# A Robust Optimization Approach to Backup Network Design With Random Failures

Matthew Johnston, *Student Member, IEEE*, Hyang-Won Lee, *Associate Member, IEEE*, and Eytan Modiano, *Fellow, IEEE*

***Abstract*—This paper presents a scheme in which a dedicated backup network is designed to provide protection from random link failures. Upon a link failure in the primary network, traffic is rerouted through a preplanned path in the backup network. We introduce a novel approach for dealing with random link failures, in which probabilistic survivability guarantees are provided to limit capacity overprovisioning. We show that the optimal backup routing strategy in this respect depends on the reliability of the primary network. Specifically, as primary links become less likely to fail, the optimal backup networks employ more resource sharing among backup paths. We apply results from the field of robust optimization to formulate an ILP for the design and capacity provisioning of these backup networks. We then propose a simulated annealing heuristic to solve this problem for large-scale networks and present simulation results that verify our analysis and approach.**

***Index Terms*—Backup network design, random failures, robust optimization.**

## I. Introduction

TODAY'S backbone networks are designed to operate at very high data rates, now exceeding 10 Gb/s [1]. Consequently, any link failure can lead to catastrophic data loss. In order to ensure fast recovery from failures, protection resources must be allocated prior to any network failures. This paper deals with providing protection in networks from multiple random link failures.

A widely used approach for recovery from a link failure is *preplanned link restoration* [2], where a backup path between the end nodes of a link is chosen for every link during the network configuration stage. In the event of a link failure, the disrupted traffic can be rerouted onto its backup path. Preplanned methods of link restoration offer benefits over other methods in terms of speed and simplicity of failure recovery, as no additional dynamic routing is necessary at the time of a failure [3]. In addition to designing a backup path for each link, preplanned link restoration requires provisioning of sufficient spare capacity along each backup path to carry the load of failed links. Backup paths can share spare capacity and network resources to reduce the total cost of protection.

Communication networks can suffer from multiple simultaneous failures, for example, if a second link fails before a first failed link is repaired. Furthermore, natural disasters or large-scale attacks can destroy several links in the vicinity of such events. Preplanning backup paths for combinations of multiple failures can be complex and impractical and can lead to significant capacity overprovisioning. Consequently, new approaches must be considered to offer protection against multiple failures.

Spare capacity allocation for link-based protection has been studied extensively in the context of single-link failures [1], [4]–[6]. The objective of these works is to allocate sufficient protection resources to recover from any single-link failure. Recently, the authors in [7] proposed the use of a dedicated backup network to protect against a single failure on the primary network. Upon such a failure, the load on the failed link is routed on a predetermined path on the backup network. The authors provide an integer linear program (ILP) to design an optimal backup network with minimal cost. They show that the cost of the optimal backup network is small relative to that of a large primary network. Specifically, they show that the ratio between the total backup capacity and the total primary capacity tends to zero as the network size grows large for certain classes of networks.

For many applications, it is insufficient to protect against only single-link failure events. Several authors have extended the results of survivability for single-link failures to dual-link failures [2], [8], [9]. The work in [10] considers protecting against up to three link failures. Most of these works require the primary network to have multiple disjoint paths between node pairs to survive multiple failures. This assumption is too restrictive when considering a large number of failures. Additionally, [11] provides a spare capacity allocation approach based on a specific set of failure events and restricted backup path lengths. However, in all of these works, large amounts of spare capacity are required if many links can fail simultaneously. The work in [12] addresses this problem by providing incremental survivability improvements for a fixed amount of additional capacity

Manuscript received October 23, 2012; revised June 01, 2013 and November 27, 2013; accepted April 16, 2014; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor S. Ramasubramanian. Date of publication May 09, 2014; date of current version August 14, 2015. This work was supported by the NSF under Grants CNS-1116209, CNS-0830961, and CNS-1017800 and the DTRA under Grants HDTRA1-07-1-0004 and HDTRA-09-1-005. The work of H.-W. Lee was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning under Grant 2012R1A1A1012610. *(Corresponding author: Hyang-Won Lee.)*

M. Johnston is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: mrj@mit.edu).

H.-W. Lee is with the Department of Internet and Multimedia Engineering, Konkuk University, Seoul 143-701, Korea (e-mail:leehw@konkuk.ac.kr).

E. Modiano is with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: modiano@mit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNET.2014.2320829

and shows that a substantial degree of protection can be provided for limited excess capacity.

Survivability amid multiple failures has also been addressed in the form of a shared risk link group (SRLG) [13]. An SRLG is a set of links sharing a common network resource, such that a failure of that resource could lead to a failure of all links in the SRLG. Many authors have proposed routing strategies for path-based protection against SRLG failures [14]–[17]. These works assume that links in an SRLG all fail simultaneously and deterministically. However, this line of work does not extend to uncorrelated, nondeterministic failures.

In this paper, we introduce a new framework for providing protection from multiple random link failures involving probabilistic survivability guarantees. Since large-scale attacks and natural disasters can result in multiple links failing randomly, providing protection from any single failure is insufficient, and networks designed for protection against single-link failures often cannot protect against multiple failures. The straightforward approach of offering guaranteed protection against any random failure scenario is to allocate capacity such that every failure event is protected. However, this approach is impractical as it requires enormous amounts of capacity to protect against potentially unlikely events. To address this issue, we take an alternative approach that provides a probabilistic protection guarantee. This approach significantly reduces the cost of protection by guaranteeing recovery from failures with high probability.

Motivated by the results of [7] and the simplicity of their approach, we extend the use of a dedicated backup network to deal with multiple random link failures. We show that a dedicated backup network is a low-cost method of providing protection against random failures, relative to large primary networks. Specifically, we show a dedicated backup network can often be constructed to provide protection with high probability using roughly half of the capacity needed to provide full protection guarantees. Additionally, we show that the structure of the minimum-cost backup network changes with the reliability of the primary network. Specifically, optimal backup networks for primary networks with a low link-failure probability employ a high level of link sharing among backup paths. On the other hand, optimal backup networks for primary networks with a high link-failure probability emphasize shorter backup paths and less capacity sharing.

Throughout this paper, we assume that links on the primary network fail with some probability, and links on the backup network are free from failure. Often, the links making up the backup network can be made robust via hardening or shielding, thus making them more resistant to failure. This is particularly relevant for failures due to physical link cuts. Yet, it is possible to extend this work to the case of unreliable backup links, as discussed in Section VI.

To design a backup network under random link failures, we develop a robust optimization approach to backup capacity provisioning. Robust optimization finds a solution to a problem that is robust to uncertainty in the optimization parameters [18]–[20]. In [20], Bertsimas and Sim propose a novel linear formulation with an adjustable level of robustness. These techniques have previously been successfully applied to

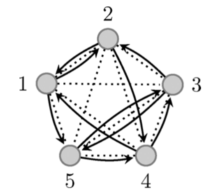


Fig. 1. Example backup network shown as solid directed links over dotted bidirectional primary network.

network flow problems [21]. We apply these results to design backup networks that are robust to the uncertainty in link failures. This leads to an ILP formulation for backup capacity provisioning. We also present a simulated annealing approach to solve the ILP for large-scale networks.

The remainder of this paper is organized as follows. In Section II, we present the network model and formulate the problem of backup network design. In Section III, we consider protection for uniform-load primary networks to investigate the impact of link failure probability on backup network design and the cost of protection. Robust optimization is introduced in Section IV to formulate an ILP for general primary link loads, and a heuristic based on simulated annealing is presented to solve it for large networks. We present simulation results in Section V. In Section VI, we consider several extensions to the survivability model, and we present concluding remarks in Section VII.

## II. Network Model

Consider a primary network made up of a set of nodes $\mathcal{V}$ and a set of directed links $\mathcal{L}$ connecting these nodes. We assume throughout that the links are directed, as the undirected case is a specific instance of the directed link case.

Each link $(s,d) \in \mathcal{L}$ has a given primary link capacity $C^{\mathrm{P}}_{sd}$, and a positive probability of failure $p$, independent of all other links. Let the random variables $X_{sd}$ equal 1 if link $(s,d)$ fails, and 0 otherwise. This probabilistic failure model represents a snapshot of a network where links fail and are repaired according to some Markovian process. Hence, $p$ represents the steady-state probability that a physical link is in a failed state. This model has been adopted by several previous works [6], [22]–[24]. A backup network is to be constructed over the same set of nodes $\mathcal{V}$ and a new set of links $\mathcal{L}_{\mathrm{B}}$, by routing a backup path for each primary link over the backup network and allocating capacity to every backup link. We assume that $\mathcal{L}_{\mathrm{B}}$ can consist only of links $(i,j)$ if there is a primary link connecting nodes $i$ and $j$. An example backup network is shown in Fig. 1. Note that not all links in $\mathcal{L}_{\mathrm{B}}$ will be used as backup links. Backup paths are routed over the links in $\mathcal{L}_{\mathrm{B}}$, and thus the resulting backup network topology consists of the links in $\mathcal{L}_{\mathrm{B}}$ that are used by the backup routing $[b^{sd}_{ij}, (i,j) \in \mathcal{L}_{\mathrm{B}}, (s,d) \in \mathcal{L}]$. Furthermore, the backup links are designed such that failures can only occur in the primary network. For each primary link $(s,d) \in \mathcal{L}$, a path on the backup network is chosen such that in the event that $(s,d)$ fails, the traffic load on $(s,d)$ is rerouted over the backup path. Let $b^{sd}_{ij} = 1$ if link $(s,d) \in \mathcal{L}$ uses backup link $(i,j) \in \mathcal{L}_{\mathrm{B}}$ in its

TABLE I
LIST OF COMMONLY USED NOTATIONS

| Variable | Definition |
|---|---|
| $\mathcal{L}$ | Set of links in the primary network. |
| $\mathcal{L}_B$ | Set of backup link candidates. |
| $C_{sd}^P$ | Capacity of primary link $(s,d)$ |
| $C_{ij}^B$ | Capacity of backup link $(i,j)$ |
| $b_{sd}^{ij}$ | Binary variable indicating the use of backup link $(i,j)$ by primary link $(s,d)$. |
| $p$ | Probability of link failure |
| $\epsilon$ | Survivability guarantee parameter |
| $X_{sd}$ | Random variable indicating failure of primary link $(s,d)$ |
| $n_{ij}$ | Number of primary links using backup link $(i,j)$. |
| $\Gamma_{ij}$ | Robustness paramater for backup link $(i,j)$. |

backup path. Hence, $b^{sd} = \{b_{ij}^{sd} | \forall (i,j) \in \mathcal{L}_{\rm B}\}$ represents the backup path for the primary link $(s,d) \in \mathcal{L}$.

A capacity $C_{ij}^{\rm B}$ is allocated to each backup link $(i,j) \in \mathcal{L}_{\rm B}$ such that $(i,j)$ can support the increased load due to a random failure scenario with probability $1-\epsilon$, where $\epsilon > 0$ is a design parameter. Naturally, as $\epsilon$ becomes smaller, more capacity is required on the backup network. Throughout this work, we only consider the case where $p > \epsilon$ since no backup capacity is required for $p \le \epsilon$. A summary of the notations throughput this paper is provided in Table I.

Each primary link has exactly one path in the backup network for protection, and the links in this path can be shared among backup paths for multiple primary links. The goal is to construct a minimal cost dedicated backup network. The problem can be formulated as follows:

Minimize:

$$\sum_{(i,j)\in\mathcal{L}_{\rm B}} C_{ij}^{\rm B}. \tag{1}$$

Subject To:

$$\mathbf{P}\left(\sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\rm P} > C_{ij}^{\rm B}\right) \le \epsilon \qquad \forall (i,j) \in \mathcal{L}_{\rm B} \tag{2}$$

$$\sum_j b_{ij}^{sd} - \sum_j b_{ji}^{sd} = \begin{cases} 1, & \text{if } s=i \\ -1, & \text{if } d=i \\ 0, & \text{o.w.} \end{cases} \qquad \forall (s,d)\in\mathcal{L}, i\in\mathcal{V} \tag{3}$$

$$b_{ij}^{sd}, \in \{0,1\} \qquad \forall (s,d) \in \mathcal{L}, (i,j) \in \mathcal{L}_{\rm B}. \tag{4}$$

The constraint in (3) is a standard flow conservation constraint for the routing of a single backup path for each primary link. The probabilistic constraint (2) is the capacity constraint, from which the backup capacities are computed. Backup link $(i,j)$ must carry the load of each failed primary link that it protects. Constraint (2) restricts the probability that the load on $(i,j)$ due to failures exceeds the backup capacity provisioned on $(i,j)$. This survivability metric, which considers the reliability of each backup link independently, is referred to as the backup-link survivability metric. There are a number of possible survivability metrics that can be considered in this setting, the choice of which will impact the network design. One can consider survivability from a primary link perspective. In this case, one constrains the joint probability that a primary link fails and its backup path has insufficient capacity. Alternatively, one can consider a survivability constraint on the entire backup network, rather than on each backup link independently. The backup-network constraint restricts the probability that *any* of the backup links have insufficient capacity. It is straightforward to show that the primary-link and backup-network constraints can be written in the form of the backup-link constraint in (2) using a union-bound argument. Therefore, we will use the backup-link constraint of (2) throughout this paper.

We start by considering the backup network design problem for networks with uniform primary link loads. In Section IV, this is generalized to primary networks with arbitrary primary link capacities.

## III. UNIFORM-LOAD NETWORKS

Any primary network can be represented by a fully connected graph, with $C_{sd}^{\rm P} = 0$ for links that are not in the primary network. However, in order to form an intuitive understanding of the general problem, we first explore the backup-network design problem for the special case where each primary link has unit capacity, i.e., $C_{sd}^{\rm P} = 1 \quad \forall (s,d) \in \mathcal{L}$. The capacity required on each backup link is dictated by the reliability constraint in (2). Let $n_{ij}$ be the number of primary links for which backup link $(i,j)$ is part of the backup path. In other words

$$n_{ij} = \sum_{(s,d)\in\mathcal{L}} b_{ij}^{sd}. \tag{5}$$

Let $Y_{ij}$ be a random variable representing the number of failed primary links using $(i,j)$ as part of their backup paths, i.e.,

$$Y_{ij} = \sum_{(s,d)\in\mathcal{L}} b_{ij}^{sd} X_{sd}. \tag{6}$$

Since each $X_{sd}$ is an i.i.d. Bernoulli random variable with parameter $p$, $Y_{ij}$ is a binomial random variable with parameters $n_{ij}$ and $p$. Furthermore, as all the primary links have unit capacity, (2) can be rewritten as

$$\mathbf{P}\left(\sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\rm P} > C_{ij}^{\rm B}\right) = \mathbf{P}\left(Y_{ij} > C_{ij}^{\rm B}\right) \tag{7}$$

$$= \sum_{y=\lfloor C_{ij}^{\rm B}\rfloor+1}^{n_{ij}} \binom{n_{ij}}{y} p^y (1-p)^{n_{ij}-y} \le \epsilon \qquad \forall (i,j)\in\mathcal{L}_{\rm B}. \tag{8}$$

Equation (8) uses the cumulative distribution function (CDF) of the binomial distribution. For each link $(i,j)$, let $\mathrm{G}(n_{ij}, p, \epsilon)$ be the minimum value of $C_{ij}^{\rm B}$ satisfying (8). Clearly, the capacity required on a backup link increases with the number of primary links it protects, and it decreases as the probability of failure decreases. Additionally, as $\epsilon$ decreases, more capacity is required on each backup link.

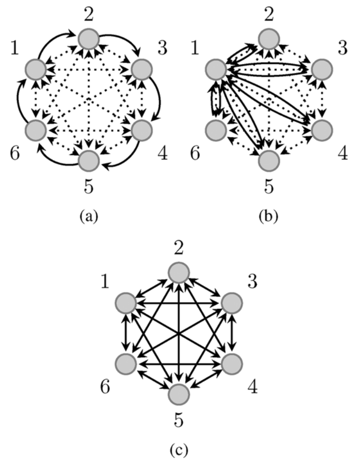


Fig. 2. Sample backup network link placement to protect a 6-node, fully connected primary network. The dotted lines represent the primary network, and the solid lines represent the backup links. (a) Cycle protection. (b) Two-hop protection. (c) One-hop protection.

### *A. Impact of Link Failure Probability*

To gain intuition about the optimal backup network design, we compare three backup routing schemes, shown in Fig. 2, and show that backup network performance depends on the link failure probability. In the cycle protection scheme of Fig. 2(a), each primary link $(s, d)$ has a backup path lying in a single Hamiltonian cycle through the network. This is the minimum-cost backup network providing protection against a single-link failure [7]. Each backup link in this cycle requires unit capacity to protect against a single-link failure, resulting in a total cost of $N$ for an $N$-node network. Due to network symmetry, each backup link protects half of the primary links. Therefore, in order to use this scheme to provide protection from a random number of failures with high probability, a total backup capacity of $C^{\mathrm{B}}_{\mathrm{total}} = N \cdot \mathrm{G}\big(\frac{N(N-1)}{2}, p, \epsilon\big)$ is required, where $\mathrm{G}(n, p, \epsilon)$ is the smallest value of $C^{\mathrm{B}}_{ij}$ satisfying (8).

For small values of $p$, only a small number of links will likely fail, and in this case, it is sufficient to provide protection against a small number of failures. Therefore, it is conceivable that for sufficiently small $p$, the optimal backup network topology is the same as the optimal topology for protecting against single-link failures [such as the one in Fig. 2(a)]. Specifically, a backup topology protecting against single-link failures, as designed in [7], is sufficient for our problem if the probability of having more than one link failure is less than $\epsilon$. The following proposition characterizes the region over which it is sufficient to provide protection against only a single failure.

*Proposition 1:* Let $M$ be the total number of primary links. Then, protecting against single-link failures is sufficient if

$$p \leq \frac{\sqrt{\epsilon}}{M-1}. \tag{9}$$

*Proof:* Assume that a link is used as a backup by $k \geq 1$ primary links. Protecting against a single failure is sufficient if

$$\mathbf{P}\big(\text{More than 1 failure}\big) \leq \epsilon \tag{10}$$

$$1 - (1-p)^k - kp(1-p)^{k-1} \leq \epsilon. \tag{11}$$

The left-hand side of the above inequality can be upper-bounded as follows:

$$\begin{aligned} &1 - (1-p)^k - kp(1-p)^{k-1} \\ &\quad = 1 - (1-p)^{k-1}(1 + (k-1)p) && (12)\\ &\quad \leq 1 - (1-(k-1)p)(1+(k-1)p) && (13)\\ &\quad = 1 - (1-(k-1)^2p^2) && (14)\\ &\quad = (k-1)^2p^2 && (15)\\ &\quad \leq (M-1)^2p^2 && (16)\end{aligned}$$

where the inequality in (13) follows from Bernoulli's Inequality, and the inequality in (16) follows since the number of primary links protected by each backup link is necessarily smaller than $M$, the total number of primary links. Therefore, for values of $p$ satisfying (9), protecting against single link failures is sufficient. ■

Note that in order to require protection to begin with, we must have $p > \epsilon$. Therefore, if $\epsilon < \frac{1}{(M-1)^2}$, then a backup network designed for single link failures is optimal for

$$\epsilon \leq p < \frac{\sqrt{\epsilon}}{M-1}. \tag{17}$$

Therefore, in the scenario of Fig. 2, the cycle protection scheme yields the optimal backup network when

$$\epsilon < p \leq \frac{\sqrt{\epsilon}}{N^2 - N - 1} \tag{18}$$

since the total number of primary links is $N(N-1)$. As discussed above, the total backup capacity of cycle protection is given by $N \cdot \mathrm{G}(\frac{N(N-1)}{2}, p, \epsilon)$, which equals $N$ when (18) is satisfied.

For sufficiently large values of $p$, the backup capacity required by this topology is $\frac{N^2(N-1)}{2}$ since $\mathrm{G}(n_{ij}, p, \epsilon) = n_{ij}$ for $p$ close to 1. This capacity can be reduced by considering the scheme in Fig. 2(c), where the backup network is a mirror of the primary network, and the backup path for $(s, d)$ is the one-hop path from $s$ to $d$. Since each backup link offers protection to a single primary link, the total capacity required is $C^{\mathrm{B}}_{\mathrm{total}} = N(N-1) \cdot \mathrm{G}(1, p, \epsilon)$. For all values of $p > \epsilon$, $C^{\mathrm{B}}_{\mathrm{total}} = N(N-1)$. Thus, the mirror scheme requires a factor of $N$ less capacity than the cycle scheme for primary networks with a high probability of link failure.

It is clear that for values of $p$ close to 1, each link requires dedicated backup capacity to protect against its probable failure. Consequently, a shortest-path backup routing scheme, as provided by the one-hop protection scheme, minimizes the total backup capacity. For example, if the probability that every link fails is greater than $\epsilon$, then every primary link requires dedicated backup capacity, and therefore the one-hop topology is optimal. While the one-hop protection scheme is preferred in the high-$p$ regime, other schemes are more capacity-efficient for smaller values of $p$. Consider the two-hop scheme in Fig. 2(b), where node 1 serves as a relay node for every backup path. The primary links from node 2 to every other node share the backup link (2, 1) and, similarly, the primary links from all nodes to node 2 share the backup link $(1, 2)$. Extending this to an $N$-node

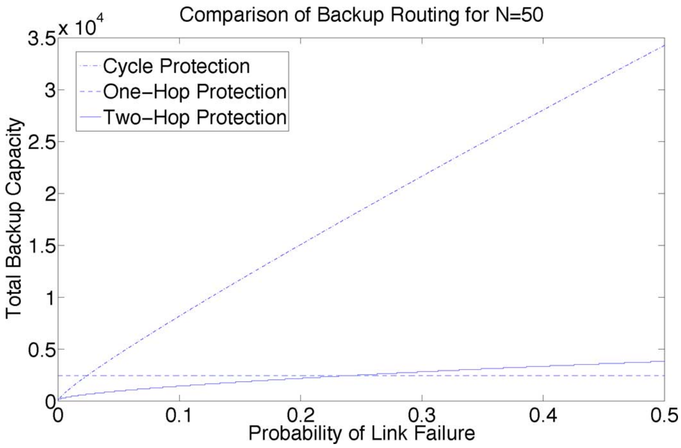


Fig. 3. Comparison of three protection schemes for an $N = 50$ fully connected network with unit load and $\epsilon = 0.0001$.

network, each backup link protects $N-1$ primaries, and there are $2(N-1)$ backup links. Thus, $C^{\rm B}_{\rm total} = 2(N-1)\cdot {\rm G}(N-1,p,\epsilon)$.

The three aforementioned routing schemes are compared in Fig. 3 for a fully connected network with 50 nodes and varying probability of link failure. The cycle-protection scheme, which is optimal in the single-failure scenario, is optimal for very small values of $p$ ($p \in [\epsilon, 0.0004]$), but requires excessive capacity for larger $p$. For small values of $p$ beyond that region, the two-hop routing strategy outperforms the other two strategies. Once $p$ exceeds roughly 0.25, there is no longer a benefit to sharing backup resources, and the one-hop starts to outperform the two-hop schemes. Hence, it is clear that the optimal backup network topology depends on the reliability of the primary network. This is further analyzed in Section IV where the problem is formulated for general primary link capacities.

### B. Scaling Properties of Backup Network Capacity

Consider the cost of the backup network with respect to that of the primary network. Let $\rho$ be defined as

$$\rho \triangleq \frac{\sum_{(i,j)\in\mathcal{L}_{\rm B}} C^{\rm B}_{ij}}{\sum_{(i,j)\in\mathcal{L}} C^{\rm P}_{ij}}. \tag{19}$$

That is, $\rho$ is the ratio of the total capacity of the optimal backup network to that of the primary network. In [7], the authors show that this ratio tends to 0 asymptotically as the network size gets very large for specific networks and single-failure protection. For fully connected, uniform-load networks, the optimal backup network under single-failure protection is shown in Fig. 2(a), and for this topology

$$\rho = \frac{N}{N(N-1)} = \frac{1}{N-1}. \tag{20}$$

Conversely, for protection against random failures, the ratio in (19) can be upper-bounded using the following proposition.

*Proposition 2:* Assuming a fully connected primary network with unit-capacity on each link and probability of link failure $p$, the ratio between the total capacity of the optimal backup network and that of the primary network can be upper-bounded as the primary network size grows large by the following:

$$\rho \le 2p. \tag{21}$$

*Proof:* The optimal total backup capacity is bounded by that of the two-hop scheme considered in Fig. 2(b)

$$\rho = \frac{\sum_{(i,j)\in\mathcal{L}_{\rm B}} C^{\rm B}_{ij}}{\sum_{(i,j)\in\mathcal{L}} C^{\rm P}_{ij}} \le \frac{2(N-1){\rm G}(N-1,p,\epsilon)}{N(N-1)}. \tag{22}$$

Consider the behavior of $G(n,p,\epsilon)$ when $n$ is large. Recall that $G(n,p,\epsilon)$ is the required number of primary links out of $n$ that need to be protected to ensure a probability of error of $\epsilon$. Fix a $\delta \ge 0$, and by the weak law of large numbers (WLLN)

$$\lim_{n\to\infty}\left[\mathbf{P}\left(\left|\frac{1}{n}\sum_{m=0}^{n} X_m - p\right| > \delta\right)\right] = 0 \qquad \forall\delta > 0 \tag{23}$$

$$\Longrightarrow \lim_{n\to\infty}\left[\mathbf{P}\left(\sum_{m=0}^{n} X_m > n(p+\delta)\right)\right] = 0 \qquad \forall\delta > 0. \tag{24}$$

Therefore, as $n$ gets large, $G(n,p,\epsilon) = n(p+\delta)$ is sufficient to meet the probability requirements (for any positive $\epsilon$). In the limit of large n, the inequality in (22) reduces to

$$\rho = \frac{\sum_{(i,j)\in\mathcal{L}_{\rm B}} C^{\rm B}_{ij}}{\sum_{(i,j)\in\mathcal{L}} C^{\rm P}_{ij}} \le \frac{2(N-1)Np}{N(N-1)} = 2p. \tag{25}$$

■

Therefore, the size of the backup network is a small fraction of the size of the primary network since $p$ is usually small. Consequently, a backup network designed using the backup-link survivability constraint is a low-cost method of providing protection against random failures in addition to single-link failures. This result is consistent with [7], in that as the primary network size grows large, $p$ approaches zero under the single-failure model. Additionally, there has been work in [12] investigating the relationship between capacity and expected traffic loss.

## IV. General-Load Networks

Next, we develop a formulation for general primary link loads. First, we apply the robust optimization results from [20] to formulate a nonlinear program for backup capacity provisioning and develop an equivalent integer linear formulation in terms of new parameters $\Gamma_{ij}$. We show that the choice of these parameters affects the amount of capacity provisioned, and hence the probability of insufficient backup capacity. Then, we add constraints to directly compute these parameters, yielding a solution satisfying the probabilistic constraint in (2).

### A. Robust Optimization Formulation

In the case of uniform link loads, capacity is allocated to the backup network by computing ${\rm G}(n_{ij},p,\epsilon)$ for each link $(i,j)$. The backup capacity provisioned is the number of primary link failures protected against, as a function of $n_{ij}$, $p$, and $\epsilon$. However, this approach does not apply directly to nonuniform primary link loads, as different links will require different capacities to provide protection. In order to mathematically formulate the problem for general link loads, we will use techniques from the field of robust optimization.

Robust optimization finds a solution to a problem that best fits all possible realizations of the data, when that data is subject to uncertainty. In [20], the authors propose a novel formulation with an adjustable level of conservatism for such problems. Their approach is to introduce an optimization parameter $\Gamma$ and provide sufficient capacity to support all scenarios in which *any* $\Gamma$ of the demands exceeds their mean. The solution is guaranteed to be robust for those scenarios and is shown to be robust for all other scenarios with high probability, determined by $\Gamma$.

Robust optimization techniques have been successfully applied to different network design problems previously [25]–[28]. The work in [27] applies the robust optimization results of [20] to solve the problem of allocating capacity to support traffic uncertainty. Given an average traffic demand and a peak power demand, the authors formulate the robust network design problem to support some of the demands reaching their peak intensity, using the fact that not all demands will reach their peak simultaneously. In [27], the demand uncertainty arises due to traffic intensity variation, whereas in our paper, the demand uncertainty on the backup network arises due to the uncertainty in which links will fail. The work in [26] uses this approach to compute the realized robustness of networks designed with a certain degree of robustness, exploring the sensitivity the traffic parameters. The work in [25] elaborates on this problem, determining the correct amount on peak traffic intensities to support to provide robustness guarantees.

A similar approach can be applied to the problem of backup network design for general link loads, where the uncertainty is in the number of primary links that fail. Consider allocating capacity on link $(i,j)$ to protect against any scenario where up to $0 \le \Gamma_{ij} \le n_{ij}$ of the primary links utilizing $(i,j)$ for protection fail. Clearly, for the specific case of uniform loads, the required backup capacity $C_{ij}^{\mathrm{B}}$ is just $\Gamma_{ij}$, and as shown in Section III, $\Gamma_{ij}$ is given by $\mathrm{G}(n_{ij},p,\epsilon)$ under the constraint in (2). For general loads, $\mathrm{G}(n_{ij},p,\epsilon)$ is not the bandwidth that needs to be allocated, as in Section III, but rather the number of primary links for which to provide protection. To extend this idea, let $L_{ij}$ be the set of primary links protected by backup link $(i,j)$, i.e., $L_{ij} = \{(s,d) | b_{ij}^{sd} = 1\}$. Let $S_{ij}$ be a set of $\Gamma_{ij}$ primary links in $L_{ij}$ with the largest capacities. Thus, for any $(s,d) \in S_{ij}$, we have

$$C_{sd}^{\mathrm{P}} \ge C_{s'd'}^{\mathrm{P}} \qquad \forall (s',d') \in L_{ij} \setminus S_{ij}. \tag{26}$$

The backup capacity required to protect against any $\Gamma_{ij}$ primary link failures is given by

$$C_{ij}^{\mathrm{B}} = \sum_{(s,d)\in S_{ij}} C_{sd}^{\mathrm{P}}. \tag{27}$$

In a complete form, this constraint can be expressed as

$$C_{ij}^{\mathrm{B}} \ge \max_{S_{ij} | S_{ij} \subseteq \mathcal{L}, |S_{ij}| = \Gamma_{ij}} \left\{ \sum_{(s,d)\in S_{ij}} C_{sd}^{\mathrm{P}} b_{ij}^{sd} \right\} \qquad \forall (i,j). \tag{28}$$

The value of $\Gamma_{ij}$ determines the probability of protection. While $\Gamma_{ij}$ should be chosen such that (2) is satisfied, for now we fix the value of $\Gamma_{ij}$ for each link. The capacity constraint in (28) replaces the probabilistic constraint in (2), leading to the following nonlinear optimization problem.

Minimize:

$$\sum_{(i,j)\in\mathcal{L}_{\mathrm{B}}} C_{ij}^{\mathrm{B}}.$$

Subject To:

$$\begin{aligned}
&C_{ij}^{\mathrm{B}} \ge \max_{S_{ij} | S_{ij} \subseteq \mathcal{L}, |S_{ij}| = \Gamma_{ij}} \left\{ \sum_{(s,d)\in S_{ij}} C_{sd}^{\mathrm{P}} b_{ij}^{sd} \right\} \qquad \forall (i,j)\\
&\sum_j b_{ij}^{sd} - \sum_j b_{ji}^{sd} = \begin{cases} 1, & \text{if } s = i \\ -1, & \text{if } d = i \\ 0, & \text{o.w.} \end{cases} \qquad \forall (s,d) \in \mathcal{L}, i \in \mathcal{V}\\
&b_{ij}^{sd} \in \{0,1\} \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}.
\end{aligned} \tag{29}$$

The above is nonlinear due to the backup capacity constraint in (28), but it can be reformulated as an ILP using duality techniques similar to [20], detailed in the Appendix. The following is an equivalent formulation to (29):

Minimize:

$$\sum_{(i,j)\in\mathcal{L}_{\mathrm{B}}} C_{ij}^{\mathrm{B}}.$$

Subject To:

$$\begin{aligned}
&C_{ij}^{\mathrm{B}} \ge \nu_{ij}\Gamma_{ij} + \sum_{(s,d)\in\mathcal{L}} \theta_{ij}^{sd} \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}\\
&\nu_{ij} + \theta_{ij}^{sd} \ge C_{sd}^{\mathrm{P}} b_{ij}^{sd} \qquad \forall (s,d) \in \mathcal{L}, (i,j) \in \mathcal{L}_{\mathrm{B}}\\
&\sum_j b_{ij}^{sd} - \sum_j b_{ji}^{sd} = \begin{cases} 1, & \text{if } s = i \\ -1, & \text{if } d = i \\ 0, & \text{o.w.} \end{cases} \quad \forall (s,d) \in \mathcal{L}, i \in \mathcal{V}\\
&b_{ij}^{sd} \in \{0,1\} \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}\\
&\nu_{ij}, \theta_{ij}^{sd} \ge 0 \qquad \forall (s,d) \in \mathcal{L}, (i,j) \in \mathcal{L}_{\mathrm{B}}.
\end{aligned} \tag{30}$$

Clearly, if fewer than $\Gamma_{ij}$ links in $L_{ij}$ fail, the capacity allocated in (28) will be sufficient. Therefore, the probability of insufficient backup capacity can be upper-bounded using the tail probability of a binomial random variable

$$\mathbf{P}\bigg( \sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > C_{ij}^{\mathrm{B}} \bigg) \le \mathbf{P}\bigg( Y_{ij} > \Gamma_{ij} \bigg). \tag{31}$$

The capacity allocated in (27) is sufficient to meet the reliability constraint in (31) with probability $\epsilon$ if $\Gamma_{ij} = \mathrm{G}(n_{ij},p,\epsilon)$. However, $n_{ij}$ is an optimization variable, on which $\Gamma_{ij}$ depends. Thus, the remaining task is to modify (30) to directly compute the value of $\Gamma_{ij}$ for each link using an ILP formulation.

### *B. Complete Formulation*

Since $\Gamma_{ij}$ cannot be computed analytically, we create a table *a priori* in which the $m$th entry $\Gamma(m)$ equals $\mathrm{G}(m,p,\epsilon)$, computed numerically. We develop an ILP that leads to the direct computation of $n_{ij}$ in order to index the table.

To compute $n_{ij}$, let $x_{ij}^m = 1$ if $n_{ij} = m$, and 0 otherwise. The following constraints are introduced:

$$\sum_{m=0}^{N(N-1)} x_{ij}^m = 1 \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}. \tag{32}$$

Constraint (32) enforces $x_{ij}^m$ to be equal to 1 for only one value of $m$ for each backup link

$$\sum_{(s,d)\in\mathcal{L}} b_{ij}^{sd} = \sum_{m=0}^{N(N-1)} m \cdot x_{ij}^m \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}. \tag{33}$$

Constraint (33) ensures that the number of primary links utilizing a backup link $(i,j)$ is equal to the value of $m$ for which $x_{ij}^m = 1$. Consequently, $\Gamma_{ij}$ can be represented by the following:

$$\Gamma_{ij} = \mathrm{G}(n_{ij}, p, \epsilon) = \sum_{m=0}^{N(N-1)} \Gamma(m) x_{ij}^m. \tag{34}$$

The capacity constraint of (30) is rewritten as

$$C_{ij}^{\mathrm{B}} \geq \sum_{m=0}^{N(N-1)} \Gamma(m) \nu_{ij} x_{ij}^m + \sum_{(s,d)\in\mathcal{L}} \theta_{ij}^{sd}. \tag{35}$$

Since the product $\nu_{ij} x_{ij}^m$ is nonlinear, another set of optimization variables is added to represent this product in linear form. Let $y_{ij}^m$ be a nonnegative variable satisfying the following constraints:

$$y_{ij}^m \geq \nu_{ij} + K(x_{ij}^m - 1) \qquad \forall (i,j), m \tag{36}$$
$$y_{ij}^m \leq K x_{ij}^m \qquad \forall (i,j), m \tag{37}$$
$$y_{ij}^m \geq 0 \qquad \forall (i,j), m. \tag{38}$$

In the above equations, $K$ is a large number such that $K > \max_{sd} C_{sd}^{\mathrm{P}}$. When $x_{ij}^m = 0$, then $x_{ij}^m \nu_{ij} = 0$, and constraints (37) and (38) force $y_{ij}^m$ to 0. On the other hand, if $x_{ij}^m = 1$, constraint (36) will force $y_{ij}^m \geq \nu_{ij}$, which at the optimal solution will be satisfied with equality. These constraints lead to an ILP formulation for backup network design, given in (39).

The following is an ILP formulation for the design of a dedicated backup network to protect against random failures:

Minimize:

$$\sum_{(i,j)\in\mathcal{L}_{\mathrm{B}}} C_{ij}^{\mathrm{B}}.$$

Subject To:

$$\begin{aligned}
& C_{ij}^{\mathrm{B}} \geq \sum_{m=0}^{N(N-1)} y_{ij}^m \Gamma(m) + \sum_{(s,d)\in\mathcal{L}} \theta_{ij}^{sd} \\
& \forall (i,j) \in \mathcal{L}_{\mathrm{B}} \\
& \nu_{ij} + \theta_{ij}^{sd} \geq C_{sd}^{\mathrm{P}} b_{ij}^{sd} \qquad \forall (s,d) \in \mathcal{L}, (i,j) \in \mathcal{L}_{\mathrm{B}} \\
& \sum_{m=0}^{N(N-1)} x_{ij}^m = 1 \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}} \\
& \sum_{(s,d)\in\mathcal{L}} b_{ij}^{sd} \leq \sum_{m=0}^{N(N-1)} m \cdot x_{ij}^m \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}} \\
& y_{ij}^m \geq \nu_{ij} + K(x_{ij}^m - 1) \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}, m \\
& y_{ij}^m \leq K x_{ij}^m \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}, m \\
& \sum_j b_{ij}^{sd} - \sum_j b_{ji}^{sd} = \begin{cases} 1, & \text{if } s = i \\ -1, & \text{if } d = i \\ 0, & \text{o.w.} \end{cases} \qquad \forall (s,d) \in \mathcal{L}, i \in \mathcal{V} \\
& b_{ij}^{sd}, x_{ij}^m \in \{0,1\} \qquad \forall (i,j) \in \mathcal{L}_{\mathrm{B}}, m \\
& \theta_{ij}^{sd} \geq 0, \nu_{ij} \geq 0, y_{ij}^m \geq 0 \quad \forall (s,d) \in \mathcal{L}, (i,j) \in \mathcal{L}_{\mathrm{B}}, m.
\end{aligned} \tag{39}$$

This formulation calculates the backup paths and capacity allocation for a dedicated backup network satisfying the survivability constraint in (2).

### C. Simulated Annealing

The ILP in (39) can be directly solved for small instances, but becomes intractable for large networks. There are a number of heuristic approaches to solving ILPs, such as randomized rounding, tabu search, and simulated annealing. Here, we employ a simulated annealing approach to estimate the backup path routing in (39).

Simulated annealing (SA) is a random search heuristic that can be used to find near-optimal solutions to optimization problems [29]. The algorithm begins with an arbitrary feasible solution, with a cost computed with respect to an objective function. Then, a random perturbation is applied to the solution, and the cost is reevaluated. The new solution is probabilistically accepted based on the relationship between the two costs. A positive probability of moving to a worse solution avoids the problem of being trapped in a local minima. SA has been used previously on network survivability problems [30].

For a fixed backup path routing, the computation of the optimal backup capacity $C_{ij}^{\mathrm{B}}$ is straightforward. Therefore, we use simulated annealing to estimate the backup path routing. For the problem in (39), the solution at each SA iteration is the backup path for each primary link, and the cost is the total backup capacity, computed using (28). Perturbations are applied to this solution by randomly recomputing the backup path for a randomly chosen primary link. This recomputation is done by choosing random links starting from the source node and ending at the destination node. The current network with cost $C_{\mathrm{total}}^{\mathrm{B}}$ is modified by changing a single backup path, and the network cost $C_{\mathrm{total}}^{\mathrm{B}\prime}$ is recomputed. The new backup network is accepted with probability $\min(q, 1)$, where

$$q = \exp\left(\frac{C_{\mathrm{total}}^{\mathrm{B}} - C_{\mathrm{total}}^{\mathrm{B}\prime}}{T}\right). \tag{40}$$

Hence, better solutions are unconditionally accepted, and worse solutions are accepted with probability $q$. The parameter $T$ in (40) represents the "temperature" of the system. At high temperatures, there is a high probability of accepting a solution with a larger cost than the current solution. This prevents the algorithm from getting trapped in a local minima. The temperature decreases after a number of iterations depending on the network size by $T' = \rho T$, for $0 < \rho < 1$. SA cannot escape local minima if $\rho$ is too small, but high values of $\rho$ result in

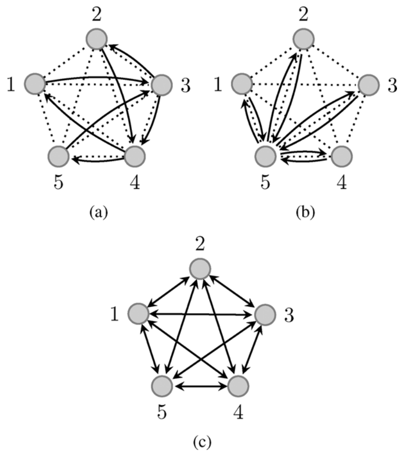


Fig. 4. Optimal backup networks shown as solid links over dotted primary networks for different probabilities of link failure. Designed using $\epsilon = 0.01$. (a) $p = 0.025$. (b) $p = 0.1$. (c) $p = 0.25$.

TABLE II
BACKUP NETWORK CAPACITY REQUIRED FOR TOPOLOGIES DESIGNED USING DIFFERENT STRATEGIES. $\epsilon = 0.01$ IN EACH DESIGN

| Strategy | $p = 0.025$ | $p = 0.05$ | $p = 0.075$ | $p = 0.1$ | $p = 0.25$ |
|---|---|---|---|---|---|
| optimal | 7 | 10 | 13 | 16 | 20 |
| cycle | 10 | 15 | 15 | 20 | 30 |
| two-hop | 8 | 16 | 16 | 16 | 24 |
| one-hop | 20 | 20 | 20 | 20 | 20 |
| SA | 7 | 11 | 13 | 16 | 20 |

long computation times. Eventually, $T$ becomes small enough that the probability of accepting a worse solution approaches zero. At this point, the algorithm terminates and returns the resulting backup network.

There are only limited theoretical results on the convergence time of SA, which is known to be highly problem-dependent. Regardless, SA approaches are widely used in practice [29]. The choice of parameters leads to an inherent tradeoff between the accuracy of SA and its convergence time. As the number of iterations before a temperature reduction increases, the accuracy of the SA approach improves at the expense of increased convergence time.

## V. Numerical Results

To begin with, consider a 5-node, fully connected topology where each primary link has unit-capacity. Due to the small size of this network, the ILP in (39) can be solved to compute the optimal backup topologies for different values of $p$. These backup networks are shown in Fig. 4. For small values of $p$, the backup topology consists of few links, whereas for large values of $p$, the backup network resembles the primary network. Table II summarizes the results of the backup networks for different values of $p$, using all of the design heuristics discussed. Cycle protection, two-hop protection, and one-hop protection refer to the strategies analyzed in Section III. The optimal column refers to the solution returned by solving the ILP in (39) using CPLEX, and the SA column refers to an approach where simulated annealing is used to solve the ILP.

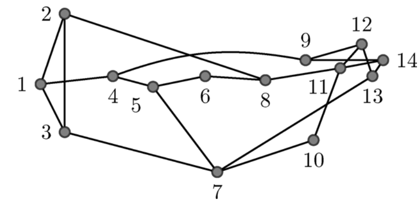


Fig. 5. 14-node NSFNET backbone network (1991).

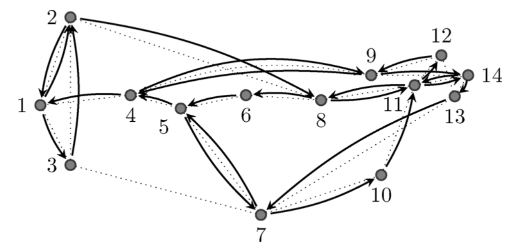


Fig. 6. Backup network (solid) shown for the NSFNET (dotted) with the restriction that the backup network must be a subgraph of the primary network. The primary network here assumes a probability of link failure of 0.075, and the backup network is designed for $\epsilon = 0.05$.

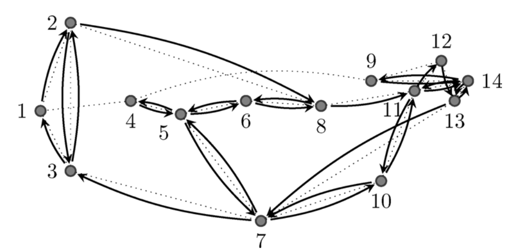


Fig. 7. Backup network (solid) shown for the NSFNET (dotted) with the restriction that the backup network must be a subgraph of the primary network. The primary network here assumes a probability of link failure of 0.1, and the backup network is designed for $\epsilon = 0.05$.

The table shows that for $p = 0.1$, the two-hop protection scheme is optimal, and for $p = 0.25$, the one-hop protection scheme is optimal. Furthermore, the simulated annealing heuristic performs very close to optimal for different values of $p$. Clearly, the optimal topology depends on the probability of link failure, and it is therefore necessary to use a different backup routing scheme depending on the link failure probabilities.

### *A. Simulated Annealing on Unit-Load Networks*

The heuristics can be extended to larger networks, but the ILP in (39) cannot be solved directly for large networks. Thus, we use the SA approach to solve the ILP for backup network design for large primary networks.

Consider the NSFNET primary network shown in Fig. 5. Each link is bidirectional, with unit capacity in each direction. Our goal is to construct a backup network consisting of links $(i, j) \in \mathcal{L}_{\mathrm{B}}$, where $i$ and $j$ are connected by a link in the NSFNET. The survivability constraint in (2) must be satisfied with probability $\epsilon = 0.05$. The SA algorithm, shown to be near-optimal for smaller networks, is used to compute the backup network for this larger example. The resulting backup networks for probability of link failure $p = 0.075$ and $p = 0.10$ are shown in Figs. 6 and 7, respectively.

TABLE III
COMPARISON OF BACKUP NETWORKS FOR NSFNET WITH DIFFERENT PROBABILITIES OF PRIMARY LINK FAILURE. NETWORKS WERE DESIGNED USING $\epsilon = 0.05$. AVERAGE $n_{ij}$ REFERS TO THE AVERAGE NUMBER OF PRIMARY LINKS BEING PROTECTED BY A BACKUP LINK

| Failure Probability | $\sum_{(i,j)\in\mathcal{L}_B} C_{ij}^B$ | Average $n_{ij}$ |
|---|---|---|
| $p = 0.06$ | 22 | 4.87 |
| $p = 0.075$ | 24 | 4.42 |
| $p = 0.085$ | 27 | 3.59 |
| $p = 0.10$ | 28 | 3 |
| $p = 0.175$ | 34 | 1.88 |
| $p = 0.25$ | 42 | 1 |

TABLE IV
COMPARISON OF BACKUP NETWORKS FOR NSFNET WITH DIFFERENT PROBABILITIES OF PRIMARY LINK FAILURE. NETWORKS WERE DESIGNED USING $\epsilon = 1 \times 10^{-5}$. AVERAGE $n_{ij}$ REFERS TO THE AVERAGE NUMBER OF PRIMARY LINKS BEING PROTECTED BY A BACKUP LINK

| Failure Probability | $\sum_{(i,j)\in\mathcal{L}_B} C_{ij}^B$ | Average $n_{ij}$ |
|---|---|---|
| $p = 0.0001$ | 16 | 10.13 |
| $p = 0.0005$ | 20 | 6.75 |
| $p = 0.001$ | 24 | 4.96 |
| $p = 0.0015$ | 24 | 2.76 |
| $p = 0.002$ | 34 | 1.94 |
| $p = 0.004$ | 42 | 1 |

TABLE V
COMPARISON OF BACKUP NETWORKS FOR NSFNET WITH DIFFERENT ROBUSTNESS CONSTRAINTS. NETWORKS WERE DESIGNED ASSUMING PROBABILITY OF LINK FAILURE $p = 0.075$. AVERAGE $n_{ij}$ REFERS TO THE AVERAGE NUMBER OF PRIMARY LINKS BEING PROTECTED BY A BACKUP LINK

| $\epsilon$ | $\sum_{(i,j)\in\mathcal{L}_B} C_{ij}^B$ | Average $n_{ij}$ |
|---|---|---|
| $\epsilon = 0.005$ | 42 | 1 |
| $\epsilon = 0.01$ | 34 | 1.71 |
| $\epsilon = 0.025$ | 29 | 2.86 |
| $\epsilon = 0.05$ | 24 | 4.52 |
| $\epsilon = 0.075$ | 23 | 5.09 |

In the backup network of Fig. 6, a total capacity of 24 is required. Most backup links protect up to five primary links. In the case of Fig. 7, where the probability of link failure is higher, a total capacity of 28 is needed. The backup links in this example protect an average of three primary links. If the probability of link failure increases to $p = 0.25$, the resulting backup topology is a mirror of the primary topology, requiring a capacity of 42. As $p$ increases, the number of backup links needed rises, and similarly the number of primary links being protected by each backup link falls, until the network follows the one-hop protection scheme. These results are summarized in Table III. In this table, we also see that by providing probabilistic protection, we only need to allocate roughly half the capacity needed for 100% protection. In Table IV, we show numerical results for smaller values of $p$ and $\epsilon$, modeling scenarios where failures are less common. Additionally, in Table V, we show the effect of varying the probabilistic constraint $\epsilon$ on the resulting backup network. As $\epsilon$ grows, the constraint becomes more lenient, and more failures can be tolerated. Thus, we would expect less backup capacity to be required, as confirmed by the results in Table V.

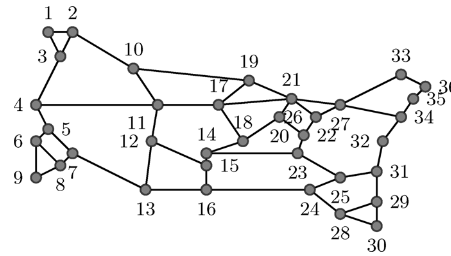

Fig. 8. 36-node Sprint backbone network.

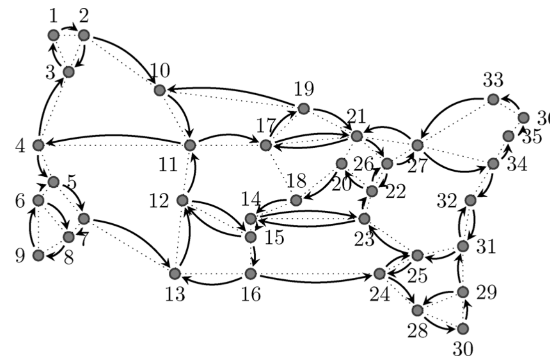

Fig. 9. Backup network (solid) shown for the Sprint backbone network (dotted) with the restriction that the backup network must be a subgraph of the primary network. The primary network assumes a probability of link failure of $p = 0.055$ and is designed for a survivability constraint of $\epsilon = 0.05$.

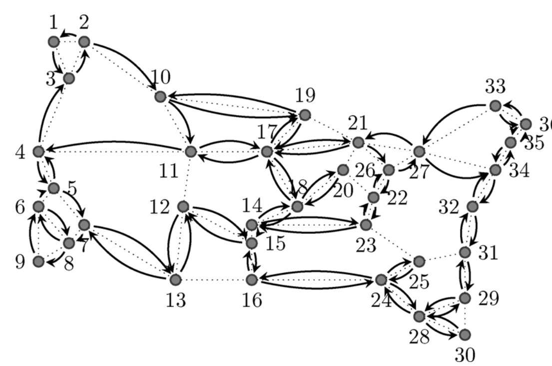

Fig. 10. Backup network (solid) shown for the Sprint backbone network (dotted) with the restriction that the backup network must be a subgraph of the primary network. The primary network assumes a probability of link failure of $p = 0.1$ and is designed for a survivability constraint of $\epsilon = 0.05$.

The simulated annealing approach can be used to solve large-scale networks as well, such as the 36-node Sprint backbone network, shown in Fig. 8. Due to the large size of the network, the simulated annealing algorithm requires a prohibitively large number of iterations to find an optimal solution. However, the number of iterations can be reduced in exchange for a less optimal solution. Assume the bidirectional links in Fig. 8 represent a unit of primary capacity in each direction. Again, the goal is to construct a backup network consisting of links $(i, j) \in \mathcal{L}_{\mathrm{B}}$, where $i$ and $j$ are connected by a link in the primary network, to satisfy the survivability constraint in (2) with probability $\epsilon = 0.05$.

The backup networks returned by the simulated annealing algorithm for a probability of primary link failure of $p = 0.055$ and $p = 0.1$ are shown in Figs. 9 and 10, respectively. For a small probability of primary link failure (Fig. 9), the optimal backup network is made up of many cycles, where backup paths are potentially many hops. However, as the probability of link

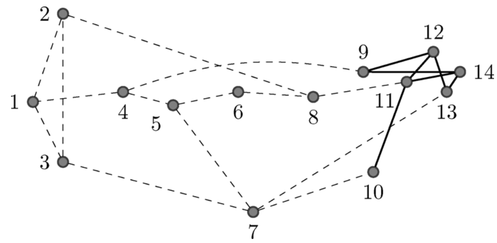


Fig. 11. 14-node NSFNET backbone network with nonuniform link loads. Bold links represent demands of 10, and dashed links represent demands of 1.

TABLE VI
COMPARISON OF BACKUP NETWORKS FOR THE SPRINT BACKBONE WITH DIFFERENT PROBABILITIES OF PRIMARY LINK FAILURE. NETWORKS WERE DESIGNED USING $\epsilon = 0.05$. AVERAGE $n_{ij}$ REFERS TO THE AVERAGE NUMBER OF PRIMARY LINKS BEING PROTECTED BY A BACKUP LINK

| Link Failure Probability | $\sum_{(i,j)\in\mathcal{L}_B} C_{ij}^B$ | Average $n_{ij}$ |
|---|---|---|
| $p = 0.055$ | 57 | 4.21 |
| $p = 0.065$ | 62 | 3.5 |
| $p = 0.075$ | 62 | 3.5 |
| $p = 0.085$ | 68 | 3.16 |
| $p = 0.1$ | 74 | 2.47 |
| $p = 0.12$ | 76 | 2.36 |
| $p = 0.14$ | 88 | 1.83 |
| $p = 0.16$ | 88 | 1.65 |
| $p = 0.23$ | 106 | 1.27 |
| $p = 0.275$ | 106 | 1.19 |
| $p = 0.3$ | 106 | 1.12 |
| $p = 0.4$ | 106 | 1 |

failure increases, long backup paths become more inefficient, and the optimal backup topology consists of more links and more direct paths. To see this clearly, Table VI summarizes the resulting backup topologies for varying probabilities of primary link failure. Similar to the results for the NSFNET, as the probability of link failure increases, the backup links protect fewer primary links, and the optimal topology resembles a mirror of the primary network. However, for small probabilities of link failure, it is more efficient for primary links to share backup resources, hence the higher average number of primary links protected by each backup link.

### B. Simulated Annealing on General-Load Networks

The previous simulation results were for primary networks where each link had a unit capacity. Our simulated annealing approach can also be applied to networks with nonuniform primary capacities. The presence of these nonuniformities greatly affects the backup topology necessary to sufficiently protect the primary network. To illustrate, we consider two distributions of primary link capacities on the NSFNET in Fig. 5. The first, shown in Fig. 11, assumes 10 directional (five bidirectional) links on the east side of the network have a high primary capacity of 10, while the rest of the links have a low primary capacity of 1. As an alternative, we consider 10 directional links mixed throughout the network to have a high capacity, while the remainder of the network has a low primary capacity, as shown in Fig. 12.

The simulated annealing algorithm is applied to each of these primary link capacity distributions in order to find a (near-)optimal backup topology. For the primary capacities in

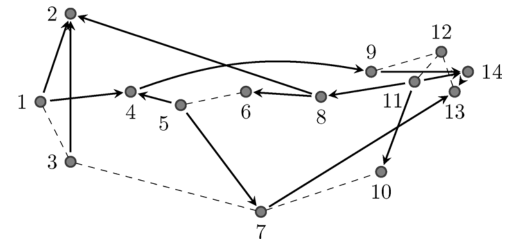


Fig. 12. 14-node NSFNET backbone network with nonuniform link loads. Directed bold links represent a primary capacity of 10 in one direction, and of 1 in the other direction, while dashed links represent primary capacity of 1 in both directions.

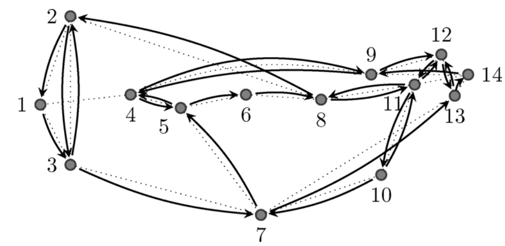


Fig. 13. Backup network (solid) shown for the NSFNET (dotted). The backup network must be a subgraph of the primary network. The primary network here assumes a probability of link failure of 0.075, and the backup network is designed for $\epsilon = 0.05$. Primary link capacities are distributed according to Fig. 11.

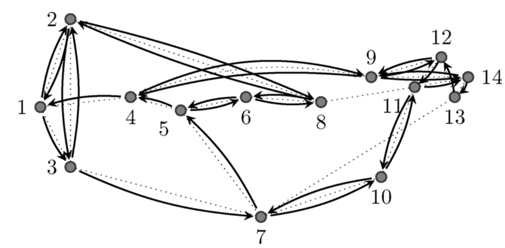


Fig. 14. Backup network (solid) shown for the NSFNET (dotted). The backup network must be a subgraph of the primary network. The primary network here assumes a probability of link failure of 0.1, and the backup network is designed for $\epsilon = 0.05$. Primary link capacities are distributed according to Fig. 11.

Fig. 11, Figs. 13 and 14 show the backup topologies when the probability of primary link failure is $p = 0.075$ and $p = 0.1$, respectively. For the lower probability of link failure, a total backup capacity of 98 is required, while the less reliable network requires a backup capacity of 119. On the other hand, Figs. 15 and 16 show the backup topologies when the probability of primary link failure is $p = 0.075$ and $p = 0.1$ for the demand structure in Fig. 12. In this case, the backup topologies require a total capacity of 141 and 148, respectively. Despite the fact that the total primary capacity is the same in both scenarios, the backup capacity is much higher in the case where the high-capacity primary links are distributed throughout the network. This is due to the fact that at low probabilities of link failure, a few high-capacity backup links are sufficient to protect many local high-capacity primary links. However, when the high-capacity primary links are spread throughout the network, they cannot share these high-capacity backup resources, and consequently more high-capacity backup links are required.

## VI. MODEL EXTENSIONS

The framework developed in this paper can be extended to include variations to the model. In this section, we highlight

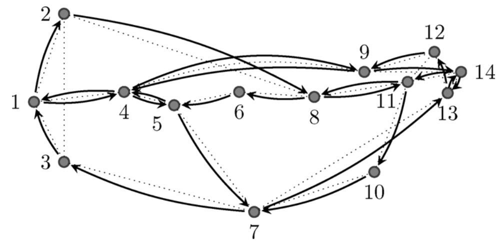


Fig. 15. Backup network (solid) shown for the NSFNET (dotted) with the restriction that the backup network must be a subgraph of the primary network. The primary network here assumes a probability of link failure of 0.075, and the backup network is designed for $\epsilon = 0.05$. Primary link capacities are distributed according to Fig. 12.

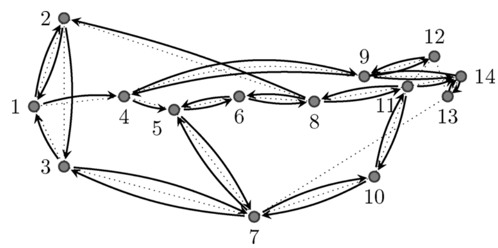


Fig. 16. Backup network (solid) shown for the NSFNET (dotted). The primary network here assumes a probability of link failure of 0.1, and the backup network is designed for $\epsilon = 0.05$. Primary link capacities are distributed according to Fig. 12.

several extensions to our problem to more appropriately model certain real-world scenarios.

### A. Nonuniform Link Failures

To begin, we can assume that link $(s,d) \in \mathcal{L}$ in the primary network has a link failure probability $p_{sd}$, allowing for primary links to fail with different probabilities. To adapt our framework to this new model, we can consider a link with probability of failure $p_{sd}$ as $k_{sd}$ links in series with the same probability of link failure $p$, where $k_{sd}$ is calculated as

$$k_{sd} = \left\lceil \frac{\log(1-p_{sd})}{\log(1-p)} \right\rceil. \tag{41}$$

The number of links is calculated such that the probability that at least one of the links fails (and the total demand over all the links needs to be rerouted over the backup network) is equal to the probability of link failure $p_{sd}$. Applying our formulation to the modified network results in an upper bound on the required capacity since our formulation allocates capacity to account for multiple links in series failing. However, this bound becomes tight for small $p$, where it is unlikely that multiples of those links to fail.

The difference between the original link failure probability $p_{sd}$ and the failure probability of the new links in series can be written as

$$\begin{aligned} &|1-(1-p)^{k_{sd}} - p_{sd}| \\ &= \left| 1-p_{sd}-(1-p)^{\frac{\log(1-p_{sd})}{\log(1-p)}}(1-p)^{\left\lceil \frac{\log(1-p_{sd})}{\log(1-p)} \right\rceil - \left(\frac{\log(1-p_{sd})}{\log(1-p)}\right)} \right| \end{aligned} \tag{42}$$

$$= (1-p_{sd}) \left| 1-(1-p)^{\left\lceil \frac{\log(1-p_{sd})}{\log(1-p)} \right\rceil - \left(\frac{\log(1-p_{sd})}{\log(1-p)}\right)} \right| \tag{43}$$

$$< (1-p_{sd})p. \tag{44}$$

Therefore, by choosing a small value of $p$, one can construct a network with uniform link failure probability that approximates the original network with nonuniform link failure probabilities, at the expense of additional links.

### B. Unreliable Backup Links

In practical networks, backup links may also experience some probability of failure. Throughout this work, we have assumed that this probability is negligible compared to that of a primary link failure. However, when this assumption is relaxed, a backup link "overflow" can also occur when the backup link fails and any primary link needs to use the failed backup link. Clearly, our formulation provides an upper bound on reliability (a lower bound on the required backup capacity) on the case with unreliable backup links. Additionally, our approach can be applied to this case, given a probability of backup-link failure $q$. Let $Z_{ij}$ be a random variable equal to 1 if backup link $(i,j)$ fails, and 0 otherwise. Assume that every primary link has nonzero traffic, i.e., $C_{sd}^{\mathrm{P}} > 0, \forall (s,d) \in \mathcal{L}$. Let $n_{ij}$ be the number of primary links whose backup paths use backup link $(i,j)$. Then, new backup link overflow constraint is

$$\begin{aligned} &\mathbf{P}\big(\text{overflow on } (i,j)\big) \\ &\quad = \mathbf{P}(Z_{ij}=1)\mathbf{P}\left( \sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > 0 \right) \\ &\qquad + \mathbf{P}(Z_{ij}=0)\mathbf{P}\left( \sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > C_{ij}^{\mathrm{B}} \right) \qquad (45) \\ &\quad = q(1-(1-p)^{n_{ij}}) \\ &\qquad + (1-q)\mathbf{P}\left( \sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > C_{ij}^{\mathrm{B}} \right) \le \epsilon. \qquad (46) \end{aligned}$$

Designing $C_{ij}^{\mathrm{B}}$ to satisfy (46) is equivalent to satisfying

$$\mathbf{P}\left( \sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > C_{ij}^{\mathrm{B}} \right) \le \frac{\epsilon - q(1-(1-p)^{n_{ij}})}{1-q} = \epsilon'. \tag{47}$$

Therefore, incorporating backup-link failures into the formulation is equivalent to solving the formulation with a modified probability constraint ($\epsilon'$), as long as $\epsilon > q(1-(1-p)^{n_{ij}})$. As an illustration, for the backup network design problem for the NSFNET in Table III, if $\epsilon' = 0.05$, then for backup link failure probability $q = 0.01$, $\epsilon = 0.053$, and for backup failure probability $q = 0.1$, which is the same order as the primary link failure probability $p$, $\epsilon = 0.08$. Thus, for a reliability requirement $\epsilon$, one can solve our formulation with a slightly smaller value of $\epsilon'$.

### C. Correlated Link Failures

As a final extension, we consider augmenting our framework to account for correlated failures. For example, consider the Probabilistic Shared Risk Link Group (PSRLG) model in [31], where once an SRLG failure event occurs, the links contained in the SRLG fail independently with probability $p$. For simplicity of exposition, assume mutually exclusive SRLGs such that each SRLG $r \in R$ fails with probability $\pi_r$ and $\sum_{r\in R}\pi_r = 1$. Then, the overflow probability at backup link $(i,j)$ can be written as

$$\mathbf{P}\left(\sum_{(s,d)\in\mathcal{L}} X_{sd} b_{ij}^{sd} C_{sd}^{\mathrm{P}} > C_{ij}^{\mathrm{B}}\right) \le \mathbf{P}\left(Y_{ij} > \Gamma_{ij}\right) \tag{48}$$

$$= \sum_{r\in R}\pi_r \sum_{y=\lfloor\Gamma_{ij}\rfloor+1}^{|r(i,j)|} \binom{|r(i,j)|}{y} p^y(1-p)^{|r(i,j)|-y} \le \epsilon \tag{49}$$

where $r(i,j)$ is the number of primary links that belong to SRLG $r$ and use $(i,j)$ as backup links. We assume an empty summation to be zero. Similar to the argument in Section IV-B, we can create *a priori* a table containing the values of $\Gamma_{ij}$ and use it in the MILP formulation. Note that in this case, a much larger table is needed since the value of $\Gamma_{ij}$ is determined by the number of links in each SRLG that use link $(i,j)$ as backup.

## VII. Conclusion

Dedicated backup networks are a low-cost and efficient method for providing protection against multiple (random) failures. In the event of a failure, the load on the failed link can be automatically rerouted over a predetermined path in the backup network, providing fast recovery from network failures. We formulated the backup network design problem as an ILP for primary networks with general link capacities and independent, identically distributed probabilities of link failure. For primary networks with rare failures, backup networks are shown to use fewer links, with more resource sharing among backup paths. Conversely, when the primary network has a high probability of link failure, the backup network consists of shorter backup paths. For larger primary networks, a simulated annealing approach was presented to solve the backup network design ILP. This approach has been shown to perform near-optimally in designing dedicated backup networks. The SA algorithm can be adjusted to trade off between computation time and accuracy. Additionally, we demonstrated our capacity allocation approach on real-world networks and have shown that, practically, protecting against failures with high probability can lead to a capacity savings of up to 50% compared to approaches providing 100% protection guarantees.

## Appendix

The following steps are used to convert formulation (29) to formulation (30) using a duality approach. For a fixed $b_{ij}^{sd}$ and $\Gamma_{ij}$, the backup capacity of link $(i,j)$

$$\beta_{ij}(\mathbf{b_{ij}},\Gamma_{ij}) = \max_{S_{ij}|S_{ij}\subseteq\mathcal{L},|S_{ij}|=\Gamma_{ij}} \left\{\sum_{(s,d)\in S_{ij}} C_{sd}^{\mathrm{P}} b_{ij}^{sd}\right\} \tag{50}$$

can be written as the solution to the following LP:

$$\begin{aligned}
\beta_{ij}(\mathbf{b_{ij}},\Gamma_{ij}) = \text{maximize} \quad & \sum_{(s,d)\in\mathcal{L}} C_{sd}^{\mathrm{P}} b_{ij}^{sd} z_{ij}^{sd} \\
\text{subject to} \quad & \sum_{(s,d)\in\mathcal{L}} z_{ij}^{sd} \le \Gamma_{ij} \\
& 0 \le z_{ij}^{sd} \le 1 \qquad \forall (s,d)\in\mathcal{L}.
\end{aligned} \tag{51}$$

Assuming the number of primary links $(s,d)$ satisfying $b_{ij}^{sd} = 1$ is larger than or equal to $\Gamma_{ij}$, the LP will choose the $\Gamma_{ij}$ of them with the largest capacities by setting $z_{ij}^{sd} = 1$ for those links $(s,d)$. This corresponds to choosing the set $S_{ij}$ in (27). If there are fewer than $\Gamma_{ij}$ primary links $(s,d)$ satisfying $b_{ij}^{sd} = 1$, then for each of these links, $z_{ij}^{sd} = 1$, and the other $(s,d)$ satisfying $z_{ij}^{sd} = 1$ are chosen arbitrarily. Note, however, that this does not affect the correctness of (51).

Let $\nu_{ij}$ be the dual variable for the first constraint in (51), and let $\theta_{ij}^{sd}$ be the dual variables for the second set of constraints. The dual problem of (51) is formulated as follows:

$$\begin{aligned}
\text{minimize} \quad & \nu_{ij}\Gamma_{ij} + \sum_{(s,d)\in\mathcal{L}} \theta_{ij}^{sd} \\
\text{subject to} \quad & \nu_{ij} + \theta_{ij}^{sd} \ge C_{sd}^{\mathrm{P}} b_{ij}^{sd} \qquad \forall (s,d)\in\mathcal{L} \\
& \nu_{ij} \ge 0 \\
& \theta_{ij}^{sd} \ge 0 \qquad \forall (s,d)\in\mathcal{L}.
\end{aligned} \tag{52}$$

Since there is zero duality gap between problem (51) and its dual (52), the optimal value of the objective function in (52) is equal to $\beta_{ij}(\mathbf{b_{ij}},\Gamma_{ij})$. Additionally, since problem (29) minimizes $\beta_{ij}(\mathbf{b_{ij}},\Gamma_{ij})$ for each $(i,j)$, problem (52) can be substituted into (29) to arrive at the formulation in (30).

## References


[1] W. Grover, *Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET, and ATM Networking*. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

[2] S. Lumetta *et al.*, "Capacity versus robustness: A tradeoff for link restoration in mesh networks," *J. Lightw. Technol.*, vol. 18, no. 12, p. 1765, Dec. 2000.

[3] D. Zhou and S. Subramaniam, "Survivability in optical networks," *IEEE Netw.*, vol. 14, no. 6, pp. 16–23, Nov.–Dec. 2000.

[4] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," *IEEE/ACM Trans. Netw.*, vol. 13, no. 1, pp. 198–211, Feb. 2005.

[5] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, *Survivable WDM Mesh Netw.*, vol. 21, no. 4, pp. 870–883, 2003.

[6] J. Zhang and B. Mukherjee, "A review of fault management in WDM mesh networks: Basic concepts and research challenges," *IEEE Netw.*, vol. 18, no. 2, pp. 41–48, Mar. 2004.

[7] M. Banner and A. Orda, "Designing low-capacity backup networks for fast restoration," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[8] H. Choi, S. Subramaniam, and H. Choi, "On double-link failure recovery in WDM optical networks," in *Proc. IEEE INFOCOM*, 2002, vol. 2, pp. 808–816.

[9] L. Guo, H. Yu, and L. Li, "Segment shared protection for survivable meshed WDM optical networks," *Opt. Commun.*, vol. 251, no. 4–6, pp. 328–338, 2005.

[10] B. Jozsa, D. Orincsay, and A. Kern, "Surviving multiple network failures using shared backup path protection," in *Proc. ISCC*, 2003, vol. 1, pp. 1333–1340.

[11] M. Herzberg, S. Bye, and A. Utano, "The hop-limit approach for spare-capacity assignment in survivable networks," *IEEE/ACM Trans. Netw.*, vol. 3, no. 6, p. 784, Dec. 1995.

[12] K. Vajanapoom and D. Tipper, "Risk based incremental survivable network design," in *Proc. 6th DRCN*, 2007, pp. 1–9.

[13] D. Papadimitriou *et al.*, "Inference of shared risk link groups," Internet Draft, May 2002 [Online]. Available: http://tools.ietf.org/html/draft-many-inference-srlg-02

[14] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing*. New York, NY, USA: Kluwer, 1999.

[15] E. Modiano and A. Narula-Tam, "Survivable lightpath routing—A new approach to the design of WDM-based networks," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 4, pp. 800–809, May 2002.

[16] E. Oki, N. Matsuura, K. Shiomoto, and N. Yamanaka, "A disjoint path selection scheme with shared risk link groups in GMPLS networks," *IEEE Commun. Lett.*, vol. 6, no. 9, pp. 406–408, Sep. 2002.

[17] D. Xu, Y. Xiong, C. Qiao, and G. Li, “Trap avoidance and protection schemes in networks with shared risk link groups,” *J. Lightw. Technol.*, vol. 21, no. 11, pp. 2683–2693, Nov. 2003.

[18] A. Soyster, “Convex programming with set-inclusive constraints and applications to inexact linear programming,” *Oper. Res.*, vol. 21, no. 5, pp. 1154–1157, 1973.

[19] A. Ben-Tal and A. Nemirovski, “Robust solutions of uncertain linear programs,” *Oper. Res. Lett.*, vol. 25, no. 1, pp. 1–14, 1999.

[20] D. Bertsimas and M. Sim, “The price of robustness,” *Oper. Res.*, vol. 52, no. 1, pp. 35–53, 2004.

[21] S. Gast and A. Keimer, “Robust optimization in network flows,” University of Erlangen-Nürnberg, Germany, Tech. Rep., 2009.

[22] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee, “Service provisioning to provide per-connection-based availability guarantee in WDM mesh networks,” in *Proc. OFC*, Atlanta, GA, USA, Mar. 2003, pp. 622–624.

[23] M. Tornatore, G. Maier, and A. Pattavina, “Availability design of optical transport networks,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 8, pp. 1520–1532, Aug. 2005.

[24] J. Segovia, E. Calle, P. Vila, J. Marzo, and J. Tapolcai, “Topology-focused availability analysis of basic protection schemes in optical transport networks,” *J. Opt. Netw.*, vol. 7, pp. 351–364, 2008.

[25] A. M. Koster, M. Kutschka, and C. Raack, “Robust network design: Formulations, valid inequalities, and computations,” *Networks*, vol. 61, no. 2, pp. 128–149, 2013.

[26] A. M. Koster, M. Kutschka, and C. Raack, “On the robustness of optimal network designs,” in *Proc. IEEE ICC*, 2011, pp. 1–5.

[27] A. M. Koster and M. Kutschka, “An integrated model for survivable network design under demand uncertainty,” in *Proc. 8th DRCN*, 2011, pp. 54–61.

[28] M. Johnston, H.-W. Lee, and E. Modiano, “Robust network design for stochastic traffic demands,” in *Proc. IEEE GLOBECOM*, 2011, pp. 1–5.

[29] S. Brooks and B. Morgan, “Optimization using simulated annealing,” *Statistician*, vol. 44, no. 2, pp. 241–257, 1995.

[30] B. Van Caenegem, W. Van Parys, F. De Turck, and P. Demeester, “Dimensioning of survivable WDM networks,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 7, pp. 1146–1157, Sep. 1998.

[31] H.-W. Lee, E. Modiano, and K. Lee, “Diverse routing in networks with probabilistic failures,” *IEEE/ACM Trans. Netw.*, vol. 18, no. 6, pp. 1895–1907, Dec. 2010.



**Matthew Johnston** (S'10) received the B.S. degree in electrical engineering and computer science from the University of California, Berkeley, CA, USA, in 2008, and the S.M. degree in electrical engineering from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2010, and is currently pursuing the Ph.D. degree in electrical engineering with the Laboratory for Information and Decision Systems, MIT.

His research interests include network control, wireless resource allocation, and network survivability.



**Hyang-Won Lee** (S'02–M'08) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2001, 2003, and 2007, respectively.

He was a Postdoctoral Research Associate with the Massachusetts Institute of Technology, Cambridge, MA, USA, during 2007 to 2011, and a Research Assistant Professor with KAIST between 2011 and 2012. He is currently an Assistant Professor with the Department of Internet and Multimedia Engineering, Konkuk University, Seoul, Korea. His research interests are in the areas of congestion control, stochastic network control, robust optimization, and reliable network design.



**Eytan Modiano** (S'90–M'93–SM'00–F'12) received the B.S. degree in electrical engineering and computer science from the University of Connecticut, Storrs, CT, USA, in 1986, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, MD, USA, in 1989 and 1992, respectively.

He was a Naval Research Laboratory Fellow between 1987 and 1992 and a National Research Council Post-Doctoral Fellow during 1992 to 1993. Between 1993 and 1999, he was with the Massachusetts Institute of Technology (MIT) Lincoln Laboratory, Lexington, MA, USA, where he was a project leader for MIT Lincoln Laboratory's Next Generation Internet (NGI) project. Since 1999, he has been on the faculty of MIT, where he is a Professor with the Department of Aeronautics and Astronautics and the Laboratory for Information and Decision Systems (LIDS). His research is on communication networks and protocols with emphasis on satellite, wireless, and optical networks.

Prof. Modiano is an Associate Fellow of the AIAA. He is an Editor-at-Large for the IEEE/ACM TRANSACTIONS ON NETWORKING and served as Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE/ACM TRANSACTIONS ON NETWORKING, and *AIAA Journal of Aerospace Information Systems*. He was the Technical Program Co-Chair for IEEE WiOpt 2006, IEEE INFOCOM 2007, and ACM MobiHoc 2007.