Minimizing the Risk From Disaster Failures in Optical Backbone Networks

Ferhat Dikbiyik, Massimo Tornatore, and Biswanath Mukherjee

I. Introduction

DISASTERS [e.g., weapons of mass destruction (WMD) attacks, earthquakes, hurricanes, tornadoes, etc.] may cause catastrophic failures in optical networks, as multiple network failures may occur in a disaster zone. Such failures could also be cascading, i.e., when a disaster occurs, initially a set of network elements may fail simultaneously, and then other failures in different parts of the network may occur subsequently (e.g., due to a power outage after an earthquake). Recent disasters show the enormous loss of network resources both by initial failure and correlated cascading failures (CCFs) [1]–[6]. For instance, in the 2008 Shichuan earthquake, around 30 000 km of fiber optic cables and 4000 telecom offices were damaged [1]. The power outages and floods caused by Hurricane Katrina reduced telecom network availability from approx. 99.99% to 85% [2]. Around 1,500 telecom buildings experienced long power outages by the mainshock on March 11 in the 2011 Japan Earthquake and Tsunami; while most were fixed, 700 telecom buildings experienced power outages by the aftershock on April 7, 2011 [4]. Because of the potential huge loss due to network disruptions, a network operator (NO) should proactively and/or reactively protect network resources from such failures, even if they are infrequent.

Several studies (e.g., [7]–[16]) aim to define the parts of the network that are more vulnerable to regional/correlated failures caused by disasters for analysis and/or design purposes. NOs can exploit the information on vulnerable regions of the network to proactively and/or reactively take necessary actions to minimize the loss. How to allocate resources before a disaster and re-allocate them after a disaster is a traffic engineering (TE) problem.

In this work, we focus on this problem by exploring the *risk* of traversing through the vulnerable parts in an optical backbone network. Risk is defined as the expected value of some outcome seen as undesirable. Ref. [17] proposes a risk model for transportation networks in case of an earthquake. We investigate a similar risk analysis for optical networks in terms of penalty paid by the NO to the customers. This penalty is usually stated in a service level agreement and expressed in terms of "penalty per unit time" for the downtime exceeding an allowed downtime (ADT).

Our contribution is three-fold. First, we develop a probabilistic *risk model* to analyze the loss/penalty, given the set of possible disasters. Second, we provide a *proactive* TE solution for disaster protection by investigating a disaster-risk-aware provisioning, where we develop a mathematical model that reduces the risk and decreases the loss/penalty in case of a disaster. Third, we investigate a *reactive* TE solution where disrupted connections and connections under the risk of CCFs are reprovisioned. We formulate the problems as mathematical models which turn out to be integer linear programs (ILPs). Since ILP models are intractable for large networks, we also develop heuristics to solve these problems. Numerical examples show that our approaches reduce the risk of disaster failures and loss to the NO with a slight increase in the capacity required to provide disaster resiliency.

A. Related Work

The first step in disaster survivability is *modelling the disaster* by using either a *deterministic* [7]–[12] or a *probabilistic* model [13]–[16]. In the deterministic model, a network element fails with probability 1 if it is in the disaster zone. With this model, network elements in a disaster zone can be defined as a shared risk group (SRG). Therefore, a SRG-disjoint pair of primary

Manuscript received November 20, 2013; revised May 19, 2014; accepted June 25, 2014. Date of publication July 1, 2014; date of current version August 11, 2014. This work was supported by the Defense Threat Reduction Agency (DTRA) under Grant HDTRA1-10-1-0011. This paper was presented in part at the OFC'12 conference.

F. Dikbiyik was with the University of California, Davis, CA 95616 USA He is now with the Department of Computer Engineering, Sakarya University, 54180, Sakarya, Turkey (e-mail: fdikbiyik@sakarya.edu.tr).
M. Tornatore is with the University of California, Davis, CA 95616 USA, and also with the, Department of Electronics and Information, Politecnico di Milano, , 20133 Milan, Italy (e-mail: tornator@elet.polimi.it).
B. Mukherjee is with the University of California, Davis, CA 95616 USA (e-mail: bmukherjee@ucdavis.edu).

Color versions of one or more of the figures in this paper are available online.

and backup paths can be used to provide survivability against disasters [18], [19].

More realistically, the disaster model can be *probabilistic*, where a network equipment in a disaster zone fails with some probability, which depends on dimensions of equipment (e.g., length of the link), its distance from the disaster's epicenter, the link length and its intersection with the failure region, etc. [14], [15]. The probability of a network-element failure caused by a disaster is also disaster dependent, e.g., earthquake versus hurricane zone. Some early works on disaster survivability [20], [21] provide relevant network survivability metrics.

Most *proactive* approaches consider deterministic or probabilistic SRG-disjoint paths [16], [18], [19], but SRG-disjointness may be infeasible. For instance, if a node has only two links which are in the same SRG and this node is destination or source of a connection, then this connection cannot be protected by two SRG-disjoint paths. Besides, SRG-disjointness considers that only one SRG failure can occur at a time. Multiple correlated scenarios (e.g., simultaneous or sequential WMD attacks) should also be considered [12], [13].

Reactive approaches try to solve the problem of reprovisioning of connections after a disaster failure. Ref. [12] develops provisioning/reprovisioning methods by creating subgraphs (obtained for each SRG by removing links of SRG). In this approach, connections' alternate paths for each SRG failure are computed in advance while provisioning the connection. If the connection cannot find an alternate path for each SRG, the connection is rejected (unless its source or destination nodes are in an SRG). Instead of rejection (because requested bandwidth is not available due to disaster failure), Ref. [22] proposes degraded service (offering less bandwidth than requested) by exploiting multipath provisioning, where connections are (re)provisioned over multiple paths, each of which carries a portion of the requested bandwidth.

B. Our Contribution

Our study uses a probabilistic disaster model that considers the physical locations of network equipments (e.g., physical routes of fiber links), their distances from the disaster's epicenter, and type of disaster. By exploiting this information, we define a vulnerability metric: disaster risk, which captures the possible disasters, their probable effects on the network, and the loss to a NO due to each disaster.

We investigate a proactive approach, disaster-risk-aware provisioning, where valuable connections (i.e., those which cost more than others when they are lost) are routed on no-(or low-) risk regions. This approach reduces the risk and penalty in case of a disaster by encouraging SRG-disjointness and finding a low-risk solution when SRG-disjointness is infeasible. We show that risk-aware provisioning can be combined with traditional approaches against single-link failures [e.g., dedicated-path protection (DPP)].

As new technologies create flexibility to reconfigure network equipments, NOs should also respond quickly to post-disaster scenarios by reprovisioning connections. Not only the connections interrupted but also the connections under the risk of CCFs should be reprovisioned. Thus, we investigate a risk-aware reprovisioning method.

In this study, results have been collected under practical assumptions to model disasters, and to evaluate proactive and reactive techniques. We investigate risk-awareness and SRG-awareness under different types of disaster scenarios; and we show that disaster failures should be expressed differently than existing SRG modelling by considering CCFs.

Our approaches are applicable to general mesh networks. However, we focus on wavelength-division multiplexing optical backbone networks where a connection requires a full wavelength channel.

II. Risk Assessment

Any risk analysis should answer three basic questions [23]:

1) What can happen?
2) How likely that it will happen?
3) If it does happen, what are the consequences?

In [17], the authors introduce a risk parameter which captures all these questions to investigate the risk of earthquakes in transportation networks. Similarly, we interpret and answer these questions to define the disaster risk in telecom networks.

What can happen? We focus on disasters which may cause failures (e.g., fiber cuts) of network elements. Disasters' scales and damage zones (usually defined by a radius) give us the network elements which might be disconnected. Thus, for a given network $G(V, E)$ (where V is set of nodes and E is the set of links), we define a set (N) of possible disasters that might cause failures, where each disaster n can be represented by S_n ($S_n \subset E$), set of fiber links[1] that might be disconnected by disaster n, and p^n_{fail} as the probability that disaster n causes failures of network elements.

How likely that it will happen? In this study, we focus not only on the probability of a disaster but also on the probability of network-element failure by a disaster on a specific scale. Let $p_{\text{fail|n}}$ and p_n denote the probability of a network-element failure in case of disaster n and the probability of disaster n, respectively. Then, the probability that disaster n causes failures of network elements (p^n_{fail}) equals $p_{\text{fail|n}} \times p_n$. Note that $p_{\text{fail|n}}$ depends on many parameters such as distance from epicenter [13], intensity of disaster, and type of disaster[2].

If it does happen, what are the consequences? Disasters may disrupt many connections. In a network, where connections' requirements are different, disrupting some connections might cost more than disrupting others. Let c_t denote the penalty per unit time of connection t. The loss (per unit time) to the NO in case of disaster n will be $\sum_{t \in T_n} c_t$, where T_n is the set of connections disrupted by disaster n. Thus, a risk

[1] Here, we define network-element failures by link failures. For instance, if a node fails, we denote this failure by failures of the links attached to it.

[2] For instance, *i*) the probability of a link failure with low-scale (non-destructive) and a high-scale (destructive) earthquake are different, as the probabilities of a low-scale and a high-scale earthquake are also different, *ii*) the probability of failure due to an earthquake is higher around the epicenter than probability of failure around the epicenter of a hurricane, while effects of hurricanes spread over a larger area than effects of earthquakes [24].

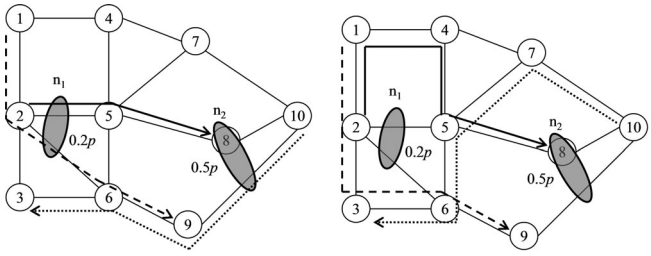

Fig. 1. Risk reduction by risk-aware provisioning. (a) Risk-unaware provisioning. (b) Risk-aware provisioning.

(i.e., expected cost) model is defined as follows:

$$\sum_{n\in N}\sum_{t\in T_n} c_t p^n_{\text{fail}}. \tag{1}$$

We also consider the following penalty model, which the NO should pay in case of a disaster. Let h_n and h^t_{ADT} denote the recovery time from disaster n and ADT of connection t. Then, the penalty in case of disaster n is

$$\sum_{t\in T_n} c_t \left(h_n - h^t_{\text{ADT}}\right). \tag{2}$$

Note that h_n may be in weeks, while h^t_{ADT} is usually in hours. For example, for a connection with 0.9999 availability requirement, ADT in a year is about 1 h. Thus, $h_n >> h^t_{\text{ADT}}$, and the penalty could be approximated by $\sum_{t\in T_n} c_t h_n$

III. Disaster-Risk-Aware Provisioning

A provisioning approach that minimizes the risk will reduce cost to a NO in case of a disaster. Fig. 1 shows how a NO can reduce this penalty by minimizing the risk. Fig. 1 depicts a ten-node topology with two disaster zones, n_1 and n_2, where $p^{n_1}_{\text{fail}} = 0.2p$, $p^{n_1}_{\text{fail}} = 0.5p$, and p is a small probability. Three connection requests arrive: t_1 from node 1 to node 9, t_2 from node 2 to node 8, and t_3 from node 10 to node 3. c_{t_1}, c_{t_2}, and c_{t_3} are equal to α, 2α, and 3α, respectively, where α is a value to parametrize penalty (e.g., penalty per hour). Fig. 1(a) shows the provisioning of connections (t_1, t_2, and t_3 are shown by dashed, solid, and dotted lines, respectively) with a shortest-path approach without risk-awareness. In this case, risk [calculated by Eq. (1)] is equal to $3.1\,p\alpha$; and if disasters n_1 or n_2 occur, penalty per unit time will be 3α for n_1 and 5α for n_2. However, risk-aware provisioning [see Fig. 1(b)] can reduce the risk by around 68% (from $3.1\,p\alpha$ to $p\alpha$) where penalty reduction for n_1 is 100% (since none of the connections traverse n_1) and 60% for n_2. Note that, since a destination node is in disaster zone n_2, we cannot avoid traversing n_2 to provision t_2. We formulate the risk-aware provisioning problem as an ILP as follows.

Given:

- $G(V, E)$: Network topology, where *V* is set of nodes and *E* is set of links.
- $T = \{t =< s_t, d_t >\}$: Set of connections where s_t and d_t are the source and destination of connection t.
- $N = \{n =< S_n, p^n_{\text{fail}} >\}$: Set of disasters with S_n ($S_n \subset E$), set of fiber links might be disconnected by disaster n, and p^{fail}_d, probability that disaster n causes a failure.
- W_{ij}: Number of wavelengths on link (i, j)

Binary variables:

- R^n_t: 1 if connection t is lost in case of disaster n.
- R^t_{ij}: 1 if connection t is routed on fiber link (i, j).

Objective

$$\min\left(\sum_{n\in N}\left(\sum_{t\in T} c_t R^n_t\right) p^n_{\text{fail}} + \epsilon \sum_{t\in T}\sum_{(i,j)\in E} R^t_{ij}\right) \tag{3}$$

Binarization

$$R^n_t \geq \frac{1}{M}\sum_{(i,j)\in S_n} R^t_{ij}, \forall t \in T, n \in N \tag{4a}$$

$$R^n_t \leq \sum_{(i,j)\in S_n} R^t_{ij}, \forall t \in T, n \in N \tag{4b}$$

Flow-conservation constraints

$$\sum_{(k,j)\in E} R^t_{kj} - \sum_{(i,k)\in E} R^t_{ik} = \begin{cases} -1, & \text{if } k = s_t \\ 1, & \text{if } k = d_t \\ 0, & \text{otherwise.} \end{cases} \quad \forall t \in T \tag{5}$$

Link-capacity constraints

$$\sum_{t\in T} R^t_{ij} \leq W_{ij}, \forall (i, j) \in E. \tag{6}$$

In the objective function [Eq. (3)], the first term is risk and the second term in the objective function is required to avoid long backup paths, where ϵ should be a small number to avoid compromising the primary objective (the first term in the objective function related to risk). From our numerical studies, we note that ϵ should not exceed 10^{-5}, otherwise the ILP starts increasing the risk to decrease total resource consumption. Eq. (4) is required to understand if a connection is lost by a disaster, where M is a large number (e.g., 10^3). Eqs. (5) and (6) show flow-conservation and link-capacity constraints.

Since we can test a solution for binary variables R^t_{ij} and R^n_t in polynomial time, our problem is in the class of NP. If we assume $|N| = 0$, then our formulation becomes the standard arc-flow multi-commodity problem (ACMP) that is proven to be NP-complete [25]. So our problem is transformable to standard ACMP and therefore NP-complete.

In this ILP, the number of variables is $|T|(|N| + |E|)$ and the number of constraints is $2|T||N| + 3|T| + |E|$ versus, for a risk-unaware approach that minimizes resources without having concern about the disaster, the number of variables is $|T||E|$ and the number of constraints is $3|T| + |E|$. Thus, the product of number of connections and the number of disasters provides additional running time for risk-aware approach compared to risk-unaware approach. So, we can easily say that the disaster type affects the running time of the ILP, because the size of the disaster set is strongly correlated to the type of the disaster.

Since ILP returns an optimal solution, but has high time complexity, we develop a heuristic, shown in Algorithm 1, which sequentially fixes the variables starting from high-cost

connections (with high c_t values) using the cost function in Eq. (7), where if the connection can find a path with SRG avoidance, this path is preferred; otherwise the path with the minimum risk is chosen. Since connections are sorted in descending order with respect to their c_t values, high-cost connections have more opportunity to be provisioned on safe links. A shortest-path algorithm has computational complexity of $O(|E| + |V| \log |V|)$ for the given topology $G(V, E)$. Shortest-path algorithm is run for each connection, so the complexity of the algorithm is $O(|T| \times (|E| + |V| \log |V|)$. Note that the ILP for risk-aware provisioning also allows us to rigorously define the re-provisioning problem in Section IV.

Algorithm 1 Risk-Aware Provisioning

1: Sort connections in descending order w.r.t. their c_t values.
2: **for all** $t \in T$ **do**
3: Update link cost as follows:

$$C_{ij} = \begin{cases} \infty, & \text{if } F_{ij} = 0 \\ \epsilon, & \text{if } \forall n \in N : (i,j) \notin S_n \\ a_{ij} + \epsilon * (W_{ij} - F_{ij}) & \text{otherwise} \end{cases} \tag{7}$$

where F_{ij} is the number of free wavelengths on link (i, j) and $a_{ij} = -c_t / \log(\max_{n \in N} p^n_{\text{fail}})$.
4: Find shortest path from s_t to d_t and provision t on it.

NOs traditionally protect connections against single-link failures by provisioning connections on a primary path and a link-disjoint dedicated-backup path (DPP). Using DPP, a connection will be lost in a disaster, if both primary and backup paths are disconnected. We modify our model by using the following binary variables.

- Z^n_t: 1 if both primary and backup paths of connection t are disconnected by disaster n.
- B^n_t: 1 if backup path of t is disconnected by disaster n.
- B^t_{ij}: 1 if backup path of t is routed on link (i, j).

The new objective function is shown below

$$\min \left(\sum_{n \in N} \left(\sum_{t \in T} c_t Z^n_t \right) p^n_{\text{fail}} + \epsilon \sum_{t \in T} \sum_{(i,j) \in E} \left(R^t_{ij} + B^t_{ij} \right) \right). \tag{8}$$

Binarization and flow-conservation constraints for backup path are similar to Eqs. (4) and (5) and can be obtained by replacing notation R^n_t and R^t_{ij} by B^n_t and B^t_{ij}, respectively. Following equations are required to understand if both primary and backup paths of a connection are disconnected by a disaster

$$Z^n_t \leq R^n_t, \forall t \in T, n \in N \tag{9a}$$

$$Z^n_t \leq B^n_t, \forall t \in T, n \in N \tag{9b}$$

$$Z^n_t \geq R^n_t + B^n_t - 1, \forall t \in T, n \in N. \tag{9c}$$

To ensure primary and backup paths are link-disjoint, we need

$$R^t_{ij} + B^t_{ij} + R^t_{ji} + B^t_{ji} \leq 1, \forall t \in T, (i,j) \in E. \tag{10}$$

Link-capacity constraints are also revised as follows:

$$\sum_{t \in T} \left(R^t_{ij} + B^t_{ij} \right) \leq W_{ij}, \forall (i,j) \in E. \tag{11}$$

Similar to our previous ILP formulation for no-protection case, we can test a solution for binary variables R^t_{ij}, R^n_t, B^t_{ij}, and B^n_t in polynomial time, so our problem is in the class of NP. If we assume $|N| = 0$, then our formulation becomes the standard arc-flow formulation for DPP (ACDPP) that is proven to be NP-complete [26]. So our problem is transformable to standard ACDPP and therefore NP-complete.

In this ILP, the number of variables is $|T|(3|N| + 2|E|)$ and the number of constraints is $7|T||N| + 6|T| + |T||E| + |E|$ versus, for a risk-unaware DPP approach that minimizes resources without having concern about the disaster, the number of variables is $2|T||E|$ and the number of constraints is $6|T| + |T||E| + |E|$. Thus, again the product of number of connections and the number of disasters provides additional running time for risk-aware DPP approach compared to risk-unaware DPP approach.

For a heuristic solution, we use Algorithm 1 to provision primary paths[3]. After provisioning each primary path, we find a backup path by updating link costs for each connection t as follows:

$$C_{ij} = \begin{cases} \infty, & \text{if } F_{ij} = 0 \vee (i,j) \in r_t \\ \epsilon, & \text{if } (i,j) \notin D_t \\ a_{ij} + \epsilon * (W_{ij} - F_{ij}), & \text{otherwise} \end{cases} \tag{12}$$

where r_t and D_t are the sets of links on primary path and those traversing a disaster zone, respectively. Note that connections are sorted with respect to their c_t values, so SRG-disjoint paths are preferable. But, if SRG-disjointness is infeasible, the links traversing less-risky regions are chosen. The complexity of the algorithm becomes $O(2|T| \times (|E| + |V| \log |V|)$, because shortest-path algorithm is run for both primary and backup paths.

IV. Risk-Aware Reprovisioning

Ref. [27] shows how to reprovision connections when network state changes (because of arrival or termination of a connection, or failure or repair of a network element). Similarly, disaster-risk-aware reprovisioning can be performed after a disaster failure or change of risk information.

After the initial impact of a disaster, some network elements may directly fail. Connections traversing these network elements can be reprovisioned by exploiting the excess capacity[4] in undamaged areas, unless the destination or source node of a connection is in the damaged area. The initial impact may also introduce CCFs, which might cause more disruptions. For instance, a disaster may cause power outages because of disruption on the electric grid (or technical problems in a power plant)

[3] After time the cost (Step 3 in Algorithm 1), searching for two link-disjoint paths from s_t to d_t, and then provisioning the primary path on the shortest one helps to guarantee that at least one link-disjoint backup path exists.

[4] Note that excess capacity is unused capacity in a network to accommodate traffic fluctuations and avoid capacity exhaustion [28].

and generator-dependent network elements will eventually suffer from power outages due to limited diesel supplies after a disaster. Some studies report such network element failures due to CCFs, especially due to power outages, after a disaster like Shichuan Earthquake in 2008 [1], Hurricane Katrina in 2005 [2], Hurricane Sandy in 2012 [3]. Some recent works [29]–[31] focus on the interdependency between the power grid and telecom networks; and they show how power outages can affect telecom networks. Another example is correlated sequential WMD attacks, where after a WMD attack, there may be possible threats for some other locations. These cascading or sequential failures are more predictable by observing the damage and location of the first impact of the disaster. Thus, we need to reprovision connections under the risk of correlated cascading or sequential failures.

Given the damaged topology $\bar{G}(\bar{V}, \bar{E})$, where some network resources are not functional, and the set of possible correlated cascading or sequential failures ($J = \{j =< S_j >\}$ where S_j is the set of links which might be disconnected by failure j, a NO can reprovision connections to relieve the network. We prefer reprovisioning a subset of connections (those traversing a damaged area and those under the risk of correlated failures), denoted by T_r, instead of reprovisioning all (T) for short reprovisioning time. The risk of CCFs can be defined as

$$\sum_{j \in J} \left(\sum_{t \in T_r} c_t Q_t^j \right) q_{\text{fail}}^j \tag{13}$$

where Q_t^j is 1 if connection t is lost by failure j and q_{fail}^j is the probability of link failure by CCF j. Note that q_{fail}^j values are usually much larger than p_{fail}^n, because, after a disaster, expectations of failures due to post-disaster events are high [32]. We formulate the risk-aware reprovisioning problem also as an ILP whose objective is

$$\min \left(\sum_{j \in J} \left(\sum_{t \in T} c_t Q_t^j \right) q_{\text{fail}}^j + \epsilon \sum_{t \in T} \sum_{(i,j) \in \bar{E}} R_{ij}^t \right) \tag{14}$$

and the binarization constraints are

$$Q_t^j \geq \frac{1}{M} \sum_{(i,j) \in S_n} R_{ij}^t, \ \ \forall t \in T, j \in J \tag{15a}$$

$$Q_t^j \leq \sum_{(i,j) \in S_j} R_{ij}^t, \ \ \forall t \in T, j \in J. \tag{15b}$$

The flow-conservation and link-capacity constraints in Eqs. (5) and (6) hold except E and W_{ij} are replaced by $\bar{E}$ and F_{ij}, respectively. Typically T_r and J are small sets (compared to T and N), so ILP is tractable for typical traffic distributions and backbone networks. However, a heuristic can be developed by modifying Alg. 1 by replacing N and T by J and T_r. Similar to risk-aware provisioning, the running time of this ILP increases with the increase of $|J||T_r|$ that is typically much smaller than $|N||T|$, thus running time for this ILP is much shorter than ILP formulation for risk-aware provisioning.

Since the q_{fail}^j values are usually close to 1, e.g., after a disaster, a power outage is highly expected and power-related CCFs on telecom networks is highly likely, risk-aware reprovisioning leads close results to a deterministic approach, i.e., the failure expectations of a network element in a CCF region is 1.

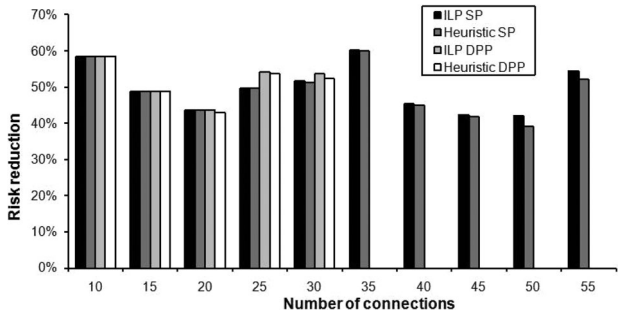

Fig. 2. Risk reduction for ILP and heuristic solutions.

Risk-aware reprovisioning is also necessary when risk information is updated. Especially, the existence of early-warning systems may help a NO to take necessary actions in advance. For instance, warning time for hurricanes may be in hours [33] and for earthquakes may be in tens of seconds [34] which can give enough time to reprovision connections. The time to reprovision a connection can be formulated as $(m+1) \times (h_p + h_c)$ where m is number of links on a connection's path, h_p and h_c are message-processing delay and time to configure, test, and setup an optical cross-connect, respectively. Then, neglecting the decision time (running time for ILP), the estimated time required to reprovision connections[5] is $|T_r| \times (\bar{m}+1) \times (h_p + h_c)$, where $\bar{m}$ is average number of links on a connection's path. Typical values for h_p and h_c [35] are 10 μs and 5–10 ms, respectively. In our numerical examples, we see that, even at high network load and a large-scale disaster, the running time for ILP is under 2 s. Then, in 10 s, hundreds of connections can be reprovisioned.

V. Illustrative Numerical Examples

A. ILP Versus Heuristic

First, we investigate the performance of the heuristic by comparing it to the optimal solution obtained by ILP on a small topology, where the ILP is tractable. We consider the 10-node topology in Fig. 1 with disaster zones n_1 and n_2. The network has 16 wavelengths/link in each direction and wavelength conversion. Traffic is uniformly distributed among node pairs. We conduct numerical examples for single-path (SP) solution and DPP, where number of connections $|T|$ varies between 10 and 55. Fig. 2 shows average risk reduction for 50 runs (compared to a risk-unaware approach that minimizes resource usage). Note that, for DPP, when $|T| \geq 35$, there is no feasible solution. For both SP and DPP, heuristic shows close performance to ILP while reducing the running time significantly. While the running time for ILP varies between 325 s (for $|T| = 10$ with SP) to 11,250 s (for $|T| = 55$ with SP), the running times for heuristics are much shorter (varies between 10 to 352 s) on a standard Intel Core i5 760 @2.80 GHz computer.

[5]The estimation of reprovisioning is estimated under the assumption of sequential reprovisioning of connections. In case of parallel reprovisioning, the total reprovisioning time would be much smaller.

Fig. 3. US-wide topology.

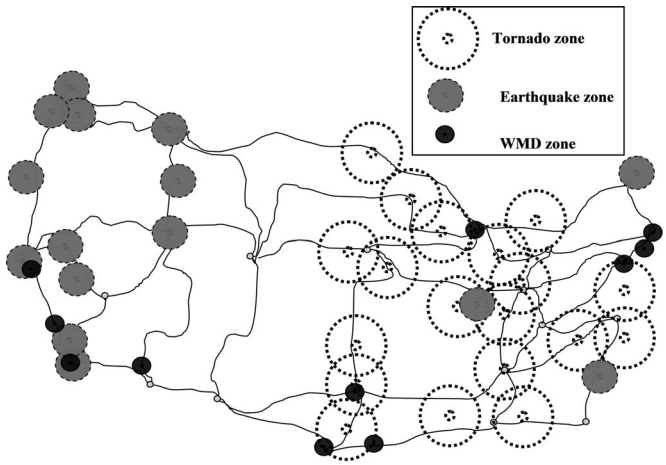

Fig. 4. Disaster zones for earthquakes, tornadoes, and WMD attacks.

B. Topology and Traffic Profile

We study our heuristics on a 24-node topology (see Fig. 3) with 32 wavelengths/link in each direction and with wavelength conversion. To understand if a link is affected by a disaster, we have to know the exact locations of the links. Thus, we match the network with the US transportation map, assuming fiber optic cables are close to highways or railroads.

We consider that connection requests are proportional to the populations of source and destination (i.e., connections are mostly originated from/destined to New York, Los Angeles, and Chicago areas) [36]. We assign connections different c_t (penalty per unit time) values: 10α, 5α, 3α, and α with the distribution 1: 2: 3: 4, where the number of connections with high penalty is less than the others. α is some value to parameterize the penalty (e.g., penalty per hour). The number of generated connections varies between 50 and 450. Results shown below are averages over 50 generations with 95% confidence intervals.

C. Disaster Zones

We consider three types of disasters: two natural disasters (earthquake and tornado) and one human-made disaster (WMD attack) and determine the values of p^n_{fail} accordingly.

1) Earthquakes and Tornadoes: Seismic hazard maps help us to understand the probability of an earthquake. For instance, the US hazard map with 2% probability of exceedence (p_n) in 50 years is provided in [39]. The probability that an earthquake is strong enough to damage network elements ($p_{\text{fail}|\text{n}}$) will be different for different seismic levels that are defined in the units of ground peak acceleration (g) in seismic hazard maps. Several surveys and geological papers (e.g., [4], [24], [40], [41]) guide us to understand damage of an earthquake on network elements, and we can assume that the probability of damage from an earthquake on network elements are negligible for the hazard levels below $0.32\,g$. For higher hazard levels, the probability increases with increasing hazard risk. For tornadoes, we consider that the probability of a tornado (p_n) at a specific location is proportional to the number of occurrences in the past and probability of failure ($p_{\text{fail}|\text{n}}$) in case of non-intense tornadoes (EF0, EF1, and EF2, where EF is Enhanced Fujita scale, which rates the strength of tornadoes) is negligible, while, for intense tornadoes (EF3 and higher), it is proportional to the intensity. We determine 15 distinct SRGs for earthquakes and 19 distinct SRGs for tonadoes (see Fig. 4) by matching seismic hazard map and tornado activity map with US topology considering that the damages of earthquakes and tornadoes (clustered in a region) may span up to 96 and 160 km, respectively [24]. Note that a large number of tornadoes may also occur simultaneously (or near simultaneously) and can create a tornado outbreak spanning a large area [38].

2) WMD Attacks: WMD attacks usually target populated cities and cities where important government, military, or resource facilities are located. As an example, we consider the ten most-populated cities and Washington DC as possible WMD targets (shown in Fig. 4), and we let the probability that a city is targeted (p_n) to be proportional to its population or its importance. We assume that the probability of damage in case of a WMD attack ($p_{\text{fail}|\text{n}}$) is close to 1, because these attacks are destructive.

D. Proactive Approach

We show the graphical distribution of 500 connections' cost on network links in Fig. 5 to compare risk-unaware and risk-aware provisioning considering the earthquake zones determined above. The thickness of a link is proportional to the cost of connections provisioned on that link. Fig. 5 shows that the risk-aware approach avoids risky regions as much as possible, usually by exploiting the excess capacity of safe links.

We evaluate our approaches in terms of risk and penalty reduction and increase in (consumed) resources (in terms of number of wavelength links) compared to an SRG-unaware approach which minimizes resource consumption. We compare our approach with two other approaches:

1) SRG-Aware Approach (SRG-A): For SP provisioning, if a path, which does not traverse any SRG, is found between s_t and d_t for connection t, the connection is provisioned on this path. Otherwise, the connection is provisioned on the shortest path. For DPP, if an SRG-disjoint (and link-disjoint) path pair exists between s_t and d_t, the connection is provisioned on this path

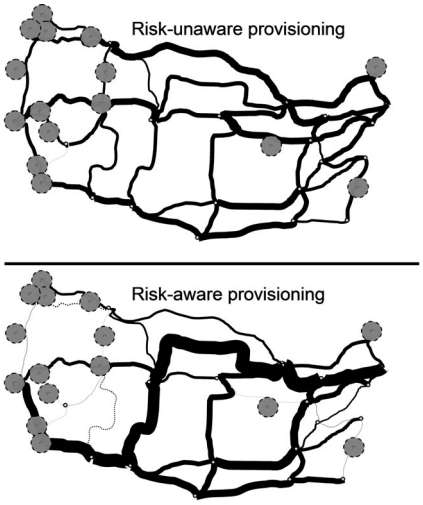

Fig. 5. Risk-aware approach versus risk-unaware approach for earthquakes.

pair. Otherwise, the connection is provisioned on the shortest link-disjoint path pair.

2) Probabilistic SRG-Aware Approach (pSRG-A): Ref. [16] investigates provisioning strategies when SRGs with different probabilities exists. For SP provisioning, connections are provisioned on a path which has minimum failure probability. For DPP, the authors consider joint path-failure probabilities. Ref. [42] enhances the work in [16] by considering load balancing using a method which finds k link-disjoint path pairs considering load balancing and selects the path pair with minimum failure probability. We consider this enhanced version to compare with our approach for DPP.

a) Single-path disaster-risk-aware provisioning: Fig. 6 shows risk reduction with SP provisioning in upper graphs for tornado (left), earthquake (middle), and WMD (right) scenarios by lines. The risk becomes closer to that with SRG-unaware (i.e., shortest-path) approach when traffic load increases, because more connections traverse disaster zones. Our risk-aware approach reduces the risk more (20–45%) compared to SRG-A and pSRG-A. Since SRG-A uses shortest path when SRG avoidance is not possible, it shows the highest risk values. Even though pSRG-A is a probabilistic approach, it only considers the probability of failures rather than loss to the NO for a specific failure (in fact, when load increases, the results for pSRG-A become closer to SRG-A). Thus, our approach reduces risk more than these two approaches. Fig. 6 also shows how much additional resources in terms of wavelength-links (by columns) are required to reduce the risk and penalty. Additional resources for risk-awareness are close to additional resources required for SRG-awareness. The increase in resources also depends on the disaster type, e.g., for WMD attacks, where disaster zones are small and usually include nodes, our approach requires more resources than earthquake and tornado zones (which are larger zones and clustered on specific regions).

The reader may ask what this risk reduction really means for disaster survivability and whether it is worth to increase consumed resources to have such risk reduction. To answer this question, we give examples of penalty reduction for some highly-likely disasters. Fig. 7 shows penalty reduction obtained by our approach, SRG-A, and pSRG-A compared to SRG-unaware approach for two tornado zones (in Kansas City MO and Frankfurt KY—both in tornado alley [37], [38]); a tornado outbreak (tornadoes occuring sequentially on multiple regions) spanning from Illionis to Alabama; two earthquake zones (San Francisco and Los Angeles—both located on San Andreas fault line); and two WMD zones (Washington DC as the federal capital and New York as the most populated city). Results show that risk-awareness helps to significantly decrease penalty.

TABLE I
AVERAGE PENALTY REDUCTION COMPARED TO SRG-UNAWARE DPP OVER POSSIBLE DISASTERS

	Tornado	Earthquake	WMD
Risk-A	24.75%	18.00%	34.52%
pSRG-A	22.76%	16.49%	26.34%
SRG-A	20.78%	14.98%	24.08%

b) Disaster-risk-aware provisioning with DPP: DPP without risk awareness may protect connections from disaster zones which affect only one link. However, it fails when a disaster affects nodes or multiple links. Fig. 6 shows risk reduction compared to SRG-unaware DPP by lines in lower graphs. Our approach significantly reduces the risk. The risk reduction is close to SRG-A and pSRG-A for tornadoes, but more for earthquakes and WMD attacks. Fig. 6 also shows increase in resources to reduce the risk by columns. The results are close to each other, i.e., additional resources required to reduce the risk are not much compared to SRG-aware approaches. Note that, even though risk results are close to each other, our approach can still reduce average penalty more than risk-unaware approaches (Table I).

E. Reactive Approach

To evaluate our reactive approach, we consider numerical examples where we provision 450 connections, and there is a WMD attack on Washington DC. After the attack, some network resources will not be available until full recovery. 43% of the connections traversing the node located in Washington DC can be reprovisioned since they are not destined to or originated from this node. For reprovisioning, we should also consider the CCFs and possible sequential attacks. For instance, the damage on the electric grid and some power station (e.g., Calvert Cliffs nuclear power plant in Lusby, Maryland, a nearby city to Washington DC) may cause large blackouts which might affect the node in Princeton NJ. Thus, there is a high risk of CCFs for this node and links in the SRG, and 16% of connections traversing this node can be reprovisioned. We also consider that Los Angeles CA is under risk of a correlated secondary WMD attack which might affect the link between Palo Alto CA and San Diego CA. All connections traversing this link can be reprovisioned (depending on the excess capacity in other parts of the network).

In Fig. 8, the first column shows the penalty from the main attack (on Washington DC) at the bottom, from CCF in Princeton

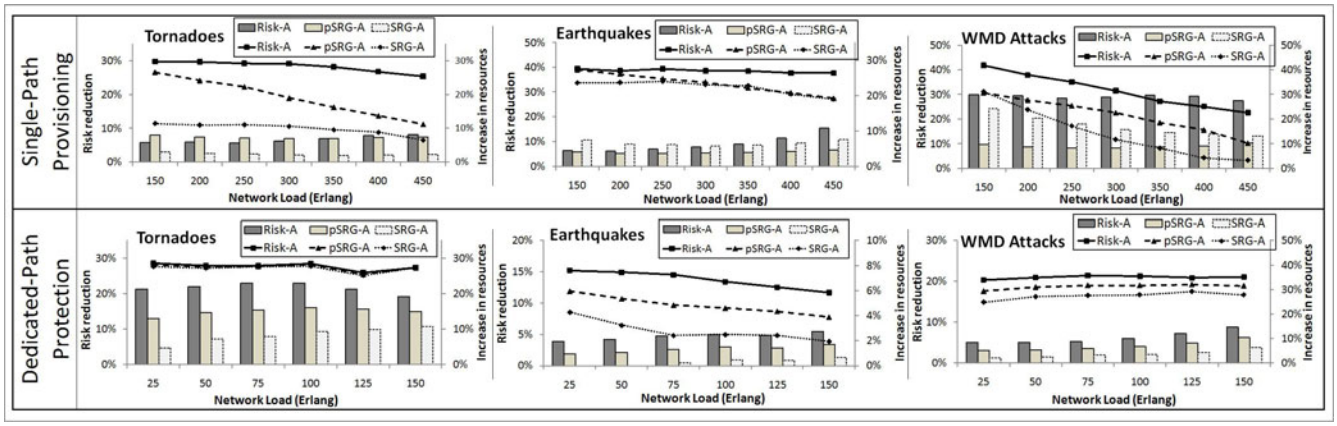

Fig. 6. Risk reduction (lines) and increase in resources (columns) compared to SRG-unaware approaches for SP provisioning and DPP.

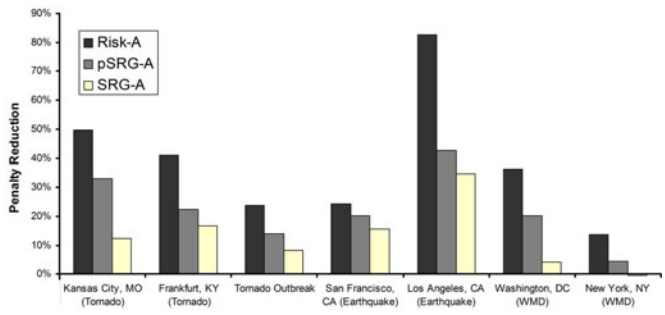

Fig. 7. Average penalty reduction (compared to SRG-unaware approach) in case of highly-likely disasters.

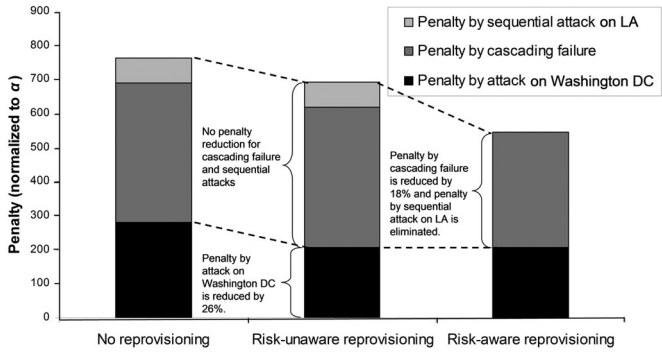

Fig. 8. Penalty for CCFs and sequential attacks.

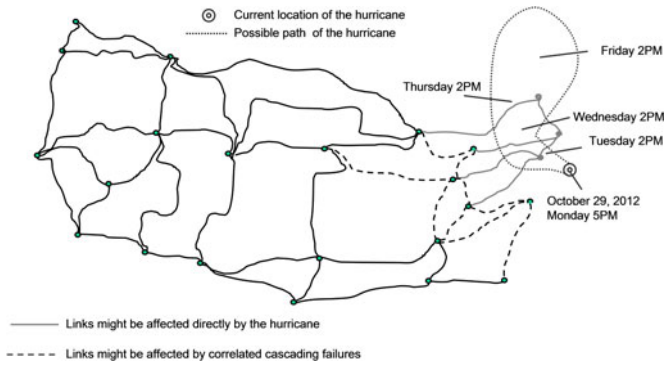

Fig. 9. Possible path of Hurricane Sandy estimated on October 29, 2012, and its possible effects on the topology.

NJ in the middle, and from a sequential attack on Los Angeles CA at the top, if the NO does not reprovision any connection. If the NO reprovisions only the connections traversing Washington DC and does not consider reprovisioning connections under the risk of CCFs or sequential attacks, i.e., risk-unaware reprovisioning (shown in second column), the penalty caused by the attack on Washington DC is reduced by 26%. However, the total penalty reduction (considering all failures) will be 9.5% since the penalties from correlated failures are not changed. Additional to 26% penalty reduction in Washington DC area, risk-aware reprovisioning (shown in third column) provides 18% penalty reduction for a CCF in Princeton NJ, and 100% penalty reduction for the connections traversing Los Angeles CA. The total penalty reduction is increased to 28.7%.

Risk-aware reprovisioning can also be useful to better prepare the network when a disaster is predicted. For instance, Fig. 9 shows the path of Hurricane Sandy estimated on October 29, 2012, and its possible effects on the topology. We consider the probability that a link fails due to CCFs is proportional to its distance to the hurricane's possible path. Without risk awareness (i.e., CCFs are not considered), reprovisioning of resources can reduce penalty by 22% for network load = 450 Erlang. However, our risk-aware reprovisioning approach (ILP in Section IV) can reduce the penalty further, up to 53%.

VI. Conclusion

In this study, we focused on disaster survivability, a topic of increasing importance. First, we explored the *risk* of disaster failures in backbone optical networks. We investigated a probabilistic disaster model and defined a risk parameter. By exploiting this information, we developed a *disaster-risk-aware provisioning* scheme (a proactive approach) for SP provisioning and DPP to reduce the risk and loss (in terms of penalty paid by NO) in case of a disaster. We also explored CCFs and sequential events after a disaster and developed a *risk-aware reprovisioning*

scheme (a reactive approach) which recovers disrupted connections and takes precautions to protect connections from CCFs and sequential events. Illustrative numerical examples showed the efficiency of our approaches by considering different disaster types. Results show that our approaches provide significant risk and penalty reduction in case of a disaster with its CCFs and sequential events.

REFERENCES

[1] Y. Ran, "Considerations and suggestions on improvement of communication network disaster countermeasures after the Wenchuan earthquake," *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 44–47, Jan. 2011.

[2] A. Kwasinski, W. W. Weaver, P. L. Chapman, and P. T. Krein, "Telecommunications power plant damage assessment for Hurricane Katrina-site survey and follow-up results," *IEEE Syst. J.*, vol. 3, no. 3, pp. 277–287, Sep. 2009.

[3] A. Kwasinski, "Lessons from field damage assessments about communication networks power supply and infrastructure performance during natural disasters with a focus on Hurricane sandy," presented at the FCC Workshop Network Resiliency, Brooklyn, NY, USA, Feb. 2013.

[4] K. Tanaka, Y. Yamazaki, T. Okazawa, T. Suzuki, T. Kishimoto, and K. Iwata, "Experiment on seismic disaster characteristics of underground cable," presented at the 14th World Conf. Earthquake Eng., Beijing, China, Oct. 2008.

[5] T. Adachi, Y. Ishiyama, Y. Asakura, and K. Nakamura, "The restoration of telecom power damages by the great east Japan earthquake," presented at the 33rd IEEE Int. Telecommun. Energy Conf., Amsterdam, The Netherlands, Oct. 2011.

[6] K. Morrison, "Rapidly recovering from the catastrophic loss of a major telecommunications office," *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 28–35, Jan. 2011.

[7] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the vulnerability of fiber infrastructure to disasters," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1610–1623, Dec. 2011.

[8] S. Banerjee, S. Shirazipourazad, and A. Sen, "Design and analysis of networks with large components in presence of region-based faults," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, pp. 1–6.

[9] S. Banerjee, S. Shirazipourazad, P. Ghosh, and A. Sen, "Beyond connectivity—New metrics to evaluate robustness of networks," in *Proc. IEEE 12th Int. Conf. High Perform. Switching Routing*, Cartagena, Spain, Jul. 2011, pp. 171–177.

[10] K. Lee, E. Modiano, and H. Lee, "Cross-layer survivability in WDM based networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1000–1013, Dec. 2011.

[11] K. Lee, H. Lee, and E. Modiano, "Reliability in layered networks with random link failures," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1835–1848, Dec. 2011.

[12] M. Frederick, P. Datta, and A. Somani, "Sub-graph routing: A generalized fault-tolerant strategy for link failures in WDM optical networks," *Comput. Netw.*, vol. 50, no. 2, pp. 181–199, Feb. 2006.

[13] M. Rahnamay-Naeini, J. Pezoa, G. Azar, N. Ghani, and M. Hayat, "Modeling stochastic correlated network failures and assessing their effects on reliability," presented at the IEEE Int. Conf. Commun., Kyoto, Japan, Jun. 2010.

[14] X. Wang, X. Jiang, and A. Pattavina, "Assessing network vulnerability under probabilistic region failure model," in *Proc. IEEE 12th Int. Conf. High Perform. Switching Routing*, Cartagena, Spain, Jul. 2011, pp. 164–170.

[15] P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The resilience of WDM networks to probabilistic geographical failures," in *Proc. IEEE Conf. Comput. Commun.*, Shanghai, China, 2011, pp. 1521–1529 .

[16] H. 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.

[17] S. E. Chang, M. Shinozuka, and J. Moore, "Probabilistic earthquake scenarios: Extending risk analysis methodologies to spatially distributed systems," *Earthquake Spectra*, vol. 16, no. 3, pp. 557–572, Aug. 2000.

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

[19] J. Hu, "Diverse routing in optical mesh networks," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 489–494, Mar. 2003.

[20] Y. Kane-Esrig, G. Babler, R. Clapp, R. Doverspike, J. Healy, D. Kobayashi, D. Kolar, Y. Lurye, R. Marzec, J. Morgan, and S. Stevenson, "Survivability risk analysis and cost comparison of SONET architectures," in *Proc. IEEE Global Telecommun. Conf.*, Orlando, FL, USA, Dec. 1992, pp. 841–846.

[21] S. C. Liew and K. W. Lu, "A framework for characterizing disaster-based network survivability," *IEEE J. Sel. Areas Commun.*, vol. 12, no. 1, pp. 52–58, Jan. 1994.

[22] S. Huang, M. Xia, C. Martel, and B. Mukherjee, "A multistate multipath provisioning scheme for differentiated failures in telecom mesh networks," *J. Lightw. Technol.*, vol. 28, no. 11, pp. 1585–1596, Jun. 2010.

[23] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk Anal.*, vol. 1, no. 1, pp. 11–27, Mar. 1981.

[24] T. L. Weems, "How far is far enough?" *Disaster Recovery J.*, vol. 16, no. 2, Spring 2003.

[25] S. Even, A. Itai, and A. Shamir, "On the complexity of time table and multi-commodity flow problems," in *Proc. 16th Annu. Symp. Found. Comput. Sci.*, Oct. 1975, pp. 184–193.

[26] 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.

[27] L. Song, J. Zhang, and B. Mukherjee, "A comprehensive study on backup-bandwidth reprovisioning after network-state updates in survivable telecom mesh networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 6, pp. 1366–1377, Dec. 2008.

[28] F. Dikbiyik, L. Sahasrabuddhe, M. Tornatore, and B. Mukherjee, "Exploiting excess capacity to improve robustness of WDM mesh networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 114–124, Feb. 2012.

[29] M. Parandehgheibi, and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," presented at the IEEE Global Telecommun. Conf., Atlanta, GA, USA, Dec. 2013.

[30] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nat. Lett.*, vol. 464, pp. 1025–1028, Apr. 2010.

[31] A. Bernsteiny, D. Bienstockz, D. Hayx, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures analysis and control implications," presented at the IEEE Conf. Comput. Commun., Toronto, ON, Canada, 2014.

[32] S. Erjongmanee and C. Ji, "Large-scale network-service disruptions: Dependencies and external factors," *IEEE Trans. Netw. Serv. Manag.*, vol. 8, no. 4, pp. 375–386, Dec. 2011.

[33] R. W. Burpee, J. L. Franklin, S. J. Lord, R. E. Tuleya, and S. D. Aberson, "The impact of Omega dropwindsondes on operational Hurricane track forecast models," *Bull. Amer. Meteorol. Soc.*, vol. 77, no. 5, pp. 925–933, May 1996.

[34] R. M. Allen, "Probabilistic warning times for earthquake ground shaking in the San Francisco bay area," *Seismol. Res. Lett.*, vol. 77, no. 3, pp. 371–376, May 2006.

[35] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *J. Lightw. Technol.*, vol. 21, no. 4, pp. 870–883, Apr. 2003.

[36] M. Batayneh, D. Schupke, M. Hoffman, A. Kristaedter, and B. Mukherjee, "On routing and transmission-range determination of multi-bit-rate signals over mixed-line-rate WDM networks for carrier ethernet," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1304–1316, Oct. 2011.

[37] S. Perkins, "Tornado alley, USA: New map defines nation's twister risk," *Sci. News*, vol. 161, no. 19, pp. 296–298, May 2002.

[38] U.S. Tornado Climatology. *National Oceanic Atmospheric Administration*, Silver Spring, MD, USA. (2012). [Online]. Available: http://www.ncdc.noaa.gov/oa/climate/severeweather/tornadoes.html

[39] Hazard map. (2008). *US Geological Survey*, Reston, VA, USA. [Online]. Available: http://earthquake.usgs.gov/hazards/products/graphic2pct50.jpg

[40] G. Grünthal (Ed.), "Europan macroseismic scale 1998 (EMS-98)," *Cahiers du Centre Europeen de Geodynamique et de Seismologie*, vol. 15, Mar. 1998, pp. 1–99.

[41] Earthquake facts and statistics. *U.S. Geological Survey National Earthquake Information Center*, Reston, VA, USA. (2012). [Online]. Available: http://earthquake.usgs.gov/earthquakes/eqarchives/year/eqstats.php

[42] O. Diaz, F. Xu, N. Min-Allah, M. Khoedir, M. Peng, S. Khan, and N. Ghani, "Network survivability for multiple probabilistic failures," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1320–1323, Aug. 2012.