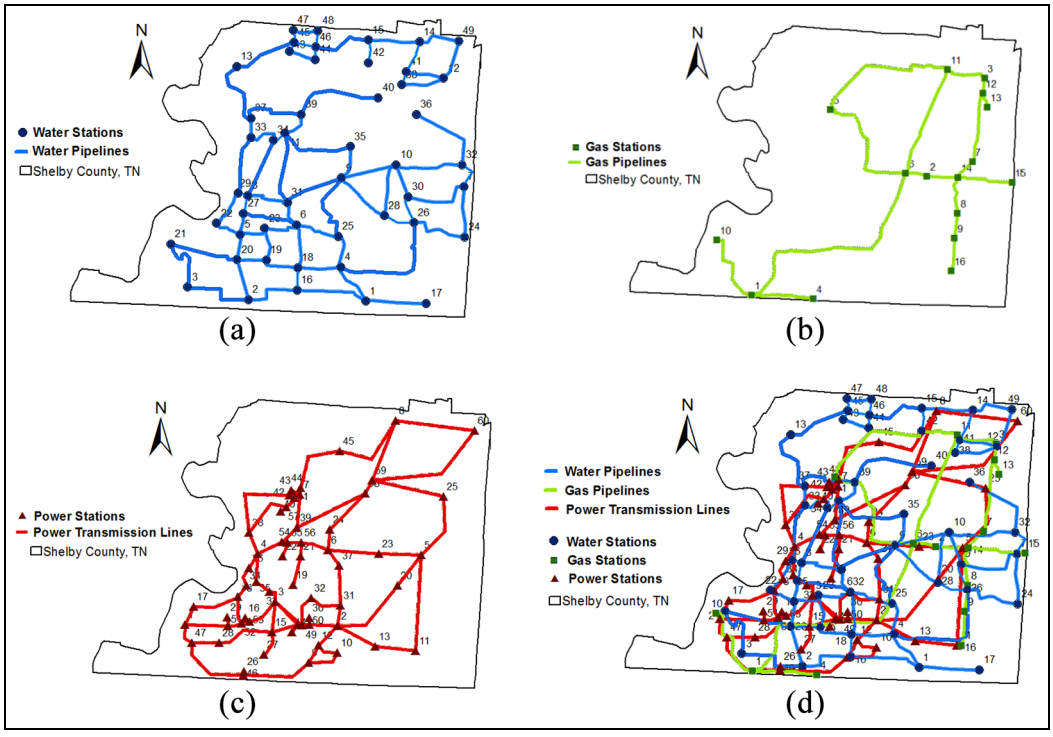

Figure 3. Critical (a) water, (b) gas, and (c) power infrastructure networks of Shelby County, TN and (d) their physical interdependencies respectively (adapted from González et al.[44]).

Table 1. Network properties of the Shelby County networks.

Network	Total nodes	Supply nodes	Demand nodes	Total links	Interdependent links
Water	49	34	15	142	46
Gas	16	2	13	34	0
Power	60	37	23	152	46

et al.,[44] we use the data related to the capacity of supply and demand nodes, the flow capacity of links in each network, and the dependency between components of different networks. Here, supply nodes include generators in the power network, drainage basins and raw water collecting points in the water network, and production stations for the gas network. For demand nodes, we consider final step-down transformers in the power network, service reservoirs in the water network, and liquefied natural gas storage tanks in the gas network. Finally, transmission nodes may refer to transmission substations in the power network, balancing reservoir in the water network, and compressor stations in the gas network. Note that all the links in Figure 3 are assumed to be bidirectional and are counted twice in Table 1. In this paper, we refer to maximum flow as the amount of electricity (in megawatts), natural gas (in cubic feet), and water (in cubic feet per second) that reach respective demand nodes at each time period aligned with the capacity and structure of each of those corresponding networks. There are two significant interdependencies of interest: (i) geographical interdependencies between the water and gas networks knowing that both networks are co-located underground,[44] where two infrastructure networks are geographically interdependent if they are affected by the same local disruptive event,[4] and (ii) physical interdependencies betweenthe water and power networks. In general, the water network depends on the power network for operation and the power network might depend on the water network for cooling and emission control.[74,75] However, for the case study considered in this paper, there exists only a physical dependency between the water and power networks as the water network depends on the power network. Though the proposed model can consider any physical interdependence among infrastructure networks, the gas and power networks are not physically interdependent in the considered case study, as shown in Table 1.

We consider four disruption scenarios, discussed in detail in Almoghathawi et al.,[47] to analyze the performance of the optimal protection strategies: (i) "Spatial," where the attack is based on the population surrounding the network components (e.g. disrupting the power transmission lines or water reservoirs in more populated areas), (ii) "Degree," where the nodes with the highest degree of connectivity are disrupted (e.g. disrupting highly connected electricity transmission substations or natural gas compressor stations), (iii) "Capacity," where the links with the highest capacity are disrupted (e.g. disrupting primary transmission line in power networks, distribution mains in water networks, and refined gas transmission line coming out of refinery plants), and (iv) "Random," where components are disrupted chosen based on random selection. To generate the disruption scenarios, we use Python 27 on an Intel Core™ i7-7500U CPU 2.90GHz (with 32 GB RAM). We also use Gurobi 8.1.0 on Python 27 to solve the multi-objective model optimally.

Social vulnerability by block group

The SoVI scores are calculated at the block group level for Shelby County using the SoVI-Lite methodology that was developed for the Mississippi Valley Region, in which the county resides. For a community that lives in a specific region, a higher level of socioeconomic status (e.g. income, political power) enhances the resilience of that community to disruption (i.e. a decrease social vulnerability by some value), as presumably resources enable it to withstand disruptions and recover from losses quickly. On the other hand, living in rural areas increases the vulnerability due to lower income and more financially dependent on location-based resources (e.g. farming and fishing). Also, living in high-density areas complicates the evacuation process[57]). Due to the high margin of error in US Census data at the block group level, the generalized categories of Low, Moderate, and High social vulnerability (ratings of 1, 2, and 3, respectively), are adopted instead. These ratings are found by standardizing the scores and assigning a rating of 1 to block groups for which the SoVI score is less than -0.5, a rating of 2 to block groups for which the SoVI score is between -0.5 and 0.5, and 3 to block groups for which the SoVI score is above 0.5. The final distribution of social vulnerability in the county, graphically depicted in Figure 4, is 31% block groups with a low rating (i.e. rating of 1), 47% with a moderate rating (i.e. rating of 2), and 22% with a high social vulnerability rating (i.e. rating of 3).

Computational results

The importance of network $k \in K$ was chosen such that $\sum_{k \in K} \mu^k = 1$. Discussed in the previous section, the SoVI rank for demand node $i \in N_d^k$ in network $k \in K$, represented by v_i^k, takes on scores 1, 2, and 3, to represent low, moderate, and high social vulnerability, respectively. It was assumed here that the social vulnerability of the serviced community commanded a higher

Table 2. Cost and slack in disrupted networks with no allocation.

Scenario	Total cost	Vulnerability	Slack		
			Water network	Gas network	Power network
Spatial	$727,000	0.375	238	379	837
Random	$887,000	0.428	148	838	788
Capacity	$1,222,000	0.608	222	1000	1222
Degree	$1,345,500	0.768	921	586	1184

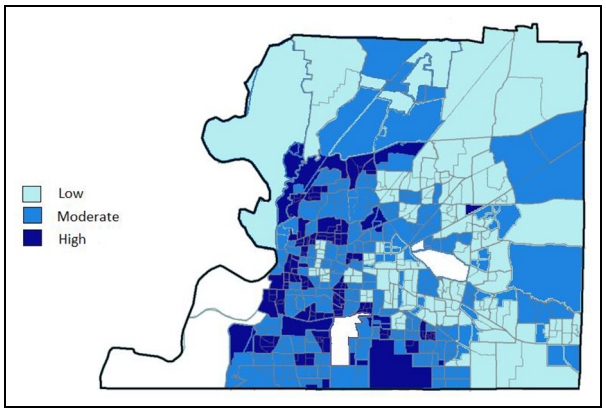

Figure 4. The distribution of social vulnerability indices over the block groups in Shelby County, TN.

weighting value relative to network importance, though any scheme could be used by a decision maker.

Table 2 shows the "no allocation" state for each disruption scenario, where "Total cost" is the sum of: (i) the allocation costs (which have been forced to zero in this run), and (ii) the costs of unmet demands, as shown in equation (27). That is, the first and second terms of equation (27) represent the allocation costs, while the third term represents the cost of unmet demand. To find the system vulnerability, or the weighted proportional slack, caused by a given disruption, the objective function was changed to minimize slack and a constraint to set the allocation amount to zero was added. For the purposes of this case study p_i^k, the cost of unmet demand for each node, was constant across the nodes and networks at $500, while q_i^k and r_{ij}^k, the cost of resource allocation for nodes and links, respectively, were randomly generated from a uniform distribution between $50 and $150.

$$T = \sum_{k\in K}\sum_{i\in N^k} q_i^k d_i^k + \sum_{k\in K}\sum_{i,j\in A^k} r_{ij}^k d_{ij}^k + \sum_{k\in K}\sum_{i\in N_d^k} p_i^k s_i^k \qquad (27)$$

Understandably, the "Spatial" and "Random" disruption scenarios result in lower total costs and vulnerabilities, see Table 2, because the components affected did not necessarily contribute significantly to the performance of the system of interdependent infrastructure networks (i.e. meeting required demand). On the other hand, the malevolent attack disruption scenarios (i.e. capacity-based, "Capacity," and degree-based, "Degree" disruption scenarios) result in higher values for total costs and vulnerability, as shown in Table 2, which indicate the criticality of the disrupted network components to the system of interdependent networks due to their influence on the performance of their individual networks as well as the whole system.

Pareto-optimal solutions. Recall that there are competing objectives representing vulnerability and protection costs, and recall that equation (19) serves as the ε constraint representing the vulnerability objective. We consider 20 values of $\varepsilon \in [0,1]$ for each of the four disruption scenarios, which result in a total of 80 potential solutions (excluding the "do nothing" solution in which no resources are allocated). Thus, a set of Pareto-optimal solutions is obtained, and the resulting Pareto-optimal frontier in Figure 5 shows the competing vulnerability and protection cost values for each of the 20 solutions found for each disruption scenario.

As expected, devoting more resources toward protection would result in lower vulnerability (i.e. weighted proportional slack) in the networks. Figure 5 shows that while the capacity-based disruption scenario has higher costs at the lower values of weighted proportional slack, the degree-based disruption scenario results in the highest costs for the majority of the curve. Moreover, it shows that the spatial and random disruption scenarios result in extremely similar curves, with the former having a lower initial (no-allocation) level of vulnerability and resulting in slightly lower costs. However, the overall shapes of the curves are similar across all four disruption scenarios; at the shallower end of the curve, particularly for degree-based, proportional slack $\geqslant 0.6$, and capacity based, proportional slack $\geqslant 0.5$, disruptions, a decrease in slack can be achieved at a small increase in cost. Furthermore, at the steeper end of the curve, proportional slack $\leqslant 0.1$, a larger expenditure is needed the same percentage decrease in slack, indicating that the decrease may not be worth the additional funds required. From Figure 5, we conclude that protecting the connectivity of the network, regardless of the capacity of protected components, costs more than protecting the maximum flow paths in the network. This means that networks with high levels of connectivity, such as small-world and scale-free networks, are more vulnerable to degree-based attacks and must be protected in hubs with the

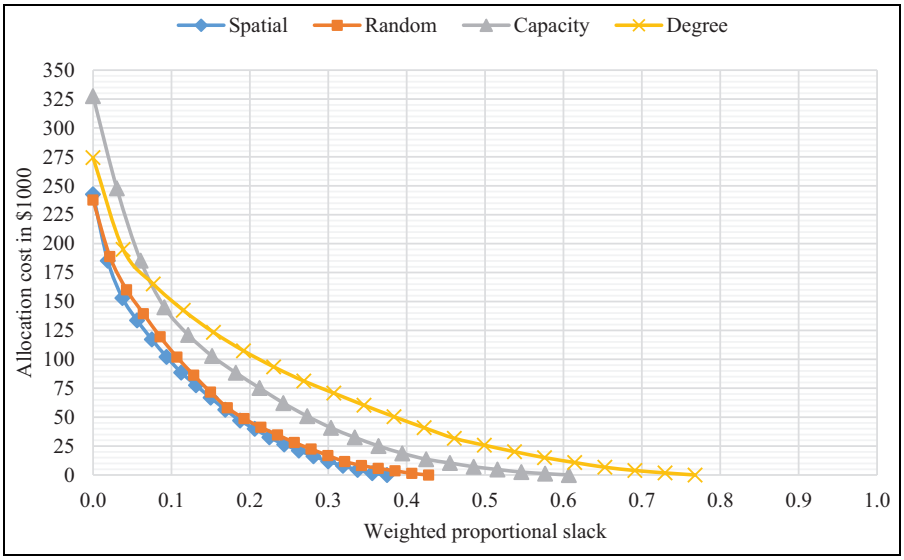

Figure 5. Pareto-optimal frontier for cost and vulnerability objectives.

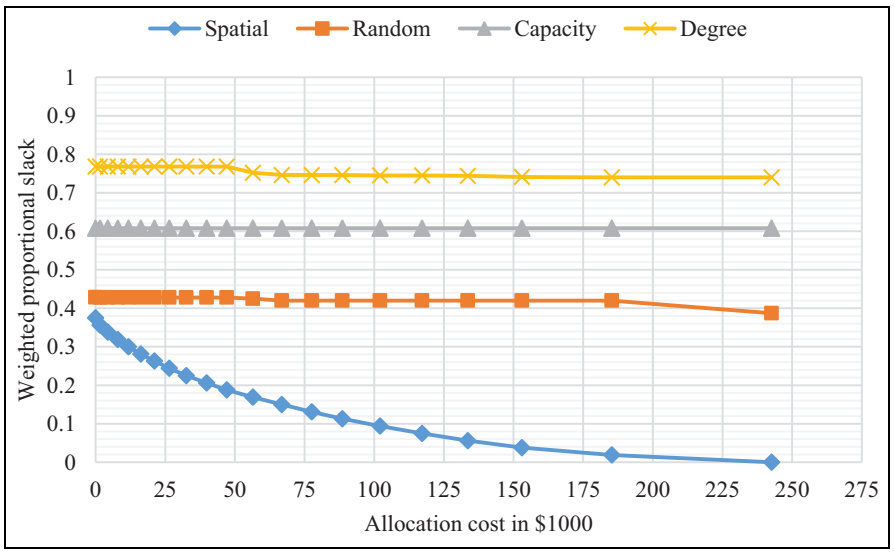

Figure 6. Robustness of spatial scenario solutions on cost and vulnerability objectives.

highest level of degree centrality multiplied by neighborhood connectivity (i.e. the connectivity of neighboring nodes around a given node) of those corresponding hubs. Also, non-hierarchical mesh networks, such as routing and wireless networks, are more vulnerable to capacity-based attacks, and thus protecting maximum flow paths is the most beneficial.

Solution robustness. The allocation amount for each Pareto-optimal solution in each disruption scenario (i.e. spatial, random, capacity-based, and degree-based disruption scenarios) was used as the allocation for each of the other three scenarios to determine how well that allocation would perform in other disruptions. For example, each allocation that produced a Pareto-optimal solution in the spatial scenario was then input into the random, capacity, and degree scenarios to determine how well it reduced vulnerability in the other scenarios. This yielded the evaluation seen in Figures 6 to 9. Figure 6 suggests that the allocation solutions from the spatial scenario are not especially effective for the three other kinds of disruptive scenarios, as the frontiers generated for random, capacity, and degree disruptions are substantially different from the frontier for the spatial scenario. Further, the vulnerability is substantially worse for degree and capacity disruptions with practically no reduction in vulnerability for increasing resource allocation. We see a similar lack of robustness in Figure 7 for the solutions generated by the random scenario. That is, the solutions for the spatial and random disruption scenarios were largely ineffective in terms of robustness. This is likely because these two scenarios do not represented the targeted

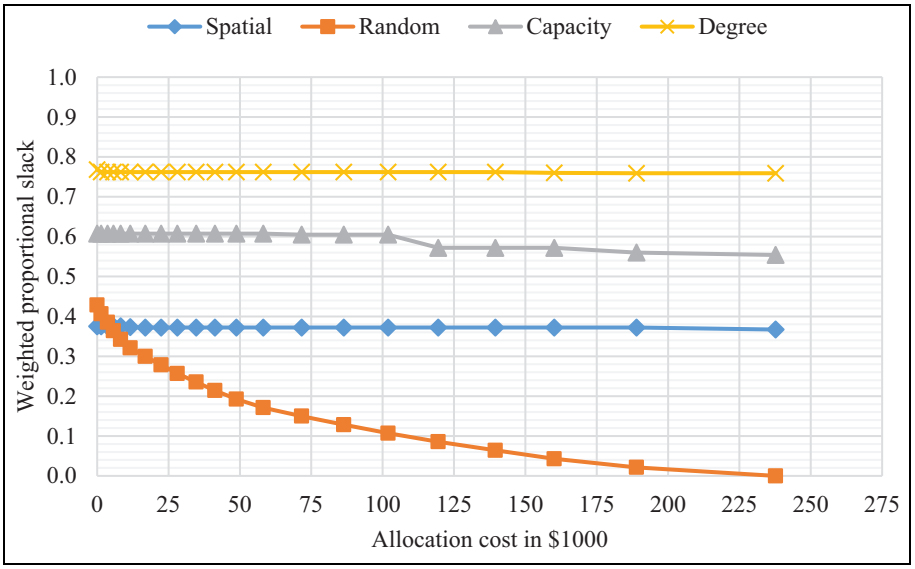

Figure 7. Robustness of random scenario solutions on cost and vulnerability objectives.

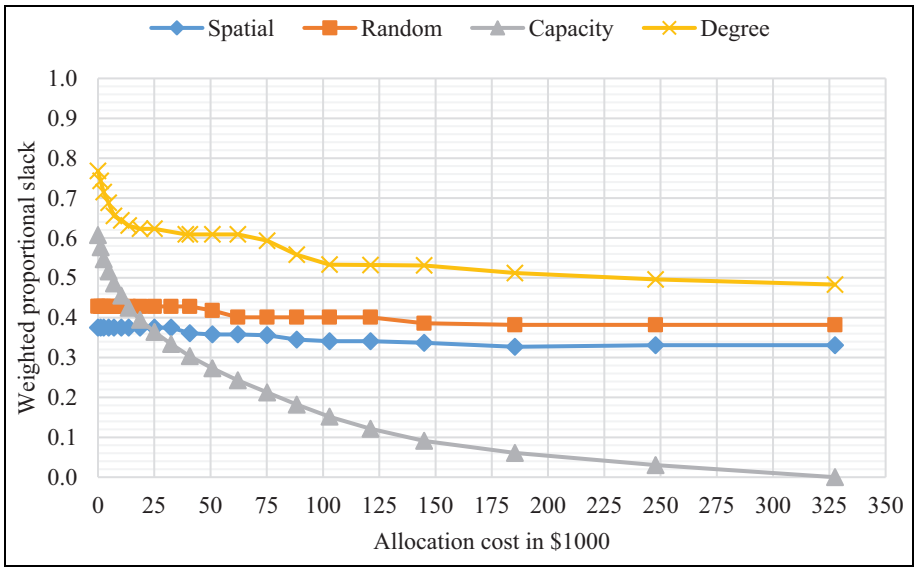

Figure 8. Robustness of capacity-based scenario solutions on cost and vulnerability objectives.

scenarios that the degree and capacity scenarios provide. Planning for degree and capacity-based scenarios, what one might expect from a malevolent attack, show a better ability at reducing vulnerability for the other scenarios as well, as shown in Figures 8 and 9. Based on this particular example, it appears that protection schemes aimed at reducing network vulnerability to a malevolent attack are better at reducing vulnerability for other scenarios as well. Note that the weighted proportional slack level for the other three scenarios on which the solutions are being tested remains steady despite more money being put into defensive allocation, as illustrated in all the figures.

Also, the solutions of the capacity-based disruption scenario, illustrated in Figure 8, offer an improvement over those for the spatial and random scenarios, especially with the degree-based disruption scenario. At an allocation cost of approximately $145,000, when the slopes of the capacity-based and degree-based disruption scenarios begin to level out, the system vulnerability is 0.091 and 0.531, respectively. While the latter is still an undesirably high level of vulnerability, it does show improvement over the initial vulnerability of the system under the degree-based disruption of 0.768, as shown in Figure 8.

Furthermore, with regards to the solution of the degree-based disruption scenario, shown in Figure 9, the spatial and random disruption scenarios are practically entirely unaffected. However, the capacity-based scenario responds to the solutions of the degree-based

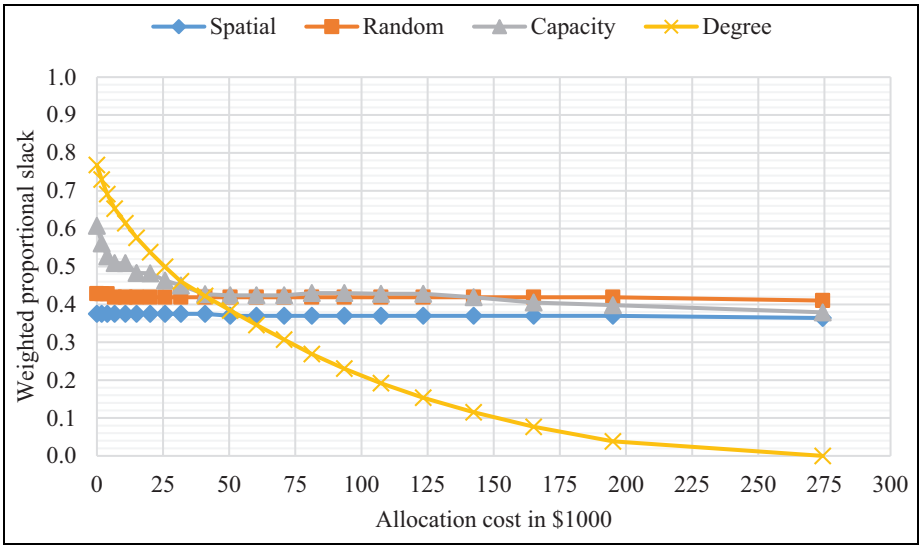

Figure 9. Robustness of degree -based scenario solutions on cost and vulnerability objectives.

Table 3. Top eight solutions based on TOPSIS rankings; strategies are named by the scenario for and the run order in which they were originally solved.

Strategy	S +	Rank	Disruption scenario				Allocation cost
			Spatial	Random	Capacity	Degree	
Cap—17	0.413	1	0.337	0.386	0.115	0.531	$144,936
Cap—18	0.411	2	0.327	0.382	0.077	0.512	$185,290
Cap—15	0.411	3	0.341	0.401	0.192	0.533	$102,886
Cap—16	0.410	4	0.341	0.401	0.154	0.532	$121,103
Cap—14	0.404	5	0.345	0.401	0.230	0.558	$88,355
Deg—18	0.399	6	0.370	0.419	0.405	0.061	$165,102
Deg—19	0.398	7	0.370	0.419	0.398	0.030	$195,028
Deg—17	0.397	8	0.370	0.419	0.419	0.091	$142,405

disruption scenario almost as well as the degree-based scenario did with the capacity-based solutions, see Figures 8 and 9. The vulnerability for the capacity-based disruption scenario drops gradually but consistently from its initial value of 0.608 to 0.424 at a corresponding allocation cost of $50,000 before it plateaus, as shown in Figure 9. This indicates that there may be more overlap in the set of disrupted components between the capacity-based and degree-based disruption scenarios than with the other two disruption scenarios, that is, spatial and random disruption scenarios. From Figures 6 to 9, we observe that degree based protection strategies are more aligned with capacity-based protection plans. Therefore, in cases where financial limitations might not allow the optimal protection of networks with certain levels of connectivity, such as small-world and scale-free networks, a capacity-based protection plan may result in a relatively good solution.

Robustness ranking. Figures 6 to 9 show that the solutions of the capacity-based and degree-based disruption scenarios slightly outperform the solutions resulting from the other two scenarios: the capacity- and degree-based allocations result in a more effective reduction in vulnerability across the other scenarios. This conclusion is confirmed in the TOPSIS evaluation in Table 3, as all the highest ranked defensive strategies are from the solutions of the capacity-based and degree-based disruption scenarios. However, none of the strategies are able to adequately decrease vulnerability across more than one disruption scenario, as shown in Figures 6 to 9. This can likely be attributed to the high distinction between the sets of components targeted; even when assigning defense resources to nodes and links reduces the vulnerability of the network by 90–95%, in comparison to the situation where no defense operation is taken place, for one disruption scenario, indicating that nearly all the disrupted components have sufficient resources, the disrupted components for another disruption scenario remain highly vulnerable.

In the TOPSIS results, the trade-off between reducing slack and reducing cost is seen. For example, the Cap-17 strategy is ranked higher than Cap-18 strategy even though the slack is lower for all four disruption scenarios, as shown in Table 3. The allocation cost in

the latter is too high to justify the relatively small decreases, see Table 3. We also observe the same result for Cap-15 and Cap-16 as the allocation cost in the latter is too high to justify the lower slack it produces against Capacity and Degree disruption scenario. Although the allocation cost plays a critical role in ranking defense strategies, the considerable decrease in vulnerability, between 0.7 to 0.1, prioritizes the defense strategies despite their high allocation cost.

Concluding remarks

In summary, it is difficult to build a robust resilience model that can cover a wide variety of attacks as disruptions may not be predictable and tractable as some natural catastrophes, such as hurricanes and tornados. Nevertheless, our proposed methodology provides a framework for decision makers to compare the effectiveness of allocation strategies for disruptions to a system of interdependent networks. Additionally, the proposed framework offers a way to include social vulnerability into disaster planning and management, which is a crucial dimension that many previous works do not represent. The resilience of both the infrastructure and the community must be incorporated in disaster planning so that the system will be optimally fortified at its weakest points following the occurrence of disruption occurs. While protecting critical infrastructure networks is undeniably important, it is good if they are still susceptible to attack in the areas in which people depend on them most.

In the course of this research, multiple limitations and opportunities for continuing improvements and expansions were identified. First, the overall accuracy of the model can be increased by gaining a better understanding of the component attributes, such as the cost of resource allocation and capacity or demand at each location. Handling the uncertainty of these attributes, and the sensitivity of decisions to this uncertainty, is a topic of on-going effort. Second, different kinds of contest functions, which could be chosen as a result of the empirical study of the effectiveness of defender and attacker resources, could produce different results. Finally, weights based of off the likelihood of each disruption scenario or the stakeholders' preferences for one criterion over another could be incorporated into the TOPSIS calculations. For example, if defenders have estimated that a capacity-based attack is more likely than an earthquake striking a given area (i.e. spatial disruption), the weights used in TOPSIS could reflect such information and influence the higher ranked strategies to include best protected strategies for the network in capacity-based disruption scenarios. Protection-minded decision makers may also consider vulnerability reduction more important than cost, or vice-versa. Even if the probability of disruption is relatively low, there are non-monetary costs, like a decreased sense of security in the public or loss of trust in the government and emergency services, that could occur in the event of an attack or natural disaster. If decision makers are more concerned with these qualitative costs than the quantitative costs of resource allocation, the vulnerability criteria can be weighted higher than the cost criterion to allow strategies with high costs but less damage to the networks to be ranked high. These changes would help represent the reality of the situation more accurately and could incorporate opinions of the community, government agencies, and infrastructure workers.

An important direction for future work is to consider the coverage, closeness, spread, and spacing of non-dominated solutions in the Pareto frontier. These analyses might help to realize how far the results might end up from optimal solutions in non-ideal conditions.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported in part by the National Science Foundation through awards 1541165 and 1635813. Further, the authors gratefully acknowledge the assistance of Ms. Deniz Berfin Karakoc.

ORCID iDs

Yasser Almoghathawi https://orcid.org/0000-0003-0527-4820
Kash Barker https://orcid.org/0000-0002-0142-1558

References

1. Al Kazimi A and Mackenzie CA. The economic costs of natural disasters, terrorist attacks, and other calamities: an analysis of economic models that quantify the losses caused by disruptions. In: *Proceedings from IEEE '16: systems and information engineering design symposium*, Charlottesville, VA, 2016.
2. Miller E. Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015. College Park, MD: START.
3. White House. *Presidential policy directive 21 - - critical infrastructure security and resilience*. Washington, DC: Office of the Press Secretary, 2013.
4. Rinaldi SM, Peerenboom JP and Kelly TK. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Syst Magaz* 2001; 21(6): 1125.
5. Barker K, Lambert JH, Zobel CW, et al. Defining resilience analytics for interdependent cyber physical-social networks. *Sustainable Resilient Infrastruct* 2017;2(2): 59–67.
6. Karakoc DB, Almoghathawi Y, Barker K, et al. Community resilience-driven restoration model for

interdependent infrastructure networks. *Int J Disaster Risk Reduct* 2019; 38: 101228.
7. Karakoc DB, Barker K, Zobel CW, et al. Social vulnerability and equity perspectives on interdependent infrastructure network component importance. *Sustainable Cities Soc* 2020; 57: 102072.
8. Valentin V, Naderpajouh N and Abraham DM. Integrating the input of stakeholders in infrastructure risk assessment. *J Manag Eng*, 2018; 34(6): 638.
9. Thekdi SA and Lambert JH. Quantification of scenarios and stakeholders influencing priorities for risk mitigation in infrastructure systems. *J Manag Eng* 2014; 30(1): 32–40.
10. Lagaros ND, Kepaptsoglou K and Karlaftis MG. Fund allocation for civil infrastructure security upgrade. *J Manag Eng* 2013; 29(2): 172–182.
11. Hosseini S, Barker K and Ramirez-Marquez JE. A review of definitions and measures of system resilience. *Reliab Eng Syst Saf* 2016; 145: 47–61.
12. Henry D and Ramirez-Marquez JE. Generic metrics and quantitative approaches for system resilience as a function of time. *Reliab Eng Syst Saf* 2012; 99(1): 114–122.
13. Johansson J, Hassel H and 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.
14. Ouyang M, Zhao L, Hong L, et al. Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. *Reliab Eng Syst Saf* 2014; 123: 38–46.
15. Rocco CM, Barker K, Moronta J, et al. Community detection and resilience in multi-source, multi-terminal networks. *J Risk Reliab* 2018; 232(6): 616–626.
16. Barker K, Ramirez-Marquez JE and Rocco CM. Resilience-based network component importance measures. *Reliab Eng Syst Saf* 2013; 117: 89–97.
17. MacKenzie CA and Barker K. Empirical data and regression analysis for estimation of infrastructure resilience, with application to electric power outages. *J Infrastruct Syst* 2013; 19(1): 25–35.
18. Morshedlou N, González AD and Barker K. Work crew routing problem for infrastructure network restoration. *Transp Res Pt B* 2018; 118: 66–89.
19. Electric grid security and resilience, establishing a baseline for adversarial threats, June 2016. https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats.
20. Qiao J, Jeong D, Lawley M, et al. Allocating security resources to a water supply network. *IIE Trans* 2007; 39(1): 740–817.
21. Bier V, Haphuriwat N, Menoyo J, et al. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Anal* 2008; 28(3): 763–770.
22. Mo H, Xie M and Levitin G. Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks. *Eur J Oper Res* 2015; 243(1): 200–210.
23. Zhang J, Zhuang J and Jose VRR. The role of risk preferences in a multi-target defender-attacker resource allocation game. *Reliab Eng Syst Saf* 2018; 169: 95–104.
24. Feng Q, Cai H and Chen Z. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. *Reliab Eng Syst Saf* 2017; 191: 105900.
25. Ramirez-Marquez JE, Rocco CM and Barker K. Bi-objective vulnerability reduction formulation for a network under diverse attacks. *J Risk Uncertainty Eng Syst* 2017; 3(4): 04017025.
26. McCarter M, Barker K, Johansson J, et al. A bi-objective formulation for robust defense strategies in multi-commodity networks. *Reliab Eng Syst Saf* 2018; 176: 154–161.
27. Bier VM, Gratz ER, Haphuriwat N, et al. Methodology for identifying near-optimal interdiction strategies for a power transmission system. *Reliab Eng Syst Saf* 2007; 92(9): 1155–1161.
28. Smith JC and Lim C. Algorithms for network interdiction and fortification games. In *Pareto optimality, game theory and equilibria*. New York: Springer, 2008, pp.609–644.
29. Levitin G, Hausken K and Ben Haim H. Active and passive defense against multiple attack facilities. *Asia-Pac J Oper Res* 2011; 28(4): 431–444.
30. Guan P, He M, Zhuang J, et al. Modeling a multi-target attacker-defender game with budget constraints. *Decis Anal* 2017; 14(2): 87–107.
31. Hausken K and Levitin G. Review of systems defense and attack models. *Int J Performability Eng* 2012; 8(4): 355–366.
32. Buldyrev SV, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks. *Nature* 2010; 464(7291): 1025–1028.
33. Buldyrev SV, Shere NW and Cwilich GA. Interdependent networks with identical degrees of mutually dependent nodes. *Phys Rev Pt E* 2011; 83: 016112.
34. Schneider CM, Yazdani N, Araujo NAM, et al. Towards designing robust coupled networks. *Sci Rep* 2013; 3: 1969.
35. Holden R, Val DV, Burkhard R, et al. A network flow model for interdependent infrastructures at the local scale. *Saf Sci* 2013; 53(1): 51–60.
36. Garas A. *Interconnected networks*, New York, NY: Springer, 2016.
37. Almoghathawi Y and Barker K. Component importance measures for interdependent infrastructure network resilience. *Comput Ind Eng* 2019; 133: 153–164.
38. Ghorbani-Renani N, González AD, Barker K, et al. Protection-interdiction-restoration: tri-level optimization for interdependent network resilience. *Reliab Eng Syst Saf* 2020; 199: 106907.
39. Wang S, Hong L, Ouyang M, et al. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Saf Sci* 2013; 51(1): 328–337.
40. Wu B, Tang A and Wu J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. *Reliab Eng Syst Saf* 2016; 147: 1–8.
41. Hausken K. Defense and attack for interdependent systems. *Eur J Oper Res* 2017; 256(2): 582–591.
42. Ouyang M. A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks. *Eur J Oper Res* 2017; 262(3): 1072–1084.
43. González AD, Dueñas-Osorio L, Medaglia AL, et al. The time-dependent interdependent network design problem (td-INDP) and the evaluation of multi-system recovery strategies in polynomial time. In: HW Huang, et al. (eds.) *The 6th Asian-Pacific symposium on structural reliability and its applications*, Shanghai, China, 2016, pp.544–550.

44. González AD, Dueñas-Osorio L, Sánchez-Silva M, et al. The interdependent network design problem for optimal infrastructure system restoration. *Comput Aided Civil Infrastruct Eng* 2016; 31(5): 334–350.
45. Sharkey TC, Cavdaroglu B, Nguyen H, et al. Interdependent network restoration: on the value of information-sharing. *Eur J Oper Res* 2015; 244(1): 309–321.
46. Sharkey TC, Nurre SG, Nguyen H, et al. Identification and classification of restoration interdependencies in the wake of hurricane sandy. *J Infrastruct Syst* 2016; 22(1): 04015007.
47. Almoghathawi Y, Barker K and Albert LA. Resilience-driven restoration model for interdependent infrastructure networks. *Reliab Eng Syst Saf* 2019; 185: 12–23.
48. Flanagan BE, Gregory EW, Hallisey EJ, et al. A social vulnerability index for disaster management. *J Homeland Secur Emerg Manag* 2011; 8(1): 215626.
49. Cutter SL, Barnes L, Berry M, et al. A place-based model for understanding community resilience to natural disasters. *Glob Environ Change* 2008; 18(4): 598–606.
50. Boin A and McConnell A. Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *J Conting Crisis Manag* 2007; 15(1): 50–59.
51. Lindell MK, Prater C and Perry RW. *Introduction to emergency management*. Hoboken, NJ: Wiley and Sons, 2007.
52. Norris FH, Stevens SP, Pfefferbaum B, et al. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *Am J Commun Psychol* 2008; 41(1–2): 127–150.
53. Bruneau M, Chang SE, Eguchi RT, et al. A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* 2003;19(4): 733–752.
54. Chang SE and Shinozuka M. Measuring improvements in the disaster resilience of communities. *Earthquake Spectra* 2004; 20(3): 739–755.
55. Ainuddin S and Routray JK. Earthquake hazards and community resilience in baluchistan. *Nat Hazards* 2012; 63(2): 909–937.
56. Rapaport C, Hornik-Lurie T, Cohen O, et al. The relationship between community type and community resilience. *Int J Disaster Risk Reduct* 2018; 31: 470–477.
57. Cutter SL, Boruff BJ and Shirley WL. Social vulnerability to environmental hazards. *Soc Sci Q* 2003; 84(2): 242–261.
58. Cutter SL, Emrich CT and Morath D. Social vulnerability and place vulnerability analysis methods and application for Corps planning: technical analyses. In: CM Dunning and S Durden. (eds.) *Social vulnerability analysis methods for corps planning*. Washington, DC: Institute for Water Resources: U.S. Army Corps of Engineers, 2011, pp.74–88.
59. Cavalieri F, Franchin P, Gehl P, et al. Quantitative assessment of social losses based on physical damage and interaction with infrastructural systems. *Earthquake Eng Struct Dyn* 2012; 41(11): 1569–1589.
60. Franchin P. A computational framework for systemic seismic risk analysis of civil infrastructural systems. In: G Syner. (ed.) *Systemic seismic vulnerability and risk assessment of complex urban, utility, lifeline systems and critical facilities*. Cham: Springer Netherlands, 2014, pp.23–56.
61. Ellingwood BR, Cutler H, Gardoni P, et al. The centerville virtual community: a fully integrated decision model of interacting physical and social infrastructure systems. *Sustainable Resilient Infrastruct* 2016; 1(3–4): 95–107.
62. Baik KH. Difference-form contest success functions and effort levels in contests. *Eur J Polit Econ* 1998; 14(4): 685–701.
63. Hirshleifer J. Conflict and rent-seeking success functions: ratio vs. difference models of relative success. *Publ Choice* 1989; 63(2): 101–112.
64. Levitin G and Hausken K. Resource distribution in multiple attacks against a single target. *Risk Anal* 2010; 30(8): 1231–1239.
65. Haimes YY, Ladson LS and Wismer DA. Bicriterion formulation of problems of integrated system identification and system optimization. *IEEE Trans Syst Man Cybernetics* 1971; 1(3): 296–297.
66. Chinchuluun A and Pardalos PM. A survey of recent developments in multiobjective optimization. *Ann Oper Res* 2007; 154: 29–50.
67. Klamroth K, Tind J and Zust S. Integer programming duality in multiple objective programming. *J Glob Optimization*, 2004; 29: 1–18.
68. Grandinetti L, Pisacane O and Sheikhalishahi M. An approximate ε-constraint method for a multi-objective job scheduling in the cloud. *Future Generat Comput Syst* 2013; 29: 1901–1908.
69. Mavrotas G. Effective implementation of the è-constraint method in multi-objective mathematical programming problems. *Appl Math Comput* 2009; 213: 455–465.
70. Cooper K, Hunter SR and Nagaraj K. An epsilon-constraint method for integer-ordered bi-objective simulation optimization. In: *Proceedings of the 2017 winter simulation conference*, 2017, pp.2303–2314.
71. Hwang CL and Yoon K. Methods for multiple attribute decision making. In: *Multiple attribute decision making*. New York: Springer, 1981, pp.58–191.
72. Chakraborty S and Yeh C. A simulation comparison of normalization procedures for TOPSIS. In: *Proceedings of the international conference computers and industrial engineering*, Troyes, France, July 6–9, 2009, pp.1815–1820.
73. Hwang CL, Lai YJ and Liu TY. A new approach for multiple objective decision making. *Comput Operat Res* 1993; 20: 889–899.
74. Dueñas-Osorio L, Craig JI and Goodno BJ. Seismic response of critical interdependent networks. *Earthquake Eng Struct Dyn* 2007; 36(2): 285–306.
75. Zhang Y, Yang N and Lall U. Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. *J Syst Sci Syst Eng* 2016; 25(1): 102–118.