2020-10

In search of network resilience: An optimization-based view

Sharkey, Thomas C.; Pinkley, Sarah G. Nurre; Eisenberg, Daniel A.; Alderson, David L.

Wiley

Sharkey, Thomas C., et al. "In search of network resilience: An optimizationbased view." Networks 77.2 (2021): 225-254.
https://hdl.handle.net/10945/67393

Received: 20 December 2019 | Revised: 17 September 2020 | Accepted: 23 September 2020 | Published on: 8 October 2020

DOI: 10.1002/net.21996

SPECIAL ISSUE ARTICLE

WILEY

In search of network resilience: An optimization-based view

Thomas C. Sharkey[1] | **Sarah G. Nurre Pinkley**[2] | **Daniel A. Eisenberg**[3] | **David L. Alderson**[3]

[1]Department of Industrial Engineering, Clemson University, Clemson, South Carolina,
[2]Department of Industrial Engineering, University of Arkansas, Fayetteville, Arkansas,
[3]Operations Research Department, Naval Postgraduate School, Monterey, California,

Correspondence
Thomas C. Sharkey, Department of Industrial Engineering, Clemson University, 263 Freeman Hall, Clemson, SC 29634.
Email: tcshark@clemson.edu

Funding information
This research was supported by the Defense Threat Reduction Agency, Grant/Award Number: DTRA-18681-M. National Science Foundation, Grant/Award Number: CMMI-1254258.

Abstract

Fifty years of research in *Networks* coincides with 50 years of advances in resilience theory and applications. The purpose of this review is to identify how these two technical communities influenced each other in the past and can bolster each other in the future. Advances in resilience theory show that there are at least four ways networks demonstrate resilience: robustness, rebound, extensibility, and adaptability. Research published in *Networks* and by the broader network optimization community has focused primarily on technical methods for robustness and rebound. We review this literature to organize seminal problems and papers on the ability of networks to manage increasing stressors and return to normal activities after a stressful event. In contrast, the *Networks* community has made less progress addressing issues for network extensibility and adaptability. Extensibility refers to the ability to stretch current operations to surprising situations and adaptability refers to the ability to sustain operations into the future. We discuss ways to harness existing network optimization methods to study these forms of resilience and outline their limitations. We conclude by providing a research agenda that ensures the *Networks* community remains central to future advances in resilience while being pragmatic about the limitations of network optimization for achieving this task.

KEYWORDS

adaptability, extensibility, improvisation, rebound, resilience, robustness

1 | INTRODUCTION

Over the last 50 years, the concept of *resilience* has become popular for characterizing behavior in the presence of stress. The current popularity of the term is often traced back to the work of Holling [108], where resilience is presented as a dynamic property of complex systems to, "measure [the] persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables." The term has since been applied to behavior at the level of a system, organization, or individual, and has become increasingly used across a variety of disciplines, including material science, ecology, psychology, emergency management, engineering, and national security (see Park et al. [168] and Seager et al. [192] for a review of the rise in popularity of this term).

There is no single agreed-upon definition of resilience. However, many notions of resilience align with Holling's early definition and refer to the ability of the system to respond or adapt when challenged by stressful events. For example, the National Research Council [152] defines resilience as "The ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events"—a definition that largely follows the five phases of emergency management as defined by the Federal Emergency Management Agency [81]. Similarly, resilience of engineered infrastructure is often defined as the capability of the social and physical systems to respond to threats via a combination of robustness, redundancy, resourcefulness, and rapidity abilities [44] or via absorptive, restorative, and adaptive capacities [87]. Social–ecological definitions of resilience also emphasize the adaptive capacity of complex systems, but further emphasize transformability, learning, and innovation as key aspects of resilience [11, 83]. These and other resilience definitions differ between application domains, where organizational, social, economic, and engineering domains define and study resilience differently [112]. Despite the lack of consensus on what resilience *is* or how to define it, there is common agreement on what it *is not*; the opposite of resilience is commonly termed vulnerability, fragility, or brittleness [221].

In this article, we focus on *network resilience* and the role of optimization models for studying it. Irrespective of definition or application domain, resilience research tends to focus on network representations of systems for demonstrating theory and developing resilience analysis methods. For example, measuring system performance can involve solving a network optimization problem given the current state of the system. Thus, the research published in *Networks* and the community of experts involved in network modeling and analysis offer important contributions for advancing the science of resilience. We focus on the development and application of optimization models—along with corresponding algorithms for solving them—for assessing and improving network resilience.

We hope to provide the audience of *Networks* with an appreciation that a particular optimization model can improve *an aspect* of network resilience and that selecting an appropriate model is important when one wants to "improve network resilience." The scope of this review is on the resilience of physical or cyber-physical systems and how networks can be used to study it. However, research published in *Networks* and by the resilience community extends beyond cyber-physical systems, meaning conclusions drawn from this work may inform broad applications and systems. Furthermore, our scope tends to focus on the underlying models and not, in detail, discussing the solution methods developed to solve the models. We review related literature published in *Networks* and of interest to the readership of *Networks* and discuss how it contributes to the resilience literature. We hope to broaden the ways in which this community views network resilience and provide an understanding of how optimization models fit into broader discussions of resilience. Finally, we outline some of the most promising and important directions for continued research and contribution, especially in areas of resilience that have been under-studied by the *Networks* community.

2 | MAPPING OPTIMIZATION MODELS TO FOUR CONCEPTS OF RESILIENCE

We use the following standard notation throughout. Let $G = (N, A)$ denote a network, where N is the set of nodes (with $n = |N|$) and A is the set of directed arcs (with $m = |A|$). We denote $f(G) = f(N, A)$ as the performance function of network G. In general, we assume the performance of the network is determined from the solution of an optimization problem that achieves the best objective subject to constraints on network operations. For example, $f(G)$ could capture the maximum flow between a source node s and sink node t subject to flow balance constraints and arc capacities. Furthermore, note that we may seek to design the network G in a way to achieve a certain level of performance.

As a start to mapping optimization models to network resilience, we review a common context for how resilience has been defined: (i) there is some set of potential events that stress the system (we purposefully use the term *stress* since an event does not need to disrupt the system), so there are clear pre-event and post-event time frames, (ii) there is some way to measure the performance of the system before, during, and/or after the event, and (iii) there is some method to measure the impact of the set of events (e.g., average impact, worst-case impact, conditional value-at-risk [CVaR] impact). Optimization models can inform network resilience by measuring how $f(G)$ changes due to stress impacting the network structure and its operations. They can also identify operations and design recommendations to overcome vulnerabilities, fragilities, or brittleness. Optimization models of this form often address a single aspect of resilience (e.g., robustness) and, therefore, can be viewed as a "tool" for a very specific resilience purpose. There can also be "multi-headed tools" (e.g., multi-objective models) that allow for an understanding of the tradeoffs between multiple aspects of network resilience. This approach may be helpful when recommendations to improve one aspect of network resilience (e.g., robustness) may conflict with efforts to improve another (e.g., adaptability).

However, because there is no agreed-upon view of resilience, there is no comprehensive way to define a complete tradeoff space. Some aspects of resilience may not be possible to study alongside others due to inherent conflict when defining model primitives, objectives, or constraints. An important role that the *Networks* community can play in resilience research is to expand the set of optimization models available for analyzing aspects of network resilience that emerge from the literature. Moreover, of particular importance are the perspectives that come from practitioners and/or applications that inform when a particular view of resilience might be most relevant.

This concept of using the *appropriate* model for improving an *aspect* of resilience is especially important when the outputs of optimization models are used to recommend network operations. A basic assumption for improving network resilience is that there are decisions that can be made before, during, and/or after a stressful event resulting in a desired system structure or function.

Woods [220] has identified four distinct concepts for resilience that are relevant for networks:

- *Robustness*: managing increasing stressors, complexity, and challenges with limited-to-no impact on normal activities;

- *Rebound*: returning to normal activities after a stressful event;
- *Extensibility*: extending system performance or capabilities to respond to surprise events that challenge current activities; and
- *Adaptability*: managing tradeoffs to build adaptive capacity to continuously evolving contexts.

The fundamental goals and outcomes for networks differ for each resilience concept. Resilience as robustness emphasizes the need for networks to continue to function as intended in lieu of stress. Resilience as rebound emphasizes the need for stressed networks to recover lost function. Resilience as extensibility emphasizes the need for networks to change intended functions to respond to stress. Resilience as adaptability emphasizes the need for networks to balance robustness, rebound, and extensibility capabilities as systems and their environments change. Together, these four concepts, while limited, provide a framework for the way the *Networks* community has influenced resilience research and can approach it in the future.

In examining the literature produced by the *Networks* community, it is clear that it has made valuable contributions to the *robustness* and *rebound* concepts. Therefore, we will take a *retrospective* look at literature in these areas including: fault tolerant and/or survivable network design, two-stage stochastic network optimization problems, interdiction problems, $N-k$ problems, defender-attacker-defender problems, robust network flows and design, problems focusing on reinstalling connectivity into disrupted networks, and network recovery problems. This retrospective look discusses how these problems address resilience within them and/or how they can be used to analyze resilience. In contrast, the *Networks* community has made fewer contributions that progress *extensibility* and *adaptability*. We will take a more *prospective* look at the types of network optimization problems that may advance these concepts.

In the following sections, we review optimization models that inform network resilience. We organize model formulations, analyses, and uses by the aspects of resilience they are meant to improve: robustness, rebound, extensibility, and adaptability. We identify areas of research that the *Networks* community has historically contributed to, and we reveal new avenues of research that require more attention. Where appropriate, we point the reader to existing reviews of network resilience, discuss advances in these areas, and provide a number of critical open areas for future research. We conclude with open issues and questions meant to provoke future advances on network resilience in the *Networks* community.

3 | OPTIMIZATION MODELS AND NETWORK ROBUSTNESS

In this section, we focus on network optimization models to analyze resilience as *robustness*. Resilience as robustness is understood as the ability of the system to continue to function as intended in lieu of stress. In the networks context, stress is often studied as perturbations in the properties of the network or its operational context. Common examples of network perturbations include removing network components or changing the supply/demand levels and capacities of network components. Less common examples of network perturbations that can also be used to study resilience as robustness include changing network objectives without changing decision variables (e.g., minimizing dropped demand vs minimizing operator costs). In all cases, the goal of robustness is to maximize or maintain minimum intended function before, during, and after network perturbations.

In analyzing resilience as robustness, we need to define the set of all potential perturbations to the network, which we denote as $\mathcal{P}$. We view a perturbation $p \in \mathcal{P}$ as a change in the input parameters associated with network $G = (N, A)$, where these changes could impact the supply/demand of the nodes, capacities/costs of the arcs, or the physical structure of the network. For example, if u_{ij} for $(i,j) \in A$ characterize initial arc capacities, a perturbation p could be a vector $\epsilon \in \mathbb{R}^m$ where the arc capacities are now $u_{ij} + \epsilon_{ij}$. A perturbation p may change the network structure by removing a subset of nodes and arcs from it, that is, $p = (N', A')$ where, typically, $N' \subseteq N$ and $A' \subseteq A$. Note that, without loss of generality, we can focus solely on the removal of arcs in the network in a perturbation since a node can be modeled as two nodes and an arc between them. Example perturbation sets include: (i) $\mathcal{P} = \{(N, A') : A' \subseteq A\}$, that is, it contains all possible scenarios that remove a subset of the arcs, (ii) $\mathcal{P} = \{(N, A') : A' \subseteq A \text{ such that } \sum_{(i,j)\in A'} b_{ij} \leq B\}$, that is, there is a cost of removing an arc (i, j) from the network and we are concerned with all perturbations that satisfy a budget constraint on arc removals, or (iii) for network (N, A) with initial parameters (c, u, b), where c_{ij} represents the flow costs of the arcs, u_{ij} represents the arc capacities, $b(i)$ represents the supply/demand of the nodes, $\mathcal{P} = \left\{(N, A) \text{ with } (c + c^\epsilon, u + u^\epsilon, b + b^\epsilon) : c^\epsilon \in [c^\epsilon_{\min}, c^\epsilon_{\max}], u^\epsilon \in [u^\epsilon_{\min}, u^\epsilon_{\max}], b^\epsilon \in [b^\epsilon_{\min}, b^\epsilon_{\max}], \text{ and } \sum_{i\in N} b^\epsilon_i = 0\right\}$ where each range contains 0, that is, we consider all possible perturbations of network parameters within the defined ranges.

Once the perturbation set is defined, determining how we measure the impact of the perturbation on the network, the types of decisions that can be made surrounding these stressful events, and the objectives or requirements for these decisions, will lead to different classes of network optimization problems. The impact may be measured as the expected impact over all perturbations (based on their likelihood of occurrence) or the worst-case impact over them. We may or may not be able to make decisions in order to prepare the network for the perturbation and thus mitigate its impact on the network. In general, the status of the network after the perturbation could be based on both our preparation decisions and the perturbation. In other words, we can change the impact of a perturbation by these preparation decisions, for example, ensuring that arc (i, j) remains operational no matter the perturbation. It may be relevant to improve robustness with these preparation decisions (typically under a budget) or to understand the level of investment needed to guarantee certain criteria are met across the set of perturbations (e.g., with probability $1 - p$, performance will remain above a threshold).

3.1 | Resilience as robustness in optimization models

We proceed by outlining network optimization literature that incorporates aspects of resilience as robustness. Here, we outline how resilience as robustness can be analyzed through the use of existing network optimization models.

3.1.1 | Survivable network design and fault tolerance problems

Survivable network design and fault tolerance problems focus on designing networks so that a minimum number of (typically node or arc disjoint) "structures" exist (call this number) within the network. These problems ensure that the network is *robust for this structure* against perturbations that remove up to $k - 1$ network components. In this case, if the perturbation set is focused on removing nodes, we have $\mathcal{P}_N = \{(N', A') : N' \subseteq N, A' \subseteq A, (i,j) \in A'$ implies $i \in N'$ or $j \in N'$, and $|N'| \leq k - 1\}$ where $p \in \mathcal{P}_N$ provides a set of nodes and arcs to remove from the network in the perturbation. If the perturbation set focused on removing arcs, we have $\mathcal{P}_A = \{(N, A') : A' \subseteq A$ such that $|A'| \leq k - 1\}$. Kerivin and Mahjoub [126] review the literature on survivable network design problems where an $s - t$ path is considered the "structure." The *node (arc) survivable network design problem* is then defined to build a least cost network that has at least k node (arc) disjoint paths between s and t. This ensures that there remains an $s - t$ path for any perturbation that removes up to $k - 1$ nodes, that is, in any $p \in P_N$ (or up to $k - 1$ arcs, i.e., in $p \in \mathcal{P}_A$), thus ensuring that an $s - t$ path robustly operates across a large number of perturbations.

We now consider a number of papers that have built upon the survivable network design problems reviewed by Kerivin and Mahjoub [126]. Bendali et al. [31] provide a branch-and-cut algorithm for the k-arc survivable network design problem (note that they call this problem the k-edge connected network design problem). Chimani et al. [56] provide integer programming formulations based on graph theory for $k = 0,1,2$-node survivable problems. Fortz et al. [84] examine a branch-and-cut method for 2-arc survivable problems that requires no arcs are included in a cycle of more than a certain length. Huygens et al. [115] study a branch-and-cut method for the extension of the 2-arc survivable network design that bounds the length of the paths to L (or "hops" taken by the path). Diarrassouba et al. [64] consider integer programming formulations for the k-arc problem with $L = 3$ hops. Botton et al. [37,38] examine Benders decomposition approaches for these problems with general k and L parameters. Balakrishnan et al. [23] propose large-scale solution methods that integrate decomposition, tabu search, and optimization to solve general survivable network design problems. Gouveia and Leitner [100] examine a survivable network design problem that focuses on path lengths and requires that a path exists between s and t of length less than or equal to H_{st} pre-perturbation and a length of most H'_{st} after $k - 1$ arcs are removed. Terblanche et al. [208], Ljubić et al. [137], and Matthews et al. [143] have studied stochastic survivable network design problems where not all design data are known initially.

Survivable network design and fault tolerance problems are closely related to one another; we refer the reader to Al-Kuwaiti et al. [2] for a discussion on the similarities and differences between fault-tolerance, reliability, and survivability in the context of communications and computer systems. Within the *Networks* journal, fault tolerance is often used to describe more general structures (or required operations) beyond $s - t$ paths. Liestman [134] examines fault tolerance of calling schemes for broadcasting messages in networks. Farrag and Dawson [79] and Dawson and Farrag [63] examine fault tolerance as it relates to preserving star configurations in networks. Harary and Hayes [102] survey results for fault tolerance with structures including cycles and various types of trees.

An important area of application for survivable network design and fault tolerant problems is designing and operating resilient telecommunications networks. This may require not only designing survivable networks but also in routing post-perturbation to maintain system operations. There are several special issues of *Networks* that focus on resilient telecommunications networks. Rak and Sterbenz [175] describe the contributions made by papers in the issue "Optimization Issues in Resilient Network Design and Modeling." Jonsson et al. [122] describe the contributions made by papers in the issue "Design of Resilient Communications Networks." Rak et al. [176] describe the contributions made by papers in the issue "Resilience of Communication Networks to Random Failures and Disasters." We refer the reader to these overviews for a more detailed discussion of the papers; here we provide a high-level categorization of the papers across these special issues.

Silva et al. [199], Canale et al. [47], Sen et al. [195], Canale et al. [48], Martins et al. [141], Ghedini et al. [92], Barbosa et al. [25], Castillo et al. [50], Lin and Zhou [135], and Vass et al. [212] analyze problems in survivability, reliability, or fault-tolerance for different required structures and/or operations. Kucharzak et al. [129], Fouquet et al. [86], Yang et al. [225], Cheng et al. [54], Myslitski et al. [150], Busing et al. [45], and Natalino et al. [151] examine novel post-perturbation routing or path selection protocols. Houthooft et al. [114], Papadimitriou and Fortz [167], Gomes et al. [97], Hmaity et al. [107], Girão-Silva et al. [94], and Kalesnikau et al. [123] consider problems that integrate network design or operations pre-perturbation with effective routing post-perturbation. Ali et al. [8] and Pasic et al. [169] examine methods to identify locations of failures after a disruption.

3.1.2 | Two-stage stochastic network optimization problems

Stochastic network optimization problems, such as network design, are broadly focused on making decisions in the face of uncertainty about the operating conditions of the network. We could view each potential operating scenario as belonging to the set of perturbations in examining how these problems build in aspects of resilience as robustness. Therefore, there is no standard way to define $\mathcal{P}$ for these problems although it is standard that there will be a probability (likelihood) of a particular perturbation. Two-stage stochastic problems would make decisions prior to the perturbation being revealed (i.e., first-stage preparation decisions) and then can make perturbation-specific decisions once it is revealed. Any two-stage network design problem where we are seeking to optimize the expected performance of the network across all perturbations (or other measures, like CVaR) or seeking to minimize design costs to ensure some level of post-perturbation performance can be viewed as addressing resilience as robustness. Note that the latter viewpoint is similar to that of survivable network design problems.

The literature on stochastic network optimization problems is vast and review papers typically focus on a specific application area [101,203,204]. Work within the *Networks* journal that addresses these types of problems may not specifically *mention* resilience, but it contributes to the area nonetheless. We will highlight a number of contributions from the journal and then discuss specific application areas.

In *Networks*, Atamturk and Bhardwaj [16] consider the problem of minimizing the cost of installed edges into a network so that the maximum flow is above a certain level with probability $1-\varepsilon$, where the capacities of the installed arcs are random variables. Although the paper does not specifically *mention* resilience, it is addressing a problem to ensure that network performance is robust across a wide set of perturbations (the realized arc capacities).

Crainic et al. [59], and its follow-up paper Rahmaniani et al. [174], examine how to solve a multicommodity, capacitated network design problem with stochastic demands using metaheuristics and Benders decomposition, respectively. The perturbations are defined based on the demands of nodes and the problem seeks to minimize the sum of the pre-planning costs (including the costs associated with building arcs) and the expected transportation costs after the perturbation occurs. By applying different weights to the pre-planning costs and the transportation costs, it would be possible to use their work to understand the tradeoffs between preparing for the perturbation and in the post-perturbation network performance.

Rysz et al. [180] consider a general class of problems which seeks to detect a "structure" (e.g., a clique) in a network with a certain property prior to the perturbation so that the structure can be repaired quickly after the perturbation to maintain this property. In other words, they seek to identify a portion of the network so that the property is quickly re-established after any perturbation. This type of problem is one where robustness includes a measure as to how the system rebounds (Section 4) from the perturbation. The papers of Heath et al. [103], Tan et al. [206], Aslan and Çelik [15], Sanci and Daskin [185], and Fang et al. [76] consider similar two-stage problems where the robustness is measured based on how well the system rebounds after the perturbation and include decisions modeling the rebound process.

There have been literature reviews that focus on stochastic network optimization problems for specific applications. Snyder [203] provides a review of facility location problems under uncertainty. In these problems, the location of the facilities is often the first-stage decisions and perturbations can be used to capture the uncertainty about facility capacities, demands, and connection costs to customers. These problems contribute to analyzing resilience as robustness for applications that can be modeled within the various classes of facility location problems. Grass and Fischer [101] provide an overview of two-stage stochastic programming in disaster management, with a specific focus on reviewing papers that are related to pre-positioning humanitarian aid within a network as well as providing an overview of solution methods. Snyder et al. [204] broadly examine supply chain planning under disruptions, and many of its referenced papers fall into how to design supply chain networks when faced with perturbations of their characteristics. Hosseini et al. [113] classify how different pre-perturbation decisions within a supply chain network impact its ability to handle (or recover from) the perturbation.

Specific papers that focus on designing resilient supply chains include [89,140,155,210]. Margolis et al. [140] examine a multi-objective network design problem that assesses the tradeoffs between design costs and the post-perturbation connectivity of the supply chain. Ni et al. [155] examine a two-stage problem where the second stage specifically accounts for losing customers in the supply chain due to disruptions after the perturbation. Gao et al. [89] propose a conic programming approach to identify the optimal inventory positioning policy for problems concerned with minimizing the CVaR of lost sales. Tucker et al. [210] study two-stage and multi-stage stochastic problems that seek to limit drug shortages and provide incentives to certain suppliers to improve the overall resilience of pharmaceutical supply chains.

Faturechi and Miller-Hooks [80] review methods to quantify the resilience of transportation infrastructure and discuss the role of two-stage optimization problems in this area. For power grid resilience, Wang et al. [215] provide a review and discussion of the types of pre-event and post-event strategies that can improve resilience; these can be modeled in two-stage problems to improve the robustness of power grid networks. It is also important to note that infrastructures are increasingly interdependent [44,162] and network models have been created to understand the performance of interdependent infrastructures [132]. In this area, Fotouhi et al. [85] examine two-stage problems for robustness of interdependent traffic and power systems.

3.1.3 | Interdiction problems

Network interdiction problems focus on situations where an attacker will select the perturbation to the network in a way that most impacts its performance and then a defender will operate the network, post-perturbation. These problems study resilience as robustness by helping to understand the worst-case impact of a perturbation to network operations. Typically, the perturbation set is defined by a feasible region of which arcs can be removed (as noted previously, this, without loss of generality, can model node removals); for example, if the arc removals follow a budget constraint, then $\mathcal{P} = \left\{(N, A') : A' \subseteq A \text{ such that } \sum_{(i,j)\in A'} b_{ij} \leq B\right\}$, where A' is the set of arcs removed from the network.

This type of problem has been studied extensively within the *Networks* community; in fact, a virtual issue of the journal is available that highlights contributions of the following papers: Alvarez et al. [9], Bayrak and Bailey [30], Cullenbine et al. [61], Israeli and Wood [118], Janjarassuk and Linderoth [120], Pan and Morton [165], Salmerón [181], and Shen and Smith [198]. We refer the interested reader to the review of Smith and Song [202] for an extensive discussion of interdiction problems, solution methods, and applications.

Two fundamental network interdiction problems are the max flow interdiction and shortest path interdiction. The max flow interdiction problem typically focuses on perturbations that remove arcs from the network so that the total arc removal costs did not exceed a budget. The shortest path interdiction problem typically focuses on perturbations that increase the length of arcs, subject to a budget. The study of these problems within the *Networks* community has helped to inform resilience analysis done by a wide range of communities and we will touch upon some of this work later in this section.

Research on the max flow network interdiction problem (MFNIP) can be traced back to the work of Wollmer [216], McMasters and Mustin [145], and Ghare et al. [91]. The seminal work of Wood [217] renewed interest in the MFNIP and set the stage for how network interdiction can be used to understand the vulnerabilities of infrastructure systems and defend them from disruptions [42]. Research on the shortest path network interdiction problem can be traced back to the work of Fulkerson and Harding [88] and Golden [96] with an impactful paper being Israeli and Wood [118], published in *Networks*.

An important extension of interdiction problems that can offer a different viewpoint on resilience is one that considers asymmetric information. Information asymmetry refers to the situation where the attacker and defender may have different information about the network; for example, the attacker may not understand the supply/demand, capacities, or costs of arcs in the network. This framework would be important in examining resilience as robustness for networks that may be attacked by malicious actors who only have partial information. We refer the reader to the works of Bayrak and Bailey [30], Salmerón [181], and Baycik and Sullivan [28] for examples of interdiction under asymmetric information. An important aspect of analyzing these problems is whether or not the attacker can learn information about the network that they initially did not have. Borrero et al. [35,36] consider learning in the context of network interdiction and show that greedy and robust learning policies will eventually match the interdiction decisions of an attacker with perfect information. Pay et al. [171] examine problems where the defender's risk preferences can be expressed using utility theory and are learned by the attacker. Interdiction with learning falls into the broader class of dynamic interdiction problems (see, e.g., [193,194]). We refer the reader to Smith and Song [202] for more details.

Interdiction problems have been applied to specifically understand the robustness of different types of infrastructure networks. There are a number of papers seeking to understand resilience as robustness of the power grid. For example, the papers of Salmerón et al. [183,184] and Salmerón and Wood [182] examine interdicting power grid networks, where the operations of the grid are modeled using the direct current (DC) flow constraints. Wang and Baldick [214] present more detailed analysis on the consequences of an interdiction in terms of both short (minutes) and near term (days) impacts. Rocco et al. [179] assess the vulnerabilities of a power grid and Zhang et al. [228] examine how to fortify supply systems against deliberate attacks.

In terms of applying interdiction to understand the resilience as robustness of transportation systems, many different transportation modes have been considered. Laporte et al. [131] examine designing robust passenger railway transit systems. Murray-Tuite and Fei [149] examine the impact of smart attacks on the travel times between origin-destination (O-D) pairs in a road transportation network. Gedik et al. [90] examine interdiction problems where the network is modeled based on operating principles of coal freight trains.

In terms of other civil infrastructure systems, the work of Jeong et al. [121] focuses on modeling the post-attack operations of a water infrastructure. Baycik and Sharkey [27] use interdiction to understand the damage done to a set of infrastructures with dependencies between them. This is based on the work of Baycik et al. [29] that examined interdicting networks where there was both an information layer (e.g., the supervisory control and data acquisition of an infrastructure) and a physical flow layer (the infrastructure), and disruptions in one could spread to the other.

3.1.4 | $N - k$ problems

The $N - k$ problem seeks to understand whether or not there exists a perturbation that removes up to k arcs from the network and causes it to fail, that is, its performance drops below a certain level. It contributes to analyzing resilience as robustness by determining if the network will be operational should or fewer components be disrupted. Mathematically, the set of perturbations is defined as $\mathcal{P} = \{(N, A') : A' \subseteq A \text{ such that } |A'| \leq k\}$, that is, we can remove up to k arcs from the network.

This problem has been extensively studied in power grids and is of practical importance since grids are often designed to not fail in the $N - 1$ setting. The book of Bienstock [33] provides an extensive discussion of how optimization can be used to examine vulnerabilities of the power grid.

From an optimization perspective, Bienstock and Verma [34] provide new models and formulations for the $N - k$ problem in power grids. Schumacher et al. [191] present approaches to address $N - k$ planning problems in the presence of line-switching that are capable of solving problems with $k = 1, 2$ for networks with up to 96 nodes. Sundar et al. [205] consider a version of the $N - k$ problem where they seek to find a set of k arcs whose removal has the highest weighted impact, where the weight corresponds to the probability that those k arcs will fail and the impact measures the loss in performance.

Wang et al. [213] examine a robust optimization framework for the unit commitment problem under $N - k$ contingency constraints and provide a decomposition framework that can solve problems with 118 buses (nodes). Kaplunovich and Turitsyn [125] utilize heuristics common in constraint programming to identify critical contingencies for the $N - 2$ problem and their methods scale to 300 node networks. Ding et al. [65] and Faghih and Dahleh [74] examine bilevel optimization models that compute a $N - k$ contingency plan which maximizes the probability it occurs times its load loss. Kim et al. [127] offer decomposition approaches to solve more general interdiction problems on power grids than $N - k$ problems, where their work is able to model power grid operations using the alternating current (AC) flow equations. Liu et al. [136] propose a simulation-optimization approach for the $N - 1$ problem that recognizes that a simulation may need to be run to determine if the system fails when a certain component is removed.

3.1.5 | Defender-attacker-defender problems

Defender-attacker-defender (DAD) models are problems that incorporate three stages of sequential decision making: (1) the *defender* first protects certain network components prior to a perturbation, (2) an *attacker* selects a feasible perturbation to the network in a way that most impacts its performance, and (3) the *defender* then selects decisions so that the network operates as best as possible after the perturbation. DAD models incorporate resilience as robustness into optimization models by focusing on preparing the network, pre-perturbation, so that its worst-case performance, post-perturbation, is as good as possible. For example, if the operations of the network seek to maximize flow, then the defender prepares the network by protecting components as to maximize the *minimum* max flow across all possible perturbations. Typically, the perturbation set is focused on imposing arc removals in the network that satisfy the attacker's budget, that is, $\mathcal{P} = \{(N, A') : A' \subseteq A \text{ such that } \sum_{(i,j) \in A'} b_{ij} \leq B\}$ where b_{ij} is the cost of removing arc (i, j), although a more general set of constraints could dictate the feasible perturbations. Note that the initial defense decisions can protect an arc from being disrupted, that is, (i, j) will be in the network even if $(i, j) \in A'$ in the perturbation (although attacking a protected arc would be suboptimal for the attacker). DAD models build off network interdiction problems by incorporating the protection decisions.

Brown et al. [42] discuss the role that DAD models play in defending critical infrastructure and apply a DAD model in protecting a power network. Alderson et al. [4,5] discuss decomposition schemes for solving DAD models. The DAD framework has been applied to several different types of networks including the power grid, transportation systems, supply chains, telecommunications, and interdependent infrastructures. We now discuss some examples in each of these areas; see additional examples in Alderson et al. [5].

Alguacil et al. [7] examine minimizing load shed in a power grid where the operations are modeled using the DC model. Yuan et al. [227] offer a constraint and column generation approach to a similar problem of Alguacil et al. [7]. Ding et al. [66] extend the analysis of DAD models for power grids to the situation where there is uncertainty in the impact of the efforts of the attackers. Ouyang and Fang [164] examine not only the immediate performance of the network after the perturbation but also on how the network recovers over time for both the DC power grid model and a generic max flow network.

Alderson et al. [6] examine highway transportation systems where the operations of the network are based on routing between O-D pairs and travel times are nonlinear functions of congestion. Sarhadi et al. [186] offer a decomposition-based heuristic for a DAD model that examines protecting components within a rail-truck multi-modal transportation network.

In terms of supply chains and facility location, Church and Scaparra [57] and Scaparra and Church [188] examine fortifying q facilities, of p initial facilities, so that the worst-case perturbation of removing r non-fortified facilities is as good as possible, where the inner problem connects a demand point to the closest operational facility. Liberatore et al. [133] examine an extension of the problem where the number of lost facilities (r) is unknown to the defender during the first stage. Bao et al. [24]

consider facility location problems in the DAD framework where the defender can protect facilities initially and then determine a combination of customer reassignments and repairs to disrupted facilities to best recover from the perturbation.

Nicholas and Alderson [156] apply the DAD framework to telecommunications infrastructure by considering the fast design of wireless mesh networks so that they are robust to worst-case jamming attacks.

Ouyang [163] examines DAD models where the operations involve multiple interdependent networks and the flows in one depend on the flows in another. For example, if power was out to a substation, then certain components within the water network would no longer be available. Ghorbani-Renani et al. [93] examine DAD models for interdependent networks that specifically capture the rebound process after the perturbation. We refer the reader to the review of Ouyang [162] that discusses modeling approaches for interdependent infrastructures. Fang and Zio [78] offer an alternative framework to that of Ouyang [163] which also involves a tri-level optimization problem but the outer problem focuses on the probabilistic impacts of a natural hazard and then an adjustable robust optimization problem is examined to capture preparation decisions prior to the actual perturbation.

3.1.6 | Robust optimization and networks

Robust optimization deals with selecting decisions that perform well across all perturbations within an *uncertainty* set. For example, a very conservative uncertainty set could define the perturbation set as: $\mathcal{P} = \{(N, A) \text{ with } (c + c^\epsilon, u + u^\epsilon, b + b^\epsilon) : c^\epsilon \in [c^\epsilon_{\min}, c^\epsilon_{\max}], u^\epsilon \in [u^\epsilon_{\min}, u^\epsilon_{\max}], b^\epsilon \in [b^\epsilon_{\min}, b^\epsilon_{\max}], \text{ and } \sum_{i \in N} b^\epsilon_i = 0\}$ where (c, u, b) are the initial parameters of network (N, A). This uncertainty set allows all parameters to change simultaneously which may be overly conservative; the more common budgeted framework [32] would only allow a fixed number of parameters (say K) to be different from their initial parameters (i.e., we only consider perturbations in $\mathcal{P}$ with K or fewer parameters of the form c^ϵ_{ij}, u^ϵ_{ij}, and b^ϵ_i are nonzero).

Robust optimization can incorporate resilience as robustness into optimization models by ensuring that decisions made pre-perturbation perform well under all perturbations within the uncertainty set and has been applied to understanding flows through a network and/or in designing networks when there is uncertain data about the network. For example, Bertsimas and Sim [32] examine robust network flow problems including a robust version of the minimum cost flow problem where the uncertainty set focuses on perturbations of the costs. This problem could be applicable to situations where the flow decisions are difficult to alter and we seek to be robust against changes to the flow cost structure. As another example, Atamturk and Zhang [17] examine robust network design and flow problems where the design decisions are selected prior to demand realization and then flow decisions can be made as recourse once demand is revealed. This problem falls under the general area of adjustable robust optimization; see Yanıkoglu et al. [226] for a review.

In general, robust network design problems would contribute to studying resilience as robustness. Within *Networks*, Ordonez and Zhao [160] examine a problem that determines how to expand capacities of a network and route flow along the arcs to be robust to uncertainty about flow costs and supply/demands within the network. This model essentially requires flows to be static (fixed) prior to the uncertainty being revealed. One could consider a problem with fully adjustable flow decisions; however, this model may be intractable. Poss and Raack [172] examine robust network design where the flows must follow affine recourse, that is, the flow may be adjusted based on the realized demand in a way that is an affine function of the demand. Aissi and Vanderpooten [1] examine bi-objective robust network design problems (with static flow decisions) that consider both cost and quality-of-service within the network.

3.2 | Using optimization models to analyze resilience as robustness

Fundamental network optimization models can be used to analyze resilience as robustness since these models can provide insights into the post-perturbation performance of the system. For example, the operations of the network may be modeled by solving a maximum flow problem. In order to understand the expected impact of a stressful event, we can apply a sampling strategy over the set of perturbations and solve the maximum flow problem for each generated perturbation. It should be noted that if the number of perturbations is large, then this may not be computationally effective and advanced sampling strategies may be necessary. In general, the model should be carefully constructed in order to provide the insights into the desired characteristics of the system and its limitations should be carefully understood [72].

For example, Brown et al. [42] discuss how interdiction and DAD models can be applied to understand the vulnerabilities of infrastructure systems, including petroleum reserve supply chains and electric power grids. Alderson et al. [5] provide a detailed overview of how to use DAD models to study infrastructure resilience. This detailed approach includes how to model the network operations (the inner problem), the applicability of classic network optimization problems as the inner problem, and how the types of protection options should be modeled for infrastructures including the power grid, highway transportation systems, and undersea communications systems.

The examples of Brown et al. [42] and Alderson et al. [5] focus on more strategic (long-term) decisions to improve resilience. Alternatively, optimization models can also factor in a combination of short-term preparations and long-term planning to improve resilience. For example, the work of Bynum et al. [46] and Zhao et al. [229] considers a combination of long-term decisions (e.g., transmission system hardening and generator procurement) and short-term decisions (dispatch) to improve the resilience of power networks.

4 | OPTIMIZATION MODELS AND NETWORK REBOUND

In this section, we focus on network optimization problems that can be applied to analyze resilience as rebound. Resilience as rebound focuses on "bouncing back" or returning network performance to normal (or an acceptable level) after the stressful event. Unlike robustness, which emphasizes the design and operation of networks that continue to function in the presence of stress, rebound focuses on the design and operation of networks that restore function after stress. To achieve this rebound, network performance is restored by updating the properties of the network after the event. This could be accomplished by repairing damaged components in the network, installing new components into the network, and/or allocating the necessary resources to provide such services.

After a stressful event, a network could experience many different types or combinations of impacts. First, the stressful event could damage the network topology by causing a subset of the arcs and/or nodes to be either fully or partially non-operational. As was indicated in Section 3, without loss of generality, we can focus solely on the operational status of arcs. When arcs are either operational or non-operational, the impact from a stressful event can be modeled by indicating a set $\overline{A} \subseteq A$ as the subset of arcs that are initially non-operational. When arcs can be partially non-operational, we can, instead, associate a continuous parameter β_{ij} with arc $(i, j) \in A$ to indicate the level of impact from the stressful event. In this context, β_{ij} could impact the function of each arc, through, for example, changes to the arc capacity (i.e., $\beta_{ij} \in (0,1)$ where the arc capacity is $u_{ij}\beta_{ij}$) or restoration processing time (i.e., $\beta_{ij} \in [0, 1]$ models the impact and where the restoration processing time is $(1 - \beta_{ij})p_{ij}$).

A stressful event could also impact the parameters or resources necessary to operate the network at a normal level. For example, the supply at specific nodes could be reduced due to disruptions caused in other interdependent networks. Furthermore, the resources (e.g., humans) could be reduced based on their ability to reach the necessary locations for conducting tasks to operate the network. Additionally, immediately following a stressful event, there is often uncertainty about the operational status of the components of the network which would impact the types of optimization models used for rebound. For example, in rebounding civil infrastructure networks from natural hazards, assessment activities of damage may not be able to be implemented immediately after the event to gather necessary information about the status of the network. How a stressful event impacts a network often influences what actions are taken to enable it to rebound.

We proceed by first outlining the current network optimization literature that studies resilience as rebound. Next, we outline how resilience as rebound can be analyzed through the use of optimization models. We then summarize how this network optimization literature has impacted resilience literature outside of the *Networks* community.

4.1 | Resilience as rebound in optimization models

To date, the most studied aspect of resilience as rebound within our community is network restoration optimization models. Typically, network restoration optimization models seek to update the network topology by selecting a subset $\widehat{A} \subseteq \overline{A}$ of the non-operational components to repair. How the network performance is evaluated influences the selection of the subset $\widehat{A}$, or, equivalently, the associated changes to the network topology. We can view the selection of $\widehat{A}$ as network design decisions. These selected network design decisions are often scheduled over time in order to quickly restore the services provided by the network or, equivalently, have the network "rebound." Resources are then allocated to implement these network design decisions. For example, in infrastructure restoration, work crews can be viewed as resources that are allocated to rebound the network. In a slightly different context, rebound can also be modeled as updating the network parameters and/or resources needed to operate the network. Specifically, the supply nodes in a network might not be damaged but could generate or require additional supply amounts (e.g., if the commodities are patients, new relief supplies).

The effectiveness of network rebound can be measured in many ways. Decision makers could set a service level they are seeking to achieve in their rebound efforts and want to minimize the time needed to meet or exceed it. Rebound could be measured as the cumulative weighted network performance over time, where performance is specific to the type of network (e.g., shortest path values between key locations, maximizing the flow through the network to meet demand). As a single network is often not the only impacted system after a stressful event, rebound could be measured as services flowing through a set of networks. Lastly, when uncertainty is present, decision makers could seek to maximize the expected performance over different uncertainty scenarios.

4.1.1 | Optimization models with rebound as establishing connectivity

Repairing network components to establish or reinstate network connectivity between key nodes in the network is one common network performance metric. Averbakh [18] and Averbakh and Pereira [20] look to optimize the total recovery time of nodes for problems with single and multiple servers (i.e., work crews, construction crews), respectively. A node is recovered when there is a path between a central depot and the node, which is equivalent to saying connectivity has been established between the node and the depot. When considering multiple servers, Averbakh [19] seeks to minimize the time the last node is recovered, that is, the makespan required to rebound the network. Averbakh and Pereira [21] seek to minimize the maximum lateness and minimize the number of tardy jobs when each node has a due date for its desired recovery.

Other researchers have focused on connectivity between all pairs of nodes. After assigning each pair of nodes a restoration due date, Averbakh and Pereira [22] look to minimize the maximum lateness of connecting all node pairs. For interested readers, Mattsson and Jenelius [144] review vulnerability and resilience of transportation systems, which often focus on connectivity between O-D pairs. Additionally, Çelik [52] provides a review wherein the infrastructure restoration and network construction classifications are most similar to establishing network connectivity. This review also considers the idea of establishing connectivity in debris clearance, debris collection and disposal, and snow removal.

For applications such as debris clearance, resources (e.g., work crews) can only move on network components which are connected to their current location. In this case, the set of arcs available for movement (i.e., connected) at a particular point in time depends on the set of tasks completed by or before this time. Furthermore, arcs that can be cleared next (to increase the overall network connectivity) are limited to those currently reachable, that is, only if a path has been established from the current location of the resource to the arc in consideration for clearance. When in a deterministic environment, Ulusan and Ergun [211] route work crews to remove debris in a transportation network. Çelik et al. [53] also route debris removal work crews through a transportation network, but consider that there is an uncertain amount of debris that must be removed on each arc.

4.1.2 | Optimization models with rebound as network flow measures

We now examine literature that uses network flow problems to measure performance in studying resilience as rebound. These network flow problems have included the shortest path, max flow, min cost flow, minimum spanning tree, and multi-commodity flow problems. Our focus here is on papers that advance theory or methodology of interest to the *Networks* community. This rebound literature focuses not just on how the network performs at a single point in time, but how the performance changes over time due to the completion of rebound-focused tasks. Thus, many problems consider aspects of scheduling rebound tasks and the cumulative performance of a network over time as tasks are completed. Network performance at time t is then based on the network after the stressful event and all tasks completed by time t.

Incremental network design problems consider restoring/installing non-operational arcs into a network over time as the rebound-focused tasks. In these problems, each non-operational arc takes one period to install and has an installation cost; during each period t there is a budget B^t limiting the total cost of arcs installed. Within this framework, Baxter et al. [26] seek to minimize the cumulative shortest path performance, Engel et al. [73] seek to minimize the cumulative value of the minimum spanning tree, and Kalinowski et al. [124] seek to maximize cumulative flow. Matisziw et al. [142] look to restore network components to balance the multi-objective problem of maximizing cumulative flow between O-D node pairs and restoration costs.

Nurre et al. [159] introduce the class of integrated network design and scheduling problems (INDS) which both selects which network components to restore/install and schedules the restoration/installation by assigning the selected arcs to resources (e.g., work crews) and sequencing the tasks over time. Contrary to incremental network design problems, INDS problems do not assume that each restoration task takes one time period and instead associates a restoration processing time p_{ij} to each non-operational arc (i, j). In this context, a non-operational arc can represent an arc damaged due to a stressful event or an arc not from the original pre-event network but one which embodies an element of extensibility, which once installed improves the network's performance. Nurre et al. [159] select and schedule arcs in an INDS problem to maximize the cumulative maximum flow. Nurre and Sharkey [157] consider a broader range of INDS problems which consider different network performance metrics. Specifically, Nurre and Sharkey [157] consider maximizing flow, minimizing the average shortest path length between O-D pairs, minimizing the maximum shortest path length between O-D pairs, minimizing the cost of a spanning tree, and minimizing the flow cost as network performance metrics. As in prior work, they consider optimizing the cumulative network performance but also consider minimizing the time it takes to achieve a desired input network performance value (e.g., restoring 80% of the lost flow).

Research in this area has progressed to not just considering restoring arcs damaged by a stressful event, but installing new arcs to improve the resulting network performance. Similar to Nurre et al. [159], Fang and Sansavini [75] consider both repairing damaged components and installing new components to minimize two objectives: the negative of the maximum flow and the investment cost of system restoration. The authors impose an antifragility constraint where the total cost of restoration (repairing selected damaged components + installing selected new components) must not exceed the total cost to repair all damaged components.

These types of models have also been applied to specific infrastructure networks, especially the power grid. Arab et al. [12] consider both the uncertainties surrounding mobilizing repair work crews prior to an event and the deterministic recovery of a power network. Tan et al. [207] consider restoration scheduling in the context of a distribution system within the power grid. Researchers also focus on the recovery of the power grid [190] by considering economic impacts [13]. In addition, Bao et al. [24] have examined the recovery of facilities as part of a DAD model for protecting facilities (see Section 3.1).

4.1.3 | Optimization models with rebound as centering/coverage measures

Next, we focus on rebound papers which consider measures, such as centering or coverage, typically used in location problems to evaluate network performance. Iloglu and Albert [116,117] seek to minimize the cumulative weighted distance between the location of emergency responders and calls for service (at demand nodes) over time. This research considers both repairing the network topology with work crews but also uses an extension to the *P*-median problem to dynamically relocate the emergency responders at nodes over time. Thus, both locations for emergency responders and connections between the established locations and demand nodes must be established throughout the duration of the problem.

Arulselvan et al. [14] consider the incremental connected facility location problem which determines facilities to open and assigns customers to open facilities over time in order to minimize total costs. This work ensures that once a customer is assigned to a facility it maintains an assignment to an open facility and that a minimum coverage of customers is met.

4.1.4 | Optimization models with rebound for interdependent networks

Stressful events do not often solely impact a single network, but instead cause stress to multiple networks within an interdependent system. Traditionally in an interdependent system, the state of one network *depends* on another network [178]. Thus, there is a growing body of knowledge which focuses on quantifying resilience as rebound for systems of interdependent networks. Cavdaroglu et al. [51] consider an INDS problem for interdependent networks. The selection and scheduling decisions are made in order to minimize a function of the flow costs, unmet demand costs, and restoration/installation costs. Building on this work, Sharkey et al. [196] incorporate new restoration interdependencies, as defined in Sharkey et al. [197], which link not just the operations of interdependent networks but also how the restoration efforts across systems are linked. They examine how centralized and decentralized decision making environments, representing different levels of coordination between networks, impact restoration. Smith et al. [201] also consider decentralized restoration planning for interdependent networks using a sequential game theoretic approach. With an input restoration budget limiting the resources used, González et al. [98] determine which network components should be restored for an interdependent system. González et al. [99] examine different recovery operators for interdependent infrastructure that were created through dynamic models. Goldbeck et al. [95] consider interdependent networks where the relationship between network flow and infrastructure assets (e.g., electric transformers, metro stations) is modeled. They capture logic dependencies, asset utilization dependencies, resource input dependencies, and also stochastic failure propagation dependencies. Loggins et al. [138] have created interdependent restoration models that account for social infrastructure that rely on civil infrastructure systems. Ghorbani-Renani et al. [93] examine rebound for interdependent networks as the inner problem within a DAD model. For a comprehensive overview of work related to interdependent networks, we point the reader to Ouyang [162].

4.1.5 | Optimization models with rebound under uncertainty

In order to address the uncertainty associated with the stressful event in resilience as rebound models, researchers have used two-stage stochastic programming, two-stage robust optimization, and online optimization.

Using two-stage robust optimization, Álvarez-Miranda and Pereira [10] consider a traditional network design problem in the first stage, and a network construction problem in the second stage. The uncertainty in the system is characterized by the necessary construction resources (e.g., cost, time) for a network design policy. Aslan and Çelik [15] formulate a two-stage stochastic program for a multi-echelon humanitarian response network. In the first stage of their model, they determine where to locate warehouses and preposition relief items. In the second stage, subject to uncertainties in the operational status of distribution centers, operational status of transportation arcs (e.g., travel times, repair times), and relief item demand, they determine the restoration of arcs to open transportation routes and the shipment of supplies through these routes. In addition, the papers of Heath et al. [103], Sanci and Daskin [185], and Fang et al. [76] consider similar two-stage problems where the first stage helps to design the network and the second stage considers how the network rebounds from the disruptive event. Fang and Sansavini [77] consider how to select and schedule restoration tasks for an infrastructure network when faced with uncertain repair times and resources. In the first stage, they select which components to repair and in the second stage, they determine which selected components are scheduled to be repaired over time. These decisions are made to maximize the expected percentage of damaged flow that has been restored.

Often uncertainties associated with stressful events are hard to forecast and predict. Online optimization, which reacts to the arrival of new information over time, is one way to overcome this challenge. Nurre and Sharkey [158] consider an INDS problem where the time when it is safe to restore/install an arc is uncertain and revealed over time. They create new online optimization algorithms which dynamically select arcs to repair/install and schedule them with work crews based on this dynamic arrival of new information and benchmark them against a best case deterministic model with all information known.

4.2 | Using optimization models to analyze resilience as rebound

In addition to incorporating aspects of resilience into optimization models to capture rebound, optimization models can be used to assess rebound. For example, one could run different what-if scenarios by changing the input network data set, the stressful event, and/or the model parameters/resources. The results from these what-if scenarios can then be used to deduce insights about how such a model is appropriate for informing resilience as rebound. Miles et al. [147] discuss the importance of modelers (and models) in building the community of disaster recovery researchers, which serves as an important opportunity for the *Networks* community.

For example, analysis can be used to incorporate improvised restoration options in terms of rebound focused activities. For example, instead of solely looking to repair damaged network components, researchers have considered the installation of temporary components. After the 2001 World Trade Center (WTC) attack, temporary shunts were used to restore the electric power network in lower Manhattan [146]. These shunts were temporary power lines laid down on city streets and protected by wooden boxes. We can capture such decisions by examining the installation of arcs from the set A_I not originally in the network, that is, $A_I \cap A = \emptyset$. The foundation of optimization models can also be adapted to incorporate application and infrastructure network specific elements. For example, we could schedule the recovery of a disrupted power network by adapting an INDS problem [157] to consider the physics of AC or DC power flow. Furthermore, optimization models can be used to quantify the impacts of different decision making environments, such as pure centralized or decentralized decision making [196].

5 | OPTIMIZATION MODELS AND NETWORK EXTENSIBILITY

In this section, we focus on network optimization to analyze resilience as extensibility. Network extensibility is a dynamic capability to reconfigure and prolong the use of constrained resources to accommodate new operations and survive stressful events. Unlike robustness and rebound, which emphasize the continuation and restoration of existing network function, extensibility focuses on creating new network function to exceed predefined operational thresholds or change functional requirements. In resilience literature, network extensibility refers to models and measures for, "how well systems stretch to handle surprises," [220]. The term surprise is used to describe stressors where network operations and functional requirements may not be known a priori [72]. Methods for analyzing network robustness and rebound are limited for managing surprises because they only consider perturbations within the predefined set, $p \in \mathcal{P}$, or produce results constrained by predefined network structure ($G = (N, A)$), design options, and objectives. Thus, extensible networks are those designed with the capacity to serve new operational and functional needs, rather than maintain or restore existing functions.

Understanding the concept of extensibility requires additional nuance to ways a network may be vulnerable to stress and might not be resilient. Networks do not exhibit *resilience as robustness* if they cannot maintain predefined operational thresholds during perturbations, and networks do not exhibit *resilience as rebound* if they cannot restore function. In contrast, networks do not exhibit *resilience as extensibility* if network function is so tightly constrained that minor perturbations in resource allocation or functional requirements lead to extreme and cascading losses. To emphasize this fact, Woods [220] introduces the notion of "graceful" extensibility as a play on the software term graceful degradation, emphasizing that extensible systems must be able to stretch in ways that do not lead to brittle failures. Here, *brittle failure* refers to the process when networks catastrophically break down as resource and functional requirements push networks beyond their operational thresholds. In the words of Woods [220], "systems with high graceful extensibility have capabilities to anticipate bottlenecks ahead, to learn about the changing shape of disturbances and possess the readiness-to-respond to adjust responses to fit the challenges [82,223,224]." In contrast, networks that are unable to redistribute limited resources, adjust operational thresholds, or serve multiple purposes will likely experience brittle failure when surprises require network operations to change.

Unlike network resilience as robustness or rebound, the optimization community has put less focus on studies of extensibility. In the history of the journal *Networks*, only Pradhan and Meyer [173] ever use the word extensible or extensibility. Despite this dearth of research, several aspects of optimization models lend themselves to the study of how systems anticipate bottlenecks to stretch and handle surprises.

5.1 | Network extensibility in optimization models

A key element of network optimization models that influences extensibility and deserves more research is the model *boundary*. Network resilience through extensibility implies that systems have an operational boundary that can be extended during stressful events. However, the operational boundary in network optimization models is often treated as a "hard" limit that cannot be exceeded or altered during analysis. For example, the boundary on an objective function is commonly defined by a block of algebraic constraints, for example, $Ax \leq b$, where the operational boundary for a single network element is represented by a subset of constraints. Despite this common representation, real systems rarely fail to function when operated in infeasible regions that exceed these thresholds (e.g., $Ax = b + \epsilon$). For example, some real networks are operated in this infeasible region during disasters, such as electric power systems increasing powerline capacity and overloading equipment during an impending blackout [128]. System operators use overloading operations to adapt these and other systems to novel stressors. Rather than assume systems fail to function once constraints are violated, one goal of network extensibility is to understand how networks *stretch* beyond their stated boundary and continue to function. Network optimization studies that inform resilience as extensibility should aim to understand the costs and benefits of crossing these thresholds. Moreover, if the operational boundary nominally defined by model constraints can be exceeded in practice, then identifying the real "hard" operational boundary where the system will fail is a non-trivial task (e.g., understanding how increased power flow on lines will eventually lead to their failure which then, in turn, can lead to cascading blackouts).

Both resilience and network optimization communities use similar language and techniques for assessing the cost of extending system operation beyond expected boundaries. One way resilience research discusses the assessment of extensibility is through the analysis of system *slack* [187]. Here, resilience experts discuss slack with respect to the dynamic re-balancing of capabilities via resilience processes. The resilience literature discussion on slack is similar to the use of slack variables in network optimization to measure the implications of extending beyond a given constraint. In the simplest terms, given an explicit cost function for exceeding a threshold, one can use the slack variables to study extensibility related questions like, "at what cost would it make sense to violate a constraint, and by how much?"

Slack may relate to real network operations via the short- and long-term degradation of network performance when extending beyond normal boundaries. Systems commonly studied with robustness and rebound methods often have known surge capacities that enable extended operations during emergencies. For example, power system components like powerlines and transformers have emergency ratings that relax flow limits during blackout operations [128].

An even more dynamic use of slack beyond overloading network components is when part of the system *compensates* for another. This process of compensation can be thought of as network reciprocity, where nodes or links within a system take on or redistribute flow to protect other parts of the same or interdependent systems. In practice, compensation has been identified in many critical systems, where tradeoffs within and among network operators stretch systems to function in ways they were not originally intended for [220,221]. Effective compensation can increase network boundaries in unanticipated ways, such as compensating for a surge in hospital patients through triage and accessing resources like beds from other parts of the hospital [153]. In contrast, these dynamic interactions can also lead to *decompensation*—when one part of a system consumes the available slack of another, reducing the overall the ability of the system to adapt. Decompensation is known to be a key contributor to how adaptive systems fail [222]. Network optimization models can make use of shared budget constraints to capture this ability for compensation (and decompensation).

Broader still would be studies that capture the difficulty of changing current operations to enable greater access to slack. This could be studied using techniques for model persistence where changes to model structure that lead to new optimal solutions are constrained by past optimal solutions that may have already been implemented [41,43]. In other words, there are more costs to consider than just the performance degradation from overloading or sharing resources, such as simply the cost of rebalancing systems to enable extensibility.

5.2 | Using optimization models to analyze network extensibility

Although the language of mathematical optimization already has much of the vocabulary for representing network extensibility, there are several elements that remain largely unaddressed. Here we present potential ways to analyze network extensibility using optimization models.

5.2.1 | Identifying the "true" network operational boundary

In optimization models, a boundary condition $Ax \leq b$ is often viewed only through the lens of whether it is feasible or not, and this implicitly assumes that all feasible solutions are equivalent. Resilience as extensibility suggests that these simple notions of boundary are not sufficient for understanding the adaptive capacity of networks. Instead, the boundary of network operations lies well beyond the constraints built into an optimization model, and this "true" boundary may be unknown in normal practice.

Importantly, significant resilience research indicates that the amount of work that a system does to adapt "far away from its boundary" is very different (and typically much less) than the amount of work that a system does "near its boundary" [221]. That is, a system might have to dedicate more resources (and perhaps reconfigure its operating procedures) to handle events that stress it as it approaches the boundary condition. A classic example is the emergency department at a hospital for which there is no sharp boundary on the capacity to treat incoming patients; rather the operations and effort of staff dramatically change as the load on the system approaches and exceeds its nominal boundary [153].

In some network optimization models, increasing effort near a boundary is represented in terms of a nonlinear function intended to capture the growing effort or cost on the system as it approaches some implicit constraint. For example, congestion on road systems is known to be highly nonlinear, and as traffic density approaches a practical threshold the traffic speed and throughput dramatically decrease (see, e.g., the classic Bureau of Public Roads function for road congestion as implemented for regional traffic in the San Francisco Bay Area [6]). Indicators of this nonlinear loss of functionality as networks reach their boundaries are referred to as *critical slowing down* [62,189] and have been identified in numerous complex systems studied by the *Networks* community like power grids [104,105,106]. Still, past work considering either slack or critical slowing down is limited to system operations that we have recognized and parameterized a priori. A broader challenge for thinking about network extensibility is how we address operational boundaries that have not been considered in advance. A first step is understanding how overloading and compensation reveal new possibilities for network operations during stressful events. Future work needs to build on this to recognize where "true" network operational boundaries exist and how systems work harder to adapt (i.e., experience nonlinear losses) near operational boundaries.

5.2.2 | Network operations when faced with fundamental surprise

The concept of extensibility further challenges how stressful events are parameterized and modeled to inform network resilience. The types of events that can stress the network can be divided into two broad classes: (1) events that stress the network in a way that we previously predicted, planned for, or understood and (2) events that stress the network in ways that we never envisioned and changes our view on what can potentially happen. The former is often called *situational surprise* [130] and can be explicitly considered as either data or stochastic processes that alter network operations. In contrast, the latter is called *fundamental surprise* [130,219] and cannot be explicitly considered with current network optimization methods.

Fundamental surprise challenges the efficacy of existing network optimization methods for capturing aspects of extensibility. In general, surprise can be viewed as uncertainty about the decision making environment. Stochastic programming and robust optimization require one to characterize or parameterize uncertainty, which means these methods can only capture situational surprise and cannot consider fundamental surprise. Online methods to adapt optimization models for network operators in situ may be more appropriate for uncertainty that cannot be characterized a priori. However, current applications of online methods are unable to capture fundamental surprise. Current applications of online optimization [119] support decision making where the future is unknown but requires a model of the decisions that can be implemented in response to current operations. This implementation of online optimization assumes the network operators know the appropriate decisions and decision variables prior to a stressful event. Systems dealing with fundamental surprise may also require consideration of new, improvised decisions and actions that were not known until the stressful event occurs. In both cases, the characterization of uncertainty or the static nature of online models suggests that current methods for considering surprise are insufficient for resilience as extensibility.

Two brief examples help to illustrate the concept of fundamental surprise. One is the impact of the 2001 WTC attack on the infrastructure networks of lower Manhattan as there was no prediction or contingency plan for when an entire section of the infrastructure network disappeared [146]. Another example occurred in October 2017 when Hurricane Ophelia hit Ireland, making it the easternmost Atlantic hurricane; it was completely unexpected that a hurricane could travel like Ophelia and impact Western Europe, and analytic tools designed to model hurricane winds had to be reconfigured in real time to adapt [72].

Typically, networks dealing with situational surprise can be managed by updating the objectives and/or data into our network models. Here, the models that have been built for network resilience can be used in contingency planning for all the types of "surprise" that we can imagine. Some methods developed for situational surprise may also support adaptation to fundamental surprise. For example, temporary shunts were used to restore the electric power network in lower Manhattan after the 2001 WTC attack [146]. These shunts could be prepositioned to a situational surprise (e.g., thunderstorms) to schedule the recovery of a disrupted power network (similar to the INDS problems of [157]). Reformulating the same INDS problem could support the 2001 WTC response where a new model would need to be quickly created to guide recovery decisions over the "temporary" network. Research is needed to understand how to adapt existing network optimization problems for fundamental surprise.

Still, many fundamental surprise events cannot yet be parametrized like situational surprises, suggesting there are numerous examples of network extensibility that cannot yet be studied. Despite there being no model prior to the 2001 WTC attack or Hurricane Ophelia that could predict the events, numerous actions taken in response helped alleviate damages and protect critical systems. Real-world extensibility suggests that there are unexplored models and methods for fundamental surprise in network optimization. Importantly, fundamental surprise occurs when optimization models themselves are proven to be inappropriate to novel stressors and need to change. This phenomenon called *model surprise* emphasizes that there is limited research within the *Networks* and other related optimization communities about how appropriate existing problems are to fundamentally surprising events.

6 | OPTIMIZATION MODELS AND NETWORK ADAPTABILITY

Finally, we consider the role of network optimization to analyze resilience as adaptability. Network resilience viewed through the lens of adaptability deals with the need for networks to manage tradeoffs to build adaptive capacity to continuously evolving contexts, often over longer timescales. Sometimes this is also called *sustained adaptability* because it tends to focus attention on how a network survives over long-term future uses and contexts. Unlike robustness, rebound, and extensibility that are concerned with the impacts of stress on a network in a single event (or several events closely related in time), sustained adaptability is less concerned with the outcome of a single event, and more concerned with how a network survives many stressful events over its life-cycle. Thus, sustained adaptability is less focused on network operations and more focused with network design problems that consider tradeoffs between robustness, rebound, and extensibility to maximize adaptability into the future. For example, network adaptability must manage tradeoffs between robustness to situational surprise and extensibility to fundamental surprise [70]. Network adaptability must also manage tradeoffs between the fast recovery of existing systems and slowing recovery to redesign systems and "bounce back better."

Similar to extensibility, a network might not exhibit *resilience as adaptability* in at least two ways: (1) not being able to manage short-term tradeoffs for maintaining, restoring, and extending system structure and function, and (2) not being able to manage long-term tradeoffs to balance these adaptive capacities into the future. Woods [220] describes at least five challenges that an adaptable system should be able to manage over its intended life:

- challenges to network model boundary conditions as surprises continue to reoccur;
- challenges to assumptions about network conditions and contexts of use;
- challenges to network adaptability that lead to resource shortfalls and necessary operator compensation to fill the breach;
- challenges to network robustness and extensibility, where the factors that produce or erode both forms of resilience will change; and,
- challenges to network definition that question the purpose of the system itself, requiring the system to readjust its relationships with respect to interdependent and interacting systems.

Similar to extensibility, sustained adaptability has received less focus from the *Networks* community. Miller-Hooks [148] studies an algorithm to provide an adaptive route to a destination in a network with stochastic travel times and congestion based on the arrival time at a particular node. Nemeth and Retvari [154] study an adaptive routing algorithm to control the rate at which traffic is sent along paths. Silva et al. [200] consider a robust network design where the first stage determines potential routing schemes and the second stage selects which one to implement. In general, the *Networks* community tends to focus on adaptation in terms of routing in networks. Essentially no studies exist that address the tradeoffs between robustness, rebound, and extensibility and/or address the challenges laid out by Woods [220]. Still, several key network concepts and network optimization methods provide avenues for advancing research on how to maximize adaptive capacity to an uncertain future.

6.1 | Network adaptability in optimization models

A key element of network optimization models that influences sustained adaptability and deserves more research is network *architecture*. Network resilience as adaptability suggests that there is internal and external architecture that enables survival of system function over long time-scales. Here, architecture is used broadly to refer to the elements that comprise a networked system, including the structure of the system, the rules that govern network operations, the available decisions and decision variables, as well as the objectives that dictate system function and model results. Thus, architecture is more than just the connectivity pattern of a network, and it ultimately "must facilitate system-level functionality as well as robustness and evolvability to uncertainty and change in components, function, and environment" [3].

The Internet is one example of a complex networked system whose architecture has received considerable study, both from a historical perspective [58] and a modern theoretical framework [166]. The layered transmission control protocol (TCP/IP) protocol stack, in particular, has received considerable attention from a network optimization perspective. At the transmission layer, the combination of the TCP running in the end hosts at the network periphery and active queue management running in routers within the network interior is now understood to be solving a decentralized primal-dual algorithm for network resource allocation [139]. Moreover, the separation and interaction of functionality across protocol layers can further be understood as a form of optimization decomposition [55]. Collectively, this enhanced view has enabled rigorous proofs of the global efficiency, dynamics, and stability of these networking protocols, and has generated new ideas for creating robustness and adaptability in design. Similar notions of architecture are prevalent in the study of biology, where the highly-evolved design of natural systems display a remarkably parallel organization for managing tradeoffs [60,67], for example, signaling mechanisms in biological organisms (e.g., neural networks) [60,68]. Similar ideas can also be found in rules for command and control systems in large-scale organizations like the military [71]. Important questions for the *Networks* community are: *What are the architectures of systems that produce adaptive networks in the future? What are the design principles to create an adaptive network?*, and *How can one ensure adaptive network design in the long-term?*

Advances in identifying adaptive network architectures may be possible with existing scenario analysis for network design. For example, it is possible to formulate separate optimization problems for the same network that consider robustness to well-modeled stressors, rebound after stressful events, and extensibility to adjust operational boundaries. Subjecting these systems to projected long-term scenarios (via forecasting or backcasting) provides one way to compare the effectiveness of one form of resilience over another. Results of this comparison may reveal that a given network architecture is better off focusing on robustness, rebound, or extensibility in the near term.

Multi-objective programs and novel network optimization methods like multistage stochastic programming also support the development of new models and tools for network adaptability. Optimization models that can incorporate objectives that consider robustness, rebound, and extensibility together may provide further insight on network architecture and resilience tradeoffs. Since network adaptability deals with uncertain future scenarios, network optimization methods like multistage stochastic programming lend themselves to adaptability questions with known or assumed probabilities for future events. However, sustained adaptability also deals with optimization over uncertainty sets we cannot characterize a priori. Moreover, the design criteria and objectives required to ensure robustness, rebound, or extensibility may not be evident, or, more likely, will conflict. This suggests that multi-objective, online, robust, and/or stochastic approaches will be necessary, but potentially untenable for a normal network life-cycle. Advances in methods that relate different perspectives on resilience and/or consider uncertainty sets into the far future would support models that reveal adaptive network architectures.

6.2 | Using optimization models to analyze network adaptability

Scenario-based analysis and multi-objective or multistage stochastic programs may reveal network architecture that is resilient over long time-scales. However, there are open issues that inhibit the implementation of these methods to generate resilient architectures.

6.2.1 | Defining objectives to resolve network adaptability problems

To compare scenarios, one first requires a means to balance different forms of adaptive capacity. There is limited work within the resilience research community to draw on that provides a mathematical and computational basis to formulate an objective that balances simultaneous needs for robustness, rebound, and extensibility. Recent advances in theory propose the notion of *net adaptive value* as a goal for adaptability in the long term [221]. Net adaptive value draws on biological and neurological literature where adaptive value refers to advantage in fitness gained when an organism adapts to its environment [40]. A model objective centered on net adaptive value would seek to maximize adaptive value over the lifespan or multiple epochs that a network may exist. Still, besides neurological and biological research showing the existence of adaptive value tradeoffs, there is essentially no work organizing these tradeoffs in networked systems. Moreover, there is even less work framing these tradeoffs through the lens of robustness, rebound, and extensibility. Research is needed to determine how to formulate objectives that capture the goals of sustained adaptability.

An equally difficult problem to formulating a proper objective function is defining the planning horizon for network adaptability models. The need to *sustain* adaptability implies that net adaptive value must be maximized in the long term through a particular mix of robustness, rebound, and extensibility. However, the short-term effects of stressors means adaptability may only be realized in the short term. What defines long- and short-term analyses is poorly understood for many network optimization problems. Generally, many real-world networks have particular time frames for which they are designed, for example, civil infrastructure designed for a 30 to 60-year operational life, or established planning horizons, for example, 10 years for the electric power industry. However, these time horizons for analysis may be inappropriate as infrastructure is recommissioned and/or used well beyond its intended operational life. Tradeoffs among resilience capacities may reveal that maximizing net adaptive value for one time horizon (e.g., 30 years) may be very sensitive to minor changes (e.g., 31 years). Importantly, the combination of network resilience capacities for one time horizon may be prone to failure in another by increasing network fragility, overemphasizing fast recovery of outdated systems, and promoting decompensation.

6.2.2 | Knowing if, when, and how to switch from one form of resilience to another

Confounding the analysis of sustained adaptability is the fact that short-term stressful events do change systems in ways that will impact long-term tradeoffs. While robustness, rebound, and extensibility achieve resilience in different ways, the effectiveness of one approach influences the effectiveness of another. For example, consider a network that seeks to meet the demands within it during "normal" operations. This situation implicitly assumes that the network has the capacity to meet its demands and is, therefore, seeking to minimize costs under a set of constraints (e.g., flow-balance and arc capacity constraints). If a disruptive event causes damage to supply nodes and/or arcs within the network, it may no longer be possible for the network to meet all demand. Therefore, the objective of the network may then *switch* to meeting as much demand as possible after the disruptive event which could be modeled as a maximum flow problem. After such an event, we may seek to make decisions to restore disrupted flow within the network *until* all demand can then be met. At this point, we may then *switch* and seek to make restoration decisions to reduce the cost of meeting demand.

Determining how this switching occurs can influence recommendations for sustained adaptability. In some cases, it is not necessary for the underlying model of network operations to change to consider different aspects of resilience. For example, a transportation network may have steady-state O-D pairs and the model for normal operations may be to understand the average travel times within the network. If a hurricane (or other forecastable event) were to impact the area of this network, then the O-D pairs may now reflect those of an emergency evacuation but we would still be interested in knowing the travel times within the network. In this case, the *input* into the network model would need to be switched between normal and stressful operations. Similarly, choice of input parameters and model objectives may need to switch to assess robustness, rebound, and extensibility. Because robustness, rebound, and extensibility all deal with travel times, it is feasible to imagine that the underlying model would not need to change to determine adaptability tradeoffs between aspects of resilience.

However, in other cases the model framing may need to change to switch between approaches to resilience. Here, switching is not simply altering a model input or objective, it relates to a network operator's ability to reflect on current situations and improvise new ways to respond to stressors. Thus, an important aspect of sustained adaptability is how network operators and model developers influence the switching process. Assessing this process requires a better understanding of how the people embedded in networked systems respond and adapt to stress. Knowing if, when, and how to switch from one form of resilience to another is confounded by not just the output of multiple conflicting models, but by the ways people use and develop them in improvised ways.

7 | NETWORK OPTIMIZATION AND RESILIENCE, REVISITED

The development and application of network optimization models and algorithms can provide a critical perspective on the resilience of systems. In practice, the resilience of real-world networks depends on both the construction and analysis of the optimization model itself *and* how decision makers interact with it [72]. Within the *Networks* research community, we identify three practical ways network optimization advances knowledge of resilience: (1) building aspects of resilience into a network optimization model; (2) using network optimization models to study the resilience of a system; and (3) adaptation by users of optimization models for resilience. This is a progression that moves from a focus on the model, to the use of the model, to the user of the model.

Building aspects of resilience into an optimization model: The explicit output(s) from solving an optimization model can inform assessments of network resilience. Here, the optimization model itself must be structured to answer a specific resilience question. Often this requires one to consider network disruptions, measures of network performance, operational constraints, and desired resilience capabilities and capacities. Questions relevant to the development of an optimization model capable of improving network resilience include:

- **a.** What are potential events or disruptions that stress the network?
- **b.** What are the physics or dynamics governing network performance? How will network performance be measured before, during, and/or after an event?
- **c.** What decisions are available to adapt the network before, during, and/or after an event?
- **d.** What constrains these decisions to adapt?
- **e.** What are the resilience objectives for the network? What criteria define optimality?

This last question is of particular importance because many researchers working in the area of resilience engineering use the term "optimization" as a synonym with the drive for "faster, better, and cheaper" solutions to operational problems that often lead to brittle systems. Just as we are deliberate in pointing out to optimization researchers that resilience is more than just robustness or rebound, we also want to make the point that *the use of optimization models does not necessarily imply a drive* *for efficiency*. It is possible to make some measure of resilience the explicit objective of an optimization model, or to use the optimization model in novel ways.

Using optimization models to analyze aspects of resilience: The innovative use of optimization models and/or the analysis of model output(s) can provide further insight on how to improve network resilience. Here, the focus is not on model formulation, but rather insight gained from using established models to answer what-if questions by including new input data representing new scenarios, changes in constraints, or changes in objectives. Questions relevant for the selection and use of existing optimization models for improving network resilience include:

a. How would network resilience be informed by parametric analysis and what-if scenarios?
b. What are the appropriate use cases for the optimization model? What are their limitations?

It is important to note that one can use optimization models that *do not have* an aspect of resilience built into them to analyze aspects of resilience. For example, one could enumerate all possible stressful events (let i index the stressful event and G^i represent the resulting network) and solve for $f(G^i)$ for each one of them to understand the potential impacts of the stressful event. This simply would require using the network optimization problem that captures $f(G^i)$. As another example, one could solve an interdiction problem to understand the worst-case scenario in terms of the performance of the network across a set of potential disruptions. In both these examples, we are using optimization models to quantify or improve an aspect of resilience.

Adaptation by users of optimization models to provide resilience: Because optimization models are ultimately meant to inform real network operations, the ease with which decision makers implement, update, or abandon models further influences how optimization can improve network resilience. A major theme of the resilience engineering literature over the last 20 years is that the humans embedded in networked systems (not models or algorithms) are primary enablers of resilience. This is possible because humans can reframe a problem in the presence of surprise and update or abandon a model when it becomes inappropriate for the problem at hand [72,110,111,218,219]. Thus, how well a model enables its "user" to adapt the decision making process is equally as important as the model formulation and parametric analysis. Questions relevant to the use of optimization models in this context include:

a. How do model users know what aspect of network resilience the model output(s) and/or analysis is meant to improve?
b. How does the user interact with model output(s) and/or analysis to respond to network events or disruptions?
c. How does the user know the appropriate real-world context for the model output(s) and/or analysis? How does the user recognize an inappropriate use of model output(s) and/or analysis?
d. How can the user know when to ignore, switch, change, modify, or abandon model output(s) and/or analysis for one more appropriate to the current context?
e. How easy it is to implement, or change, or abandon the model, and what are the implications for the underlying decision processes? What recourse is available when the model becomes stale?

The ultimate goal is to make optimization models accessible, usable, and adaptable in a variety of different contexts, processes, and systems. For a detailed discussion of the way optimization modelers and users can adapt in the presence of surprise, see Eisenberg et al. [72].

The *Networks* community has established the importance of its work in a variety of contexts, processes, and systems surrounding resilience. To highlight this importance, we provide a retrospective analysis of the references in this paper in Section 7.1. We then look to the future in Section 7.2 by discussing how, in our opinion, the *Networks* community can expand its impact in resilience by tackling problems related to extensibility and adaptability.

7.1 | A retrospective view: impact of the *Networks* community on resilience concepts

In this section, we analyze the impact that the *Networks* community has had with respect to resilience. This impact can be seen by where papers citing the discussed references in this paper are being published. Therefore, we analyze the types of *subject categories* from the Web of Science (WoS) (originally produced by the Institute for Scientific Information) where these citations appear. We do so for *all* papers referenced in Section 3, Section 4, and those referenced published in *Networks*.

In each of these three areas, each citing article counts once (i.e., it is not weighted by the number of papers it cites from the area) in the total counts for a particular journal it appears in. However, note that the journal it is published in may appear in multiple categories, so the count for the journal would be added to each subject category. We will point out that these subject category classifications may not be perfect but given the prevalence of WoS are sufficient for purposes of this analysis. The data for citations was collected on May 15, 2020. Our analysis examines a total of 133 referenced articles for the analysis of Section 3 yielding 4783 citing articles, 42 referenced articles for the analysis of Section 4 yielding 1508 citing articles, and 53 referenced articles for the *Networks* analysis yielding 742 citing articles.

TABLE 1 The top 20 categories citing papers from Section 3, that is, resilience as robustness

Rank	Discipline	Count
1	Operations Research & Management Science	1482
2	Engineering, Electrical & Electronic	847
3	Engineering, Civil	576
4	Engineering, Industrial	560
5	Management	465
6	Computer Science, Interdisciplinary Applications	353
7	Transportation Science & Technology	333
8	Computer Science, Information Systems	282
9	Mathematics, Applied	273
10	Computer Science, Theory & Methods	256
11	Energy & Fuels	255
12	Transportation	238
13	Telecommunications	221
14	Water Resources	198
15	Computer Science, Artificial Intelligence	193
16	Engineering, Multidisciplinary	191
17	Computer Science, Hardware & Architecture	182
18	Economics	176
19	Environmental Sciences	160
20	Environmental Studies	159

TABLE 2 The top 20 categories citing papers from Section 4, that is, resilience as rebound

Rank	Discipline	Count
1	Operations Research & Management Science	257
2	Engineering, Electrical & Electronic	221
3	Engineering, Civil	217
4 (tied)	Computer Science, Information Systems	163
4 (tied)	Engineering, Industrial	163
6	Transportation Science & Technology	127
7	Computer Science, Theory & Methods	117
8	Computer Science, Interdisciplinary Applications	101
9	Engineering, Multidisciplinary	99
10	Transportation	96
11	Telecommunications	88
12	Water Resources	86
13	Environmental Sciences	81
14	Geosciences, Multidisciplinary	79
15	Energy & Fuels	72
16	Meteorology & Atmospheric Sciences	72
17 (tied)	Green & Sustainable Science & Technology	65
17 (tied)	Physics, Multidisciplinary	65
19	Environmental Studies	64
20	Multidisciplinary Sciences	60

Tables 1 to 3 provide the top 20 categories of citations for references in Section 3, Section 4, and in papers published in *Networks* referenced in Sections 3 and 4, respectively. In the remainder of this analysis, we refer to these areas as robustness, rebound, and *Networks*. Table 4 provides a comparative summary of each category that appears in the top 20 for at least one of robustness, rebound, and *Networks* and provides the ranking of each category across these areas.

As expected, Operations Research & Management Science is the highest ranking category in all three tables. Electrical & Electronic Engineering is also highly ranked (second, second, third) across robustness, rebound, and *Networks*. This indicates that the work done by the *Networks* community is impacting research into power grid resilience. The categories of Civil

TABLE 3 The top 20 categories citing papers from *Networks*

Rank	Discipline	Count
1	Operations Research & Management Science	359
2	Mathematics, Applied	108
3	Engineering, Electrical & Electronic	107
4	Computer Science, Hardware & Architecture	103
5	Computer Science, Interdisciplinary Applications	88
6	Computer Science, Theory & Methods	84
7	Management	83
8	Engineering, Industrial	77
9	Telecommunications	66
10	Computer Science, Information Systems	57
11	Transportation Science & Technology	45
12	Computer Science, Artificial Intelligence	44
13	Computer Science, Software Engineering	32
14	Transportation	29
15 (tied)	Economics	27
15 (tied)	Engineering, Civil	27
17	Automation & Control Systems	20
18	Engineering, Multidisciplinary	15
19	Mathematics, Interdisciplinary Applications	11
20 (tied)	Geography	10
20 (tied)	Mathematics	10

Engineering, Transportation, and Transportation Science & Technology also all appear in the top 20 for robustness, rebound, and *Networks* indicating that the *Networks* community is impacting research into resilience of civil infrastructure, especially transportation systems. Telecommunications appears in the top 20 for all three areas and in the top 10 for *Networks*, which is to be expected given the number of special issues published by *Networks* on resilient telecommunications systems. Industrial Engineering appears in the top 10 for all three areas and Management appears in the top 10 for robustness and *Networks*. This demonstrates the impact of these areas on supply chain and business resilience. The data also show the reach of the *Networks* community in a broad range of non-traditional categories including Environmental Sciences, Green & Sustainable Science & Technology, Water Resources, and Multidisciplinary Sciences. When examining these categories, we observe impacts in wildlife conservation research, hazard risk and mitigation modeling, electric vehicles, urban water design, and renewable energy.

In terms of examining the uniqueness of *Networks* for these categories, Applied Mathematics ranks second in Table 3 and other mathematical categories appear in the top 20. There are also six different categories associated with Computer Science that appear in the *Networks* top 20. Note that the high ranking of Computer Science, Hardware & Architecture in Table 3 comes from *Networks* own classification in this category. The appearance of the mathematical and computer science categories speaks to the reputation of *Networks* across these areas. It is also interesting to observe that there is much more overlap in the top 20 of *Networks* and robustness than *Networks* and rebound. We believe this comes from the fact that robustness has more research to date and that *Networks* has established its presence in the communities that are applying optimization to study robustness of their physical systems.

It is clear from comparing Table 1 with Table 2 that resilience as robustness has significantly more research surrounding it to date. This fact arises because optimization approaches for resilience as rebound is a relatively recent development: with the exception of a reference helping to introduce the concept of interdependencies, the earliest referenced paper in Section 4 is in 2010 [142]. No papers referenced in Section 4 appeared in 2011 and only three papers in 2012 [18,20,159]. Figure 1 analyzes the trend in citations for robustness and rebound. In both cases, rapid growth in the number of citations occurred starting in 2013. In particular, robustness citations grew from 208 in 2013 to 771 in 2019 and rebound citations from 56 to 281. Part of this growth is a function of the number of papers analyzed. In Figure 2, we normalize the data by presenting the number of citations in year divided by the total number of papers published before or during year t (i.e., the cumulative number of papers published) which all could have contributed to the citations for that year. With this metric, we observe a spike for rebound in 2009 which corresponds to the emergence of the field as a small number of papers led to the growth of many future papers. The trend for rebound appears to level out to an impact value consistent with robustness. Furthermore, in terms of overall comparison, there are 133 referenced articles for robustness and 4783 citing articles, for a ratio of citing articles to references of 35.96. This is

TABLE 4 Comparative analysis of ranks within the top 20 of categories across areas (— indicates not ranked in top 20) ordered by *Networks* rank

Category	*Networks*	Robustness	Rebound
Operations Research & Management Science	1	1	1
Mathematics, Applied	2	9	—
Engineering, Electrical & Electronic	3	2	2
Computer Science, Hardware & Architecture	4	17	—
Computer Science, Interdisciplinary Applications	5	6	8
Computer Science, Theory & Methods	6	10	7
Management	7	5	—
Engineering, Industrial	8	4	4 (tied)
Telecommunications	9	13	11
Computer Science, Information Systems	10	8	4 (tied)
Transportation Science & Technology	11	7	6
Computer Science, Artificial Intelligence	12	15	—
Computer Science, Software Engineering	13	—	—
Transportation	14	12	10
Economics	15 (tied)	18	—
Engineering, Civil	15 (tied)	3	3
Automation & Control Systems	17	—	—
Engineering, Multidisciplinary	18	16	9
Mathematics, Interdisciplinary Applications	19	—	—
Geography	20 (tied)	—	—
Mathematics	20 (tied)	—	—
Environmental Studies	—	20	19
Environmental Sciences	—	19	13
Multidisciplinary Sciences	—	—	20
Energy & Fuels	—	11	15
Geosciences, Multidisciplinary	—	—	14
Green & Sustainable Science & Technology	—	—	17 (tied)
Physics, Multidisciplinary	—	—	17 (tied)
Meteorology & Atmospheric Sciences	—	—	16
Water Resources	—	14	12

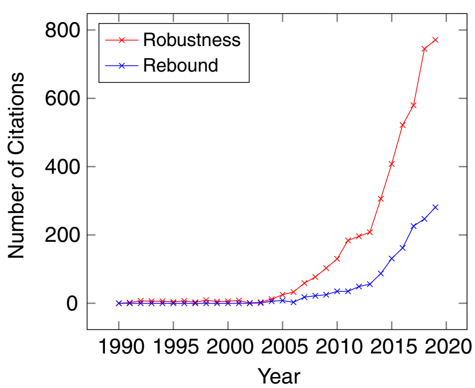

FIGURE 1 The ratio of the number of citations over time and cumulative number of papers published in an area for papers from Sections 3 and 4 [Color figure can be viewed at wileyonlinelibrary.com]

compared to 42 referenced articles for rebound and 1508 citing articles, for a ratio of 35.90. Therefore, the normalized impact of the papers produced by the network optimization community influencing robustness and rebound is almost identical.

Figure 3 presents a similar analysis for the *Networks* references. Although impressive growth still occurred from 36 citations in 2013 to 83 citations in 2019, there is room for the journal to be part of a larger dialogue on resilience. We now transition to a prospective view on how we believe this may be accomplished.

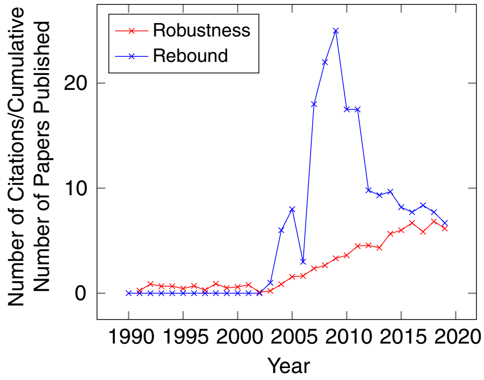

FIGURE 2 Number of citations over time for papers from Sections 3 and 4 [Color figure can be viewed at wileyonlinelibrary.com]

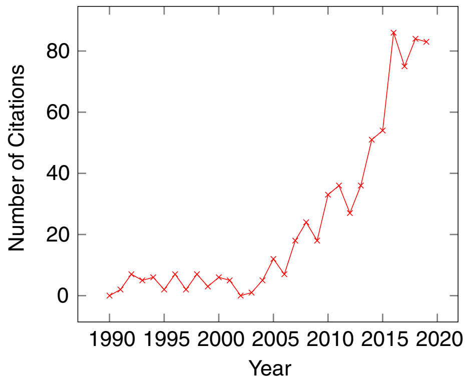

FIGURE 3 Number of citations over time for papers from *Networks* [Color figure can be viewed at wileyonlinelibrary.com]

7.2 | A prospective view: resilience concepts that require greater consideration by the *Networks* community

Robustness and rebound are two resilience concepts that are most commonly studied by the *Networks* community, but they do not capture all aspects of network resilience. Robustness and rebound are important because they characterize how systems perform immediately before or after a stressful event. However, they tend to focus only on *what happened* as opposed to *what was done*. That is, robustness and rebound optimization problems focus on resilient outcomes, such as limiting impacts to current operations or speeding up recovery, but do not provide knowledge about the processes that are present to govern such behavior. Understanding the processes that govern resilience in addition to measuring resilient outcomes is important because there is a longstanding opinion in the resilience research community, that, "resilience is not just about what you *have*, it's what you *do*" [72].

Extensibility and sustained adaptability focus attention on the processes that govern how well a network will adapt to current and future stress. Extensibility and adaptability focus on managing interconnected resources as systems change or as the effects of a stressful event are materializing. The goal of extensibility and sustained adaptability is to maximize the adaptive capacity of a network, which differs from robustness and rebound approaches to minimize the negative impacts of stress. Thus, extensibility and adaptability are more about the process and are concepts that focus less on outcomes and more on capabilities (sometimes referred to as *capacity to maneuver* [221]).

Resilience processes that underlie extensibility and sustained adaptability have been defined in a number of ways across the literature [170,177], but generally refer to four interrelated activities that enable adaptive capacity. For example, Boyd [39] introduced the observe-orient-decide-act loop to characterize the ability of a pilot to gain advantage in combat by adapting faster than an adversary [161]. Hollnagel [109] re-characterizes these processes as monitoring-responding-learning-anticipating to emphasize the need for learning new ways to anticipate future events. Park et al. [168] operationalize these processes for networked systems using the terms sensing-anticipating-adapting-learning. Seager et al. [192], Eisenberg et al. [71], and Thomas et al. [209] advance these perspectives with greater definition and integration:

- *Observing/orienting/monitoring/sensing*: the process of acquiring, apprehending, or accessing information about network operational states and conditions;

- *Deciding/anticipating*: the process of using existing or new models to interpret sensed information and decide a course of action;
- *Acting/responding/adapting*: the process of taking actions to change network structure or function in response to stress; and
- *Learning*: the process of updating and revising sensing, anticipating, and adapting processes to changing conditions.

These processes are not traditionally considered by the *Networks* community. However, they *could* be. Solving optimization problems for robustness and rebound that overlook these processes cannot provide new knowledge or decision support to improve extensibility or sustain adaptability. Importantly, a focus on resilience processes emphasizes the role of the individuals who create and use network optimization models to adapt in addition to the models themselves. For example, significant research shows that there are tradeoffs between perspectives on resilience, such as increasing robustness to particular stressors produces brittle networks that lack adaptive capacity [49,69]. How model developers and users interpret and implement these resilience goals provides information about resilience processes. Many of the modeling techniques used by the *Networks* community could be applied to these concepts. In Section 8, we articulate several opportunities for contributions.

8 | IN SEARCH OF NETWORK RESILIENCE: A RESEARCH AGENDA FOR THE *NETWORKS* COMMUNITY

Advances in network optimization championed by the journal *Networks* over the last 50 years coincide with similar efforts to understand and apply concepts of resilience. The journal has helped establish a vibrant community of researchers that has made significant contributions to the resilience literature. In particular, the *Networks* community has created and analyzed many network optimization problems that help address aspects of resilience. At the same time, advances made by the resilience community over its 50 years inform the themes that the *Networks* community should be building into our optimization problems in the future.

There is no single agreed upon definition of resilience, but several aspects of resilient systems inform network optimization research. There are at least four ways networks demonstrate resilience: robustness, rebound, extensibility, and adaptability. Network robustness and rebound emphasize desired resilience outcomes for networked systems via limiting the impacts of stressful events and speeding up recovery from losses. Network extensibility and adaptability emphasize improving resilience processes to maximize adaptive capacity to unforeseen stressors and uncertain futures. Together, resilience is not just about the network itself (i.e., what you have) but what decision makers do in response to a stressful event. These fundamental differences between robustness, rebound, extensibility, and adaptability emphasize that there is no “uber model” that offers support for all aspects of resilience simultaneously. They also emphasize that it does not make sense to “optimize resilience”—we can optimize *an aspect* of resilience or analyze tradeoffs between aspects within the models and analysis conducted by the *Networks* community, but not all aspects simultaneously.

Network optimization models can be used to address each of the four concepts of resilience. To date, the literature produced by the *Networks* community has been dominated by work addressing robustness and rebound. The research agenda for our community going forward should seek to address key challenges that will enable continued contributions to robustness and rebound and new contributions to extensibility and adaptability. These challenges include:

- **Capturing the *boundary* of network operations**: A focus on the level of network performance (e.g., current maximum flow) does not provide an understanding of how hard the network is working to deliver that performance. Moreover, the boundaries embedded in network models that define model feasibility are not often the “true” boundaries on network operations. An understanding of how close the network is to its “true” boundary where performance degrades and the system will fail is necessary to study its extensibility. An improved understanding of boundary could also provide an alternative understanding of robustness. Knowing how hard the network is working to operate provides a new reference point to measure the impacts of stressful events. Furthermore, by understanding the boundary, we can capture where rebound activities are essential to restore network performance.
- **Methods to better handle “unknown” uncertainty that *surprise* parameters, decisions, and constraints**: Methods to model or handle uncertainty are critical when characterizing the surprise from stressful events. Research can be undertaken to examine rebound from events where there is uncertain information about the impact of the stressful event. A critical future research direction for the *Networks* community is on modeling uncertainty with regard to the types of decisions and constraints that arise after situational and fundamental surprises. While classic methods to handle decision making under uncertainty (e.g., stochastic programming, robust optimization, or online optimization) can handle parameter uncertainty, it is less clear how to model uncertainty when it impacts the types of decisions that can be implemented. If research is conducted in this area, it will help to address how networks handle fundamental surprise.

- **Revealing the implications of network *architecture***: Despite the importance of architecture in networks, like the internet, there is limited work within the network optimization community studying the implications of architecture on resilience. Important research directions should include an understanding of how architecture optimized for one aspect of resilience influences another. For example, how do interpretations of fast recovery or extensibility change for robust or brittle networks? Similar questions can be asked of networks optimized for rebound and extensibility.
- **Problems balancing *tradeoffs* among multiple aspects of resilience**: Research has begun to incorporate multiple aspects of resilience into the same problem; for example, we can examine network robustness by measuring *rebound* after stressful events. There are many important directions in this area since network adaptability must be sustained in the short- and long-term. Identifying and managing the tradeoffs between robustness, rebound, and extensibility is essential for adaptability. Another important direction is on problems that examine the tradeoff between immediate rebound and implementing recovery decisions that improve robustness and/or extensibility for future stressful events, thereby embodying sustained adaptability.
- **Models and/or methods that enable *improvisation***: Models that capture a network's ability to improvise its operations based on the current state of the world would help to address aspects related to extensibility and adaptability. Methods that enable network operators and modelers to improvise new, reformulated, optimization models would also overcome issues with fundamental surprise. Future research directions should seemlessly inform network operators to implement improvised decisions while modelers reformulate and validate new models directly related to fundamental surprise.
- **Methods for model *switching***: The types of optimization problems that impact *an aspect* of resilience are part of the toolbox available to network operators. Methods that can formalize when an operator can and should switch the problem being applied to resilience is valuable in practice. This process of switching also has implications for long-term network adaptability. An important area of research is examining the current state of network optimization models and their use to determine whether these models are fit for purpose. Determining if, when, and how to switch models will help establish how to best employ the current toolbox of resilience methods. Furthermore, research should examine how to determine when parts of the toolbox fit or if, instead, new optimization problems, models, and methods should be developed.

Ultimately, the use of network optimization to address these challenges must remain pragmatic because resilience is not just about the model. Future work must frame the importance of new models and methods alongside the modelers and the operators who will use them. All will have to work together to achieve resilience in the presence of future stress.

ACKNOWLEDGMENTS

We thank the review team for their extensive comments that helped shape the structure of the paper and offer more precision for the discussions throughout the paper. We greatly appreciate the opportunity to contribute to this special issue. We thank the guest editors, S. Raghu Raghavan and J. Cole Smith, and the co-Editors in Chief, Bruce Golden and Douglas Shier, for their work on the special issue. The research of Thomas C. Sharkey was partially supported by the National Science Foundation under grant number CMMI-1254258 and partially conducted while he was on the faculty of Rensselaer Polytechnic Institute. The research of David L. Alderson and Daniel A. Eisenberg was partially supported by the U.S. Defense Threat Reduction Agency (grant no. DTRA-18681-M). The views and opinions expressed in this article are those of the individual authors and not those of the U.S. Navy, or other sponsor organizations.

ORCID

Thomas C. Sharkey https://orcid.org/0000-0001-6210-9448

REFERENCES

[1] H. Aissi and D. Vanderpooten, *Robust capacity expansion of a network under demand uncertainty: A bi-objective approach*, Networks **68** (2016), 185–199.

[2] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, *A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability*, IEEE Commun. Surv. Tutor. **11** (2009), 106–124.

[3] D.L. Alderson and J.C. Doyle, *Contrasting views of complexity and their implications for network-centric infrastructures*, IEEE Trans. Syst. Man Cybernet. A: Syst. Hum. **40** (2010), 839–852.

[4] D.L. Alderson, G.G. Brown, W.M. Carlyle, and R.K. Wood, "*Solving defender-attacker-defender models for infrastructure defense*," *Operations Research, Computing, and Homeland Security*, R.K. Wood and R.F. Dell (eds), Institute for Operations Research and the Management Sciences, Hanover, MD, 2011, pp. 28–49.

[5] D.L. Alderson, G.G. Brown, and W.M. Carlyle, "*Assessing and improving operational resilience of critical infrastructures and other systems*," *Tutorials in Operations Research: Bridging Data and Decisions*, A. Newman and J. Leung (eds), Institute for Operations Research and Management Science, Hanover, MD, 2014, pp. 180–215.

[6] D.L. Alderson, G. Brown, W.M. Carlyle, and R.K. Wood, *Assessing and improving the operational resilience of a large highway infrastructure system to worst-case losses*, Transp. Sci. **52** (2017), 1012–1034.
[7] N. Alguacil, A. Delgadillo, and J.M. Arroyo, *A trilevel programming approach for electric grid defense planning*, Comput. Oper. Res. **41** (2014), 282–290.
[8] M.L. Ali, P.-H. Ho, and J. Tapolcai, *SRLG failure localization using nested m-trails and their application to adaptive probing*, Networks **66** (2015), 347–363.
[9] C. Alvarez, M. Blesa, J. Diaz, M. Serna, and A. Fernandez, *Adversarial models for priority-based networks*, Networks **45** (2005), 23–35.
[10] E. Álvarez-Miranda and J. Pereira, *Designing and constructing networks under uncertainty in the construction stage: Definition and exact algorithmic approach*, Comput. Oper. Res. **81** (2017), 178–191.
[11] J. Anderies, C. Folke, B. Walker, and E. Ostrom, *Aligning key concepts for global change policy: Robustness, resilience, and sustainability*, Ecol. Soc. **18** (2013), 8.
[12] A. Arab, A. Khodaei, Z. Han, and S.K. Khator, *Proactive recovery of electric power assets for resiliency enhancement*, IEEE Access **3** (2015), 99–109.
[13] A. Arab, A. Khodaei, S.K. Khator, and Z. Han, *Electric power grid restoration considering disaster economics*, IEEE Access **4** (2016), 639–649.
[14] A. Arulselvan, A. Bley, and I. Ljubić, *The incremental connected facility location problem*, Comput. Oper. Res. **112** (2019), 104763.
[15] E. Aslan and M. Çelik, *Pre-positioning of relief items under road/facility vulnerability with concurrent restoration and relief transportation*, IISE Trans. **51** (2019), 847–868.
[16] A. Atamturk and A. Bhardwaj, *Network design with probabilistic capacities*, Networks **71** (2018), 16–30.
[17] A. Atamturk and M. Zhang, *Two-stage robust network flow and design under demand uncertainty*, Oper. Res. **55** (2007), 662–673.
[18] I. Averbakh, *Emergency path restoration problems*, Discrete Optim. **9** (2012), 58–64.
[19] I. Averbakh, *Minimizing the makespan in multiserver network restoration problems*, Networks **70** (2017), 60–68.
[20] I. Averbakh and J. Pereira, *The flowtime network construction problem*, IIE Trans. **44** (2012), 681–694.
[21] I. Averbakh and J. Pereira, *Network construction problems with due dates*, Eur. J. Oper. Res. **244** (2015), 715–729.
[22] I. Averbakh and J. Pereira, *Lateness minimization in pairwise connectivity restoration problems*, INFORMS J. Comput. **30** (2018), 522–538.
[23] A. Balakrishnan, M. Banciu, K. Glowacka, and P. Mirchandani, *Hierarchical approach for survivable network design*, Eur. J. Oper. Res. **225** (2013), 223–235.
[24] S. Bao, C. Zhang, M. Ouyang, and L. Miao, *An integrated tri-level model for enhancing the resilience of facilities against intentional attacks*, Ann. Oper. Res. **283** (2019), 87–117.
[25] F. Barbosa, A. de Sousa, and A. Agra, *Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes*, Networks **75** (2020), 356–373.
[26] M. Baxter, T. Elgindy, T.A. Ernst, T. Kalinowski, and M.W.P. Savelsbergh, *Incremental network design with shortest paths*, Eur. J. Oper. Res. **238** (2014), 675–684.
[27] N.O. Baycik and T.C. Sharkey, *Interdiction-based approaches to identify damage in disrupted critical infrastructures with dependencies*, J. Infrastruct. Syst. **25** (2019), 04019013.
[28] N.O. Baycik and K.M. Sullivan, *Robust location of hidden interdictions on a shortest path network*, IISE Trans. **51** (2019), 1332–1347.
[29] N.O. Baycik, T.C. Sharkey, and C. Rainwater, *Interdicting layered physical and information flow networks*, IISE Trans. **50** (2018), 316–331.
[30] H. Bayrak and M.D. Bailey, *Shortest path network interdiction with asymmetric information*, Networks **52** (2008), 133–140.
[31] F. Bendali, I. Diarrassouba, A.R. Mahjoub, M. Didi Biha, and J. Mailfert, *A branch-and-cut algorithm for the k-edge connected subgraph problem*, Networks **55** (2010), 13–32.
[32] D. Bertsimas and M. Sim, *Robust discrete optimization and network flows*, Math. Program. **98** (2003), 49–71.
[33] D. Bienstock, *Electrical Transmission System Cascades and Vulnerability: An Operations Research Viewpoint*, SIAM-MOS, Philadelphia, PA, 2016.
[34] D. Bienstock and A. Verma, *The* $N-k$ *problem in power grids: New models, formulations, and numerical experiments*, SIAM J. Optim. **20** (2010), 2352–2380.
[35] J.S. Borrero, O.A. Prokopyev, and D. Saure, *Sequential shortest path interdiction with incomplete information*, Decis. Anal. **13** (2015), 68–98.
[36] J.S. Borrero, O.A. Prokopyev, and D. Saure, *Sequential interdiction with incomplete information and learning*, Oper. Res. **67** (2019), 72–89.
[37] Q. Botton, B. Fortz, L. Gouveia, and M. Poss, *Benders decomposition for the Hop-constrained survivable network design problem*, INFORMS J. Comput. **25** (2013), 13–26.
[38] Q. Botton, B. Fortz, and L. Gouveia, *On the hop-constrained survivable network design problem with reliable edges*, Comput. Oper. Res. **64** (2015), 159–167.
[39] J. Boyd. A discourse on winning and losing: Patterns of conflict. *Unpublished Briefing*, December 7, 1986.
[40] N. Brenner, W. Bialek, and R.D.R. Van Steveninck, *Adaptive rescaling maximizes information transmission*, Neuron **26** (2000), 695–702.
[41] G. Brown and R. Dell, *Formulating linear and integer linear programs: A rogues' gallery*, INFORMS Trans. Educ. **7** (2007), 153–159.
[42] G. Brown, M. Carlyle, J. Salmerón, and R.K. Wood, *Defending critical infrastructure*, Interfaces **36** (2006), 530–544.
[43] G.G. Brown, R.F. Dell, and R.K. Wood, *Optimization and persistence*, Interfaces **27** (1997), 15–37.
[44] M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, T.D. O'Rourke, A.M. Reinhorn, M. Shinozuka, K. Tierney, W.A. Wallace, and D. von Winterfeldt, *A framework to quantitatively assess and enhance the seismic resilience of communities*, Earthquake Spectra **19** (2003), 733–752.
[45] C. Busing, A. Grub, A.M.C.A. Koster, W. Laube, and M. Tieves, *Robust spectrum allocation in elastic flexgrid optical networks: Complexity and formulations*, Networks **70** (2017), 342–359.
[46] M. Bynum, A. Staid, B. Arguello, A. Castillo, J.-P. Watson, and C.D. Laird, *Proactive operations and investment planning via stochastic optimization to enhance power systems extreme weather resilience*, Optim. Online Repos. (2018).
[47] E. Canale, H. Cancela, F. Robledo, P. Romero, and P. Sartor, *Diameter constrained reliability: Complexity, distinguished topologies and asymptotic behavior*, Networks **66** (2015), 296–305.
[48] E. Canale, P. Romero, and G. Rubino, *Factorization and exact evaluation of the source-terminal diameter-constrained reliability*, Networks **70** (2017), 283–291.
[49] J.M. Carlson and J. Doyle, *Highly optimized tolerance: Robustness and design in complex systems*, Phys. Rev. Lett. **84** (2000), 2529–2532.
[50] A. Castillo, T. Nakashima-Paniagua, and J. Doucette, *Dual-failure restorability analysis of span-restorable meta-mesh networks*, Networks **75** (2020), 405–419.
[51] B. Cavdaroglu, E. Hammel, J.E. Mitchell, T.C. Sharkey, and W.A. Wallace, *Integrating restoration and scheduling decisions for disrupted interdependent infrastructure systems*, Ann. Oper. Res. **203** (2013), 279–294.

[52] M. Çelik, *Network restoration and recovery in humanitarian operations: Framework, literature review, and research directions*, Surv. Oper. Res. Manage. Sci. **21** (2016), 47–61.
[53] M. Çelik, O. Ergun, and P. Keskinocak, *The post-disaster debris clearance problem under incomplete information*, Oper. Res. **63** (2015), 65–85.
[54] Y. Cheng, D. Medhi, and J.P.G. Sterbenz, *Geodiverse routing with path delay and skew requirement under area-based challenges*, Networks **66** (2015), 335–346.
[55] M. Chiang, S.H. Low, A.R. Calderbank, and J.C. Doyle, *Layering as optimization decomposition: A mathematical theory of network architectures*, Proc. IEEE **95** (2007), 255–312.
[56] M. Chimani, M. Kandyba, I. Ljubić, and P. Mutzel, *Orientation-based models for {0,1,2}-survivable network design: Theory and practice*, Math. Program. Ser. B **124** (2010), 413–439.
[57] R.L. Church and M.P. Scaparra, *Protecting critical assets: The r-interdiction median problem with fortification*, Geogr. Anal. **39** (2007), 129–146.
[58] D.D. Clark, *The design philosophy of the DARPA internet protocols*, Proc. ACM SIGCOMM '88, ACM Comput. Commun. Rev., 18, 1988, pp. 106–114.
[59] T.G. Crainic, X. Fu, M. Gendreau, W. Rei, and S.W. Wallace, *Progressive hedging-based metaheuristics for stochastic network design*, Networks **58** (2011), 114–124.
[60] M. Csete and J.C. Doyle, *Bow ties, metabolism and disease*, Trends Biotechnol. **22** (2004), 446–450.
[61] C.A. Cullenbine, R.K. Wood, and A.M. Newman, *Theoretical and computational advances for network diversion*, Networks **62** (2013), 225–242.
[62] V. Dakos, S.R. Carpenter, E.H. van Nes, and M. Scheffer, *Resilience indicators: Prospects and limitations for early warnings of regime shifts*, Philos. Trans. R. Soc. B: Biol. Sci. **370** (2015), 20130263.
[63] R.J. Dawson and A.A. Farrag, *Fault-tolerant extensions of star networks*, Networks **21** (1991), 373–385.
[64] V. Diarrassouba, A.R. Gabrel, L.G. Mahjoub, and P. Pesneau, *Integer programming formulations for the k-edge-connected 3-hop-constrained network design problem*, Networks **67** (2016), 148–169.
[65] T. Ding, C. Li, C. Yan, F. Li, and Z. Bie, *A bilevel optimization model for risk assessment and contingency ranking in transmission system reliability evaluation*, IEEE Trans. Power Syst. **32** (2017), 3803–3813.
[66] T. Ding, L. Yao, and F. Li, *A multi-uncertainty-set based two-stage robust optimization to defender-attacker-defender model for power system protection*, Reliab. Eng. Syst. Saf. **169** (2018), 179–186.
[67] J.C. Doyle and M. Csete, *Rules of engagement*, Nature **446** (2007), 860.
[68] J.C. Doyle and M. Csete, *Architecture, constraints, and behavior*, Proc. Natl. Acad. Sci. U. S. A. **108** (2011), 15624–15630.
[69] J.C. Doyle, D.L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, *The "robust yet fragile" nature of the internet*, Proc. Natl. Acad. Sci. U. S. A. **102** (2005), 14497–14502.
[70] D.A. Eisenberg, How to think about resilient infrastructure systems, Ph.D. thesis, Arizona State University, 2018.
[71] D.A. Eisenberg, D.L. Alderson, M. Kitsak, A. Ganin, and I. Linkov, *Network foundation for command and control (C2) systems: Literature review*, IEEE Access **6** (2018), 68782–68794.
[72] D.A. Eisenberg, T.P. Seager, and D.L. Alderson, *Rethinking resilience analytics*, Risk Anal. **39** (2019), 1870–1884.
[73] K. Engel, T. Kalinowski, and M.W.P. Savelsbergh, *Incremental network design with minimum spanning trees*, J. Graph Algorithms Appl. **21** (2017), 417–432.
[74] A. Faghih and M.A. Dahleh, *On enhancing resilience to cascading failures via post-disturbance tweaking of line reactances*, IEEE Trans. Power Syst. **34** (2019), 4921–4930.
[75] Y. Fang and G. Sansavini, *Emergence of antifragility by optimum postdisruption restoration planning of infrastructure networks*, J. Infrastruct. Syst. **23** (2017), 04017024.
[76] Y. Fang, C. Fang, E. Zio, and M. Xie, *Resilient critical infrastructure planning under disruptions considering recovery scheduling*, IEEE Trans. Eng. Manage. (2019), 1–15.
[77] Y.-P. Fang and G. Sansavini, *Optimum post-disruption restoration under uncertainty for enhancing critical infrastructure resilience*, Reliab. Eng. Syst. Saf. **185** (2019), 1–11.
[78] Y.-P. Fang and E. Zio, *An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards*, Eur. J. Oper. Res. **276** (2019), 1119–1136.
[79] A.A. Farrag and R.J. Dawson, *Designing optimal fault-tolerant star networks*, Networks **19** (1989), 707–716.
[80] R. Faturechi and E. Miller-Hooks, *Measuring the performance of transportation infrastructure systems in disasters: A comprehensive review*, J. Infrastruct. Syst. **21** (2015), 04014025.
[81] Federal Emergency Management Agency, *National Preparedness Goal*, second edn, Washington D.C., Department of Homeland Security, 2015.
[82] M. Finkel and M. Tlamim, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield*, Palo Alto, CA, Stanford University Press, 2011.
[83] C. Folke, *Resilience: The emergence of a perspective for social–ecological systems analyses*, Glob. Environ. Chang. **16** (2006), 253–267.
[84] B. Fortz, A.R. Mahjoub, S.T. McCormick, and P. Pesneau, *Two-edge connected subgraphs with bounded rings: Polyhedral results and branch-and-cut*, Math. Program. **105** (2006), 85–111.
[85] H. Fotouhi, S. Moryadee, and E. Miller-Hooks, *Quantifying the resilience of an urban traffic-electric power coupled system*, Reliab. Eng. Syst. Saf. **163** (2017), 79–94.
[86] Y. Fouquet, D. Nace, M. Pioro, M. Poss, and M. Zotkiewicz, *Generalized elastic flow rerouting scheme*, Networks **66** (2015), 267–281.
[87] R. Francis and B. Bekera, *A metric and frameworks for resilience analysis of engineered and infrastructure systems*, Reliab. Eng. Syst. Saf. **121** (2014), 90–103.
[88] D.R. Fulkerson and G.C. Harding, *Maximizing minimum source-sink path subject to a budget constraint*, Math. Program. **13** (1977), 116–118.
[89] Y. Gao, D. Simchi-Levi, C.-P. Teo, and Z. Yan, *Disruption risk mitigation in supply chains – The risk exposure index revisited*, Oper. Res. **67** (2019), 831–852.
[90] R. Gedik, H. Medal, C. Rainwater, E.A. Pohl, and S.J. Mason, *Vulnerability assessment and re-routing of freight trains under disruptions: A coal supply chain network application*, Transp. Res. E: Logist. Transp. Rev. **71** (2014), 45–57.
[91] P.M. Ghare, D.C. Montgomery, and W.C. Turner, *Optimal interdiction policy for a flow network*, Nav. Res. Logist. **18** (1971), 37–45.
[92] C. Ghedini, C. Ribeiro, and L. Sabattini, *Toward fault-tolerant multi-robot networks*, Networks **70** (2017), 388–400.
[93] N. Ghorbani-Renani, A.D. González, K. Barker, and N. Morshedlou, *Protection-interdiction-restoration: Tri-level optimization for enhancing interdependent network resilience*, Reliab. Eng. Syst. Saf. **199** (2020), 106907.

[94] R. Girão-Silva, B. Nedic, M. Gunkel, and T. Gomes, *Shared risk link group disjointness and geodiverse routing: A trade-off between benefit and practical effort*, Networks **75** (2020), 374–391.

[95] N. Goldbeck, P. Angeloudis, and W.Y. Ochieng, *Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models*, Reliab. Eng. Syst. Saf. **188** (2019), 62–79.

[96] B.L. Golden, *A problem in network interdiction*, Nav. Res. Logist. **25** (1978), 711–713.

[97] T. Gomes, L. Raposo, and G. Ellinas, *Dedicated protection of multicast sessions in mixed-graph sparse-splitting optical networks*, Networks **70** (2017), 360–372.

[98] A.D. González, L. Dueñas-Osorio, M. Sánchez-Silva, and A.L. Medaglia, *The interdependent network design problem for optimal infrastructure system restoration*, Comput. Aided Civil Inf. Eng. **31** (2016), 334–350.

[99] A.D. González, A. Chapman, L. Dueñas-Osorio, M. Mesbahi, and M.R. D'Souza, *Efficient infrastructure restoration strategies using the recovery operator*, Comput. Aided Civil Inf. Eng. **32** (2017), 991–1006.

[100] L. Gouveia and M. Leitner, *Design of survivable networks with vulnerability constraints*, Eur. J. Oper. Res. **258** (2017), 89–103.

[101] E. Grass and K. Fischer, *Two-stage stochastic programming in disaster management: A literature survey*, Surv. Oper. Res. Manage. Sci. **21** (2016), 85–100.

[102] F. Harary and J.P. Hayes, *Node fault tolerance in graphs*, Networks **27** (1996), 19–23.

[103] E.A. Heath, J.E. Mitchell, and T.C. Sharkey, *Applying ranking and selection procedures to long-term mitigation for improved network restoration*, EURO J. Comput. Optim. **4** (2016), 447–481.

[104] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, 2010. Potential indicators of cascading failure risk in power systems. https://cnls.lanl.gov/~chertkov/SmarterGrids/Talks/Hines2.pdf.

[105] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, *Topological models and critical slowing down: Two approaches to power system blackout risk analysis*, 2011 44th Hawaii International Conference on System Sciences, IEEE, 2011, pp. 1–10.

[106] P. Hines, E. Cotilla-Sanchez, B. O'hara, and C. Danforth, *Estimating dynamic instability risk by measuring critical slowing down*, 2011 IEEE Power and Energy Society General Meeting, IEEE, 2011, pp. 1–5.

[107] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, *Protection strategies for virtual network functions placement and service chains provisioning*, Networks **70** (2017), 373–387.

[108] C.S. Holling, *Resilience and stability of ecological systems*, Annu. Rev. Ecol. Syst. **4** (1973), 1–23.

[109] E. Hollnagel, *Resilience engineering and the built environment*, Build. Res. Inf. **42** (2014), 221–228.

[110] E. Hollnagel, J. Pariés, D.D. Woods, and J. Wreathall (eds), *Resilience Engineering in Practice: A Guidebook*, Ashgate Publishing, Ltd., Surrey, UK, 2013.

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

[112] S. Hosseini, K. Barker, and J.E. Ramirez-Marquez, *A review of definitions and measures of system resilience*, Reliab. Eng. Syst. Saf. **145** (2016), 47–61.

[113] S. Hosseini, D. Ivanov, and A. Dolgui, *Review of quantitative methods for supply chain resilience analysis*, Transp. Res. E: Logist. Transp. Rev. **125** (2019), 285–307.

[114] R. Houthooft, S. Sahhaf, W. Tavernier, F. De Turck, D. Colle, and M. Pickavet, *Optimizing robustness in geometric routing via embedding redundancy and regeneration*, Networks **66** (2015), 320–334.

[115] D. Huygens, M. Labbé, A.R. Mahjoub, and P. Pesneau, *The two-edge connected hop-constrained network design problem: Valid inequalities and branch-and-cut*, Networks **49** (2007), 116–133.

[116] S. Iloglu and L.A. Albert, *An integrated network design and scheduling problem for network recovery and emergency response*, Oper. Res. Perspect. **5** (2018), 218–231.

[117] S. Iloglu and L.A. Albert, *A maximal multiple coverage and network restoration problem for disaster recovery*, Oper. Res. Perspect. **7** (2020), 100132.

[118] E. Israeli and R.K. Wood, *Shortest path network interdiction*, Networks **40** (2002), 97–111.

[119] P. Jaillet and M.R. Wagner, "*Online optimization – An introduction*," *Risk and Optimization in an Uncertain World*, J.J. Hasenbein (ed.), Institute for Operations Research and Management Science, Hanover, MD, 2010, pp. 142–152.

[120] U. Janjarassuk and J. Linderoth, *Reformulation and sampling to solve a stochastic network interdiction problem*, Networks **52** (2008), 120–132.

[121] H.S. Jeong, J.H. Qiao, D.M. Abraham, M. Lawley, J.-P. Richard, and Y. Yih, *Minimizing the consequences of intentional attack on water infrastructure*, Comput. Aided Civil Inf. Eng. **21** (2006), 79–92.

[122] M. Jonsson, J. Rak, and A. Somani, *Preface: Design of resilient communication networks*, Networks **70** (2017), 281–282.

[123] I. Kalesnikau, M. Pióro, M. Poss, D. Nace, and A. Tomaszewski, *A robust optimization model for affine/quadratic flow thinning: A traffic protection mechanism for networks with variable link capacity*, Networks **75** (2020), 420–437.

[124] T. Kalinowski, D. Matsypura, and M.W.P. Savelsbergh, *Incremental network design with maximum flows*, Eur. J. Oper. Res. **242** (2015), 51–62.

[125] P. Kaplunovich and K. Turitsyn, *Fast and reliable screening of $n-2$ contingencies*, IEEE Trans. Power Syst. **31** (2016), 4243–4252.

[126] H. Kerivin and A.R. Mahjoub, *Design of survivable networks: A survey*, Networks **46** (2005), 1–21.

[127] T. Kim, S.J. Wright, D. Bienstock, and S. Harnett, *Analyzing vulnerability of power systems with continuous optimization formulations*, IEEE Trans. Netw. Sci. Eng. **3** (2016), 132–146.

[128] U.G. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*, Hoboken, NJ, Wiley, 2001.

[129] M. Kucharzak, K. Walkowiak, P. Kopec, D. Bulira, and A. Kasprzak, *Integer programming, constraint programming, and metaheuristic approaches for static optimization of anycast flows in elastic optical networks*, Networks **66** (2015), 253–266.

[130] Z. Lanir, *Fundamental surprises*, Decision Research, Eugene, OR, 1986.

[131] G. Laporte, J.A. Mesa, and F. Perea, *A game theoretic framework for the robust railway transit network design problem*, Transp. Res. B: Methodol. **44** (2010), 447–459.

[132] E.E. Lee, J.E. Mitchell, and W.A. Wallace, *Restoration of services in interdependent infrastructure systems: A network flows approach*, IEEE Trans. Syst. Man Cybernet. C: Appl. Rev. **37** (2007), 1303–1317.

[133] F. Liberatore, M.P. Scaparra, and M.S. Daskin, *Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification*, Comput. Oper. Res. **38** (2011), 357–366.

[134] A.L. Liestman, *Fault-tolerant broadcast graphs*, Networks **15** (1985), 159–171.

[135] T. Lin and Z. Zhou, *Robust network function virtualization*, Networks **75** (2020), 438–462.

[136] Y. Liu, G. Pedrielli, H. Li, L.H. Lee, C. Chen, and J.F. Shortle, *Optimal computing budget allocation for stochastic $N-k$ problem in the power grid system*, IEEE Trans. Reliab. **68** (2019), 778–789.

[137] I. Ljubić, P. Mutzel, and B. Zey, *Stochastic survivable network design problems: Theory and practice*, Eur. J. Oper. Res. **256** (2017), 333–348.

[138] R. Loggins, R.G. Little, J.E. Mitchell, T.C. Sharkey, and W.A. Wallace, *CRISIS: Modeling the restoration of interdependent civil and social infrastructure systems following an extreme event*, Nat. Hazards Rev. **20** (2019), 04019004.
[139] S.H. Low, *A duality model of TCP and queue management algorithms*, IEEE/ACM Trans. Netw. **11** (2003), 525–536.
[140] J.T. Margolis, K.M. Sullivan, S.J. Mason, and M. Magagnotti, *A multi-objective optimization model for designing resilient supply chain networks*, Int. J. Prod. Econ. **204** (2018), 174–185.
[141] L. Martins, T. Gomes, and D. Tipper, *Efficient heuristics for determining node-disjoint path pairs visiting specified nodes*, Networks **70** (2017), 292–307.
[142] T.C. Matisziw, A.T. Murray, and T.H. Grubesic, *Strategic network restoration*, Netw. Spatial Econ. **10** (2010), 345–361.
[143] L.R. Matthews, G.E. Gounaris, and I.G. Kevrekidis, *Designing networks with resiliency to edge failures using two-stage robust optimization*, Eur. J. Oper. Res. **279** (2019), 704–720.
[144] L.-G. Mattsson and E. Jenelius, *Vulnerability and resilience of transport systems – A discussion of recent research*, Transp. Res. A: Policy Pract. **81** (2015), 16–34.
[145] A.W. McMasters and T.M. Mustin, *Optimal interdiction of a supply network*, Nav. Res. Logist. **17** (1970), 261–268.
[146] D. Mendonça and W.A. Wallace, *Factors underlying organizational resilience: The case of electric power restoration in New York City after 11 September 2001*, Reliab. Eng. Syst. Saf. **141** (2015), 83–91.
[147] S.B. Miles, H.V. Burton, and H. Kang, *Community of practice for modeling disaster recovery*, Nat. Hazards Rev. **20** (2018), 04018023.
[148] E. Miller-Hooks, *Adaptive least-expected time paths in stochastic, time-varying transportation and data networks*, Networks **37** (2001), 35–52.
[149] P.M. Murray-Tuite and X.A. Fei, *A methodology for assessing transportation network terrorism risk with attacker and defender interactions*, Comput. Aided Civil Inf. Eng. **25** (2010), 396–410.
[150] K. Myslitski, J. Rak, and L. Kuszner, *Toward fast calculation of communication paths for resilient routing*, Networks **70** (2017), 308–326.
[151] C. Natalino, A. de Sousa, L. Wosinska, and M. Furdek, *Content placement in 5G-enabled edge/core data center networks resilient to link cut attacks*, Networks **75** (2020), 392–404.
[152] National Research Council, 2012. Disaster resilience: A national imperative. https://doi.org/10.17226/13457 .
[153] C. Nemeth, R. Wears, D. Woods, E. Hollnagel, and R. Cook, "*Minding the gaps: Creating resilience in health care*," *Advances in Patient Safety: New Directions and Alternative Approaches (Vol. 3: Performance and Tools)*, Agency for Healthcare Research and Quality (US), 2008.
[154] G. Nemeth and G. Retvari, *Rate-adaptive multipath routing: Distributed, centralized, and hybrid architectures*, Networks **66** (2015), 118–135.
[155] N. Ni, B.J. Howell, and T.C. Sharkey, *Modeling the impact of unmet demand in supply chain resiliency planning*, Omega **81** (2018), 1–18.
[156] P.J. Nicholas and D.L. Alderson, *Fast design of wireless mesh networks to defend against worst-case jamming*, Mil. Oper. Res. **23** (2018), 5–20.
[157] S.G. Nurre and T.C. Sharkey, *Integrated network design and scheduling problems with parallel identical machines: Complexity results and dispatching rules*, Networks **63** (2014), 306–326.
[158] S.G. Nurre and T.C. Sharkey, *Online scheduling problems with flexible release dates: Applications to infrastructure restoration*, Comput. Oper. Res. **92** (2018), 1–16.
[159] S.G. Nurre, B. Cavdaroglu, J.E. Mitchell, T.C. Sharkey, and W.A. Wallace, *Restoring infrastructure systems: An integrated network design and scheduling problem*, Eur. J. Oper. Res. **223** (2012), 794–806.
[160] F. Ordonez and J. Zhao, *Robust capacity expansion of network flows*, Networks **50** (2007), 136–145.
[161] F.P.B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, New York, Routledge, 2007.
[162] M. Ouyang, *Review on modeling and simulation of interdependent critical infrastructure systems*, Reliab. Eng. Syst. Saf. **121** (2014), 43–60.
[163] M. Ouyang, *A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks*, Eur. J. Oper. Res. **262** (2017), 1072–1084.
[164] M. Ouyang and Y. Fang, *A mathematical framework to optimize critical infrastructure resilience against intentional attacks*, Comput. Aided Civil Inf. Eng. **32** (2017), 909–929.
[165] F. Pan and D.P. Morton, *Minimizing a stochastic maximum-reliability path*, Networks **52** (2008), 111–119.
[166] A. Papachristodoulou, L. Li, and J.C. Doyle, *Methodological frameworks for large-scale network analysis and design*, Comput. Commun. Rev. **34** (2004), 7–20.
[167] D. Papadimitriou and B. Fortz, *A rolling horizon heuristic for the multiperiod network design and routing problem*, Networks **66** (2015), 364–379.
[168] J. Park, T.P. Seager, P.S.C. Rao, M. Convertino, and I. Linkov, *Integrating risk and resilience approaches to catastrophe management in engineering systems*, Risk Anal. **33** (2013), 356–367.
[169] A. Pasic, P. Babarczi, and J. Tapolcai, *Unambiguous switching link group failure localization in all-optical networks*, Networks **70** (2017), 327–341.
[170] R. Patriarca, J. Bergstrom, G. Di Gravio, and F. Costantino, *Resilience engineering: Current status of the research and future challenges*, Saf. Sci. **102** (2018), 79–100.
[171] B.S. Pay, J.R.W. Merrick, and Y. Song, *Stochastic network interdiction with incomplete preference*, Networks **73** (2019), 3–22.
[172] M. Poss and C. Raack, *Affine recourse for the robust network design problem: Between static and dynamic routing*, Networks **61** (2013), 180–198.
[173] D.K. Pradhan and F.J. Meyer, *Communication structures in fault-tolerant distributed systems*, Networks **23** (1993), 379–389.
[174] R. Rahmaniani, T.G. Crainic, M. Gendreau, and W. Rei, *Accelerating the Benders decomposition method: Application to stochastic network design problems*, SIAM J. Optim. **28** (2018), 875–903.
[175] J. Rak and J.P.G. Sterbenz, *Preface: Optimization issues in resilient network design and modeling*, Networks **66** (2015), 251–252.
[176] J. Rak, P.E. Heegaard, and B.E. Helvik, *Resilience of communication networks to random failures and disasters: An optimization perspective*, Networks **75** (2020), 337–339.
[177] A.W. Righi, T.A. Saurin, and P. Wachs, *A systematic literature review of resilience engineering: Research areas and a research agenda proposal*, Reliab. Eng. Syst. Saf. **141** (2015), 142–152.
[178] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies*, IEEE Control Syst. Mag. **21** (2001), 11–25.
[179] C.M. Rocco, J.E. Ramirez-Marquez, D.E. Salazar, and C. Yajure, *Assessing the vulnerability of a power system through a multiple objective contingency screening approach*, IEEE Trans. Reliab. **60** (2011), 394–403.
[180] M. Rysz, P.A. Krokhmal, and E.L. Pasiliao, *Detecting resilient structures in stochastic networks: A two-stage stochastic optimization approach*, Networks **69** (2017), 189–204.
[181] J. Salmerón, *Deception tactics for network interdiction: A multiobjective approach*, Networks **60** (2012), 45–58.

[182] J. Salmerón and R.K. Wood, *The value of recovery transformers in protecting an electric transmission grid against attack*, IEEE Trans. Power Syst. **30** (2015), 96–104.
[183] J. Salmerón, R.K. Wood, and R. Baldick, *Analysis of electric grid security under terrorist threat*, IEEE Trans. Power Syst. **19** (2004), 905–912.
[184] J. Salmerón, R.K. Wood, and R. Baldick, *Worst-case interdiction analysis of large-scale electric power grids*, IEEE Trans. Power Syst. **24** (2009), 96–104.
[185] E. Sanci and M.S. Daskin, *Integrating location and network restoration decisions in relief networks under uncertainty*, Eur. J. Oper. Res. **279** (2019), 335–350.
[186] H. Sarhadi, D.M. Tulett, and M. Verma, *An analytical approach to the protection planning of a rail intermodal terminal network*, Eur. J. Oper. Res. **257** (2017), 511–525.
[187] T.A. Saurin and N.J.B. Werle, *A framework for the analysis of slack in socio-technical systems*, Reliab. Eng. Syst. Saf. **167** (2017), 439–451.
[188] M.P. Scaparra and R.L. Church, *An exact solution approach for the interdiction median problem with fortification*, Eur. J. Oper. Res. **189** (2008), 76–92.
[189] M. Scheffer, S.R. Carpenter, T.M. Lenton, J. Bascompte, W. Brock, V. Dakos, J. Van de Koppel, I.A. Van de Leemput, S.A. Levin, E.H. Van Nes, M. Pascual, and J. Vandermeer, *Anticipating critical transitions*, Science **338** (2012), 344–348.
[190] M. Schmitz, V.J. Garcia, and D.P. Bernardon, *Matheuristic for emergency response in the electric distribution system with unforeseen islanding*, Electr. Power Syst. Res. **169** (2019), 1–17.
[191] K.M. Schumacher, A.E.M. Cohn, and R.L.-Y. Chen, *Algorithm for the $n-2$ security-constrained unit commitment problem with transmission switching*, INFORMS J. Comput. **29** (2017), 645–659.
[192] T.P. Seager, S.S. Clark, D.A. Eisenberg, J.E. Thomas, M.M. Hinrichs, R. Kofronand, C.N. Jensen, L.R. McBurnett, M. Snell, and D.L. Alderson, "*Redesigning resilient infrastructure research*," *Resilience and Risk*, I. Linkov and J.M. Palma-Oliveira (eds), Heidelberg, Germany, Springer, 2017, pp. 81–119.
[193] J.A. Sefair and J.C. Smith, *Dynamic shortest-path interdiction*, Networks **68** (2016), 315–330.
[194] J.A. Sefair and J.C. Smith, *Exact algorithms and bounds for the dynamic assignment interdiction problem*, Nav. Res. Logist. **64** (2017), 373–387.
[195] A. Sen, A. Mazumder, S. Banerjee, A. Das, C. Zhou, and S. Shirazipourazad, *Region-based fault-tolerant distributed file storage system design in networks*, Networks **66** (2015), 380–395.
[196] T.C. Sharkey, B. Cavdaroglu, H. Nguyen, J. Mitchell, and W. Wallace, *Interdependent network restoration: On the value of information-sharing*, Eur. J. Oper. Res. **244** (2015), 309–321.
[197] T.C. Sharkey, S.G. Nurre, H. Nguyen, J.H. Chow, J.E. Mitchell, and W.A. Wallace, *Identification and classification of restoration interdependencies in the wake of Hurricane Sandy*, J. Infrastruct. Syst. **22** (2016), 04015007.
[198] S. Shen and J.C. Smith, *Polynomial-time algorithms for solving a class of critical node problems on trees and series-parallel graphs*, Networks **60** (2012), 103–119.
[199] J. Silva, T. Gomes, D. Tipper, L. Martins, and V. Kounev, *An effective algorithm for computing all-terminal reliability bounds*, Networks **66** (2015), 282–295.
[200] M. Silva, M. Poss, and N. Maculan, *Solving the bifurcated and nonbifurcated robust network loading problem with k-adaptive routing*, Networks **72** (2018), 151–170.
[201] A.M. Smith, A.D. González, L. Dueñas-Osorio, and R.M. D'Souza, *Interdependent network recovery games*, Risk Anal. **40** (2020), 134–152.
[202] J.C. Smith and Y. Song, *A survey of network interdiction models and algorithms*, Eur. J. Oper. Res. **283** (2020), 797–811.
[203] L.V. Snyder, *Facility location under uncertainty: A review*, IIE Trans. **38** (2006), 537–554.
[204] L.V. Snyder, Z. Atan, P. Peng, Y. Rong, A.J. Schmitt, and B. Sinsoysal, *OR/MS models for supply chain disruptions: A review*, IIE Trans. **48** (2016), 89–109.
[205] K. Sundar, C. Coffrin, H. Nagarajan, and R. Bent, *Probabilistic $N-k$ failure-identification for power systems*, Networks **71** (2018), 302–321.
[206] Y. Tan, A.K. Das, P. Arabshahi, and D.S. Kirschen, *Distribution systems hardening against natural disasters*, IEEE Trans. Power Syst. **33** (2018), 6849–6860.
[207] Y. Tan, F. Qiu, A.K. Das, D.S. Kirschen, P. Arabshahi, and J. Wang, *Scheduling post-disaster repairs in electricity distribution networks*, IEEE Trans. Power Syst. **34** (2019), 2611–2621.
[208] S.E. Terblanche, R. Wessaly, and J.M. Hattingh, *Survivable network design with demand uncertainty*, Eur. J. Oper. Res. **210** (2011), 10–26.
[209] J.E. Thomas, D.A. Eisenberg, T.P. Seager, and E. Fisher, *A resilience engineering approach to integrating human and socio-technical system capacities and processes for national infrastructure resilience*, J. Homeland Secur. Emerg. Manage. **16** (2019).
[210] E.L. Tucker, M.S. Daskin, B.V. Sweet, and W.J. Hopp, *Incentivizing resilient supply chain design to prevent drug shortages: Policy analysis using two- and multi-stage stochastic programs*, IISE Trans. **52** (2020), 394–412.
[211] A. Ulusan and O. Ergun, *Restoration of services in disrupted infrastructure systems: A network science approach*, PLoS ONE **13** (2018), e0192272.
[212] B. Vass, L. Németh, and J. Tapolcai, *The Earth is nearly flat: Precise and approximate algorithms for detecting vulnerable regions of networks in the plane and on the sphere*, Networks **75** (2020), 340–355.
[213] Q. Wang, J. Watson, and Y. Guan, *Two-stage robust optimization for $N-k$ contingency-constrained unit commitment*, IEEE Trans. Power Syst. **28** (2013), 2366–2375.
[214] Y. Wang and R. Baldick, *Interdiction analysis of electric grids combining cascading outage and medium-term impacts*, IEEE Trans. Power Syst. **29** (2014), 2160–2168.
[215] Y. Wang, C. Chen, J. Wang, and R. Baldick, *Research on resilience of power systems under natural disasters – A review*, IEEE Trans. Power Syst. **31** (2016), 1604–1613.
[216] R. Wollmer, *Removing arcs from a network*, Oper. Res. **12** (1964), 934–940.
[217] R.K. Wood, *Deterministic network interdiction*, Math. Comput. Model. **17** (1993), 1–18.
[218] D.D. Woods, "*Essentials of resilience, revisited. Chapter 4*," *Handbook on Resilience of Socio-Technical Systems*, M. Ruth and S. Goessling-Reisemann (eds), Northampton, MA, Edward Elgar Publishing, 2019.
[219] D.D. Woods, *Risk and human performance: Measuring the potential for disaster*, Reliab. Eng. Syst. Saf. **29** (1990), 387–405.
[220] D.D. Woods, *Four concepts for resilience and the implications for the future of resilience engineering*, Reliab. Eng. Syst. Saf. **141** (2015), 5–9.
[221] D.D. Woods, *The theory of graceful extensibility: Basic rules that govern adaptive systems*, Environ. Syst. Decis. **38** (2018), 433–457.
[222] D.D. Woods and M. Branlat, "*Basic patterns in how adaptive systems fail*," *Resilience Engineering Perspectives Volume 3: Resilience Engineering in Practice*, E. Hollnagel, J. Pariès, D.D. Woods, and J. Wreathall (eds), Surrey, UK, Ashgate, 2011, pp. 127–144.
[223] D.D. Woods and J. Wreathall, *Stress-strain plots as a basis for assessing system resilience*, Resilience Eng. Perspect. **1** (2008), 145–161.

[224] D.D. Woods, Y.J. Chan, and J. Wreathall, *The stress–strain model of resilience operationalizes the four cornerstones of resilience engineering*, 5th Resilience Engineering Symposium, 2014, pp. 17–22.
[225] S. Yang, S. Trajanovski, and F.A. Kuipers, *Availability-based path selection and network vulnerability assessment*, Networks **66** (2015), 306–319.
[226] I. Yanıkoglu, B.L. Gorissen, and D. den Hertog, *A survey of adjustable robust optimization*, Eur. J. Oper. Res. **277** (2019), 799–813.
[227] W. Yuan, L. Zhao, and B. Zeng, *Optimal power grid protection through a defender-attacker-defender model*, Reliab. Eng. Syst. Saf. **121** (2014), 83–89.
[228] X.-Y. Zhang, Z. Zheng, and K.-Y. Cai, *A fortification model for decentralized supply systems and its solution algorithms*, IEEE Trans. Reliab. **67** (2018), 381–400.
[229] S. Zhao, Y. Zou, X. Lin, D. Aliprantis, H. Villegas, M. Chen, and A. Castillo, *Leveraging generators with complementary capabilities for robust multi-stage power grid operations*, IEEE Trans. Control Netw. Syst. **7** (2020), 1441–1452.

How to cite this article: Sharkey TC, Nurre Pinkley SG, Eisenberg DA, Alderson DL. In search of network resilience: An optimization-based view. *Networks.* 2021;77:225–254. https://doi.org/10.1002/net.21996