IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 11, 2019, accepted May 4, 2019, date of publication May 14, 2019, date of current version May 28, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2916834

Risk Minimization Routing Against Geographically Correlated Failures

AN XIE, XIAOLIANG WANG, AND SANGLU LU

State Key Laboratory for Novel Software Technology, Department of Computer Science and Technology, Nanjing University, Nanjing 210023, China

Corresponding author: Xiaoliang Wang (waxili@nju.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB1001801, in part by the National Natural Science Foundation of China under Grant 61832008, and in part by the Key Technology Research and Development Program of Jiangsu under Grant BE2018116.

ABSTRACT Regional failures, such as natural disaster or malicious attack, have become a major threat to the construction of future reliable communication network. The regional failures usually cause a large number of disconnected nodes simultaneously and influence the network for a long time. However, a routing scheme that is resilient to such geographically correlated failures is still unexplored. In this paper, we provide a comprehensive study of the disaster resilient routing dealing with the regional failure in operational IP backbone networks. It is notable that the path with minimal risk (i.e., minimal failure probability) is not necessarily the shortest path. The main challenge of finding such paths is that regional failure is unpredictable in terms of time, location, and the affected area. To this end, in combination with the computational geometry tool, we develop effective algorithms to find the minimal risk path between end node pairs to tolerate random regional failures. We show that in contrast to the conventional shortest path, a little longer path can be more effective to the disasters. After selecting such a path as the primary path, we turn to find a secondary backup path. In contrast to the conventional single link/node failure, a regional failure disrupts a large number of network components, simultaneously. As a result, how to find backup paths for re-establishment of the corrupted paths will raise a novel *fairness* issue. Specifically, during the backup path allocation, we focus on routing *fairness* to bound the worst-case user experience. A metric is proposed based on which an ILP is formulated. The extensive simulations validate that such an issue is non-negligible in face of regional failure scenarios.

INDEX TERMS Network reliability, network protection, network recovery, regional failure, routing.

I. INTRODUCTION

With the explosive growth of network-based applications, people increasingly rely on the large-scale networks to provide high reliability and high capacity communication services. However, it has been shown that the current communication networks are vulnerable to regional failures, such as natural disasters, malicious attacks, etc. Such large-scale regional failure may destroy numerous network components (e.g., links or nodes) within a specific area at the same time, and result in significant outage of network services for a long period. For example, Taiwan earthquake in Dec. 2006 affected six major cable systems including resilience paths, impacted around 300km × 150km area and slowed down the communication in Asia for months. Recently, the power outage caused by Hurricane Sandy in 2012 took several data centers and the corresponding cloud services offline [1], [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Haider Abbas.

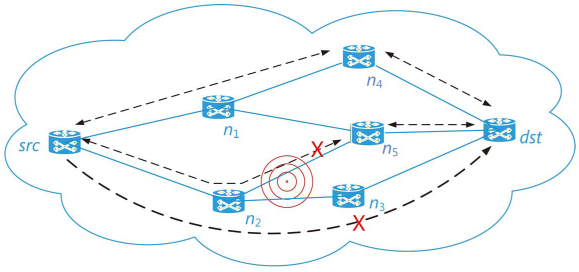


FIGURE 1. Geographically correlated failure may cause multiple links fail and disconnect a pair of primary and backup paths simultaneously.

Due to the frequent reports of communication network disruptions caused by natural disasters, research community has paid more attention on such widespread failure events [2]–[6]. Following the traditional cross layer design, the studies on disaster-resilient networks mainly adopted the concept of Shared Risk Link Group (SRLG) [6]–[11] or Disaster Zones (DZ) [12] to emulate large scale

network-component failure scenarios, inherently assuming that the characteristics of the possible failure scenarios are known in advance. However, with regard to the uncertain nature of disasters (or malicious attacks), we may face a serious scalability problem to enumerate all the failure scenarios since the regional failures can be anywhere, any shape and any size. An unexpected failure may destroy the current design, although a number of redundant resources have been provided. Therefore, it is crucial to design an appropriate methodology to cope with the unpredictable large-scale failures for the future highly survivable networks.

In this paper, we consider a different approach that targets at the fundamental routing schemes with respect to the uncertainty of geographically correlated failures in the operational networks. In order to mitigate the influence of such large-scale failures, we address the Risk Minimization Routing (RMR) problem which provides routing for end-to-end connections with the minimum failure probability under regional failures, and the Fair Backing up RMR (FBRMR) problem that offers approximately equal recovery overhead among nodes in the network. The contributions of this paper are as follows:

1) We develop an effective algorithm (Algorithm 1) to find the minimum risk path (RMR problem) to tolerate random regional failures. Routing under regional failures is difficult in general due to the uncertainty of regional failures and the geographical correlation of links. To solve this problem, we use the computational geometry tool: random sampling estimation. Extensive experiments validate that the shortest path is not necessarily the most robust path, especially when the geographical deployment of the network is dense.
2) After selecting the minimum risk path derived from RMR as the primary path, we turn to find a backup path with fairness (the FBRMR problem). The backup paths are selected so that they start to work once the primary path is disrupted. It is notable that the geographically correlated regional failure can disrupt a large number of network components simultaneously and lead to multiple disconnected end nodes. Such large number of disconnected end nodes requires a lot of reconnections. A simple strategy of minimizing the deployment cost (path length) or region-disjointness of backup paths will lead to an unfair situation in which some nodes may bear exceedingly more rerouting paths than others. How to backup primary paths such that each node bears an approximately equal rerouting paths in face of a regional failure remains yet unexplored. To overcome this issue, we provide a metric for the fairness after which an ILP is proposed to bound the worst case, i.e., the most unfair scenario.

The final aim of our work is to design a pre-disaster path-routing scheme which can tolerate a large set of geographically correlated failure scenarios and at the same time can react to regional failures guaranteeing a fair distribution of protection rerouting operations between the remaining nodes, once a disaster has occurred. Our work is helpful to achieve a better understanding of the impact of geographically correlated failures and contribute to the deployment of future ISP networks towards achieving higher survivability and fairer user experience.

The rest of this paper is organized as follows. Section II introduces the related work. Section III describes fundamental concepts and notations. Section IV addresses the problem of Risk Minimization Routing (RMR). Section V discusses the FBRMR problem. Experiments are provided in Section VI. Finally, Section VII concludes our paper.

II. RELATED WORK

Network survivability and its related routing, protection and restoration issues have been widely investigated (e.g., [13], [14]). These studies mainly focus on the single physical link failure scenario, assuming this is the main failure mode that interrupts network normal operation [15]. As the network scale is increasing and the network robustness requirement is becoming more stringent, recently researchers are paying attention to the multiple failure scenarios to provide better network survivability. The work in [16] explored the connectivity recovery mechanism in presence of cascading failures. The works in [17], [18] considered the *oblivious* routing issue to deal with multiple independent link failures. It is notable that these works mainly focus on the network logical connection while neglecting its geographical layout.

The cross layer designs of survivable IP/Optical network consider both logical layer and physical layer topologies [6]–[11]. They focus on how to embed the logical connection onto the physical optical network, such that the logical topology is still connected even when single physical link/node corrupt. To address this problem, the concept of shared risk link group (SRLG) was proposed by defining a group of logical links that are susceptible to a common physical resource failure (e.g., fiber, conduit) [7]. Researchers have studied the SRLG diverse routing problem to find SRLG-disjoint paths between a given pair of nodes, and the corresponding localization, protection and restoration issues with respect to a smaller number of predetermined failures [6], [8]–[11].

To address the disaster resilient routes, existing work usually targets few disasters that have the most impact on the network (the problem of network assessment [19]–[22]). With this network assessment, routes can be found to avoid these most vulnerable zones. Limitations can be applied to the routes, for example, [23] studies special rectangular physical routes, while [24] considers how to find two regional-disjoint paths. In general, the existing work on disaster resilient routing mainly considers failures with either determined sizes or locations.

III. PRELIMINARY

This section first presents the adopted network model and failure model. Then we introduce the concept of vulnerable zone of a path and the tool to measure it.

A. NETWORK MODEL

We consider a physical network $G(V, E)$ as a graph inside the deployment area $D \subset \mathbb{R}^2$. V is the set of nodes and E is the set of links. By e_{ij} we denote the link between adjacent nodes i and j, $i, j \in V$, $e_{ij} \in E$. Note that the geographical position of the nodes in the deployment area is fixed and known. For simplicity, we assume that each link e_{ij} is deployed on the straight segment ij on the plane D. Therefore, the length of the link is exactly the cartesian distance between i and j. We have $\{x_{st}^{ij} = 1 | e_{ij} \in E\}$ if the primary routing path x_{st} from source s to destination t traverses link e_{ij} and 0 otherwise. Then, a routing path from s to t can be expressed as follows,

[x_{st} is a routing path]

$$\sum_{j:e_{ij}\in E} x_{st}^{ij} - \sum_{j:e_{ji}\in E} x_{st}^{ji} = \begin{cases} 1 & i = s\,, \\ -1 & i = t\,, \forall i \in V \\ 0 & \text{o.w.} \end{cases} \tag{1}$$

B. FAILURE MODEL

During the extreme events such as disasters or malicious attacks, multiple network components located closely to each other will fail together. We summarize the behaviors of such large scale attacks to model geographically correlated failures.

Definition 1 (*Regional Failure*): is characterized by an epicenter $p \in D$ and a radius r. The regional failure is the circular area having center p and radius r. The following properties hold:

1) Network components (links and nodes) falling within the region of failure fail simultaneously and are removed from the network.
2) The radius r follows the distribution functions $f(r)$, $r_a \le r \le r_b$, where r_a (resp. r_b) is the minimum (resp. maximum) considered region size.
3) Each point of D has a given probability of being an epicenter (see later for a more precise definition).

Compared to the fairly well studied regional failure models, like the distance-based models [25], circular model and line model [4], [19], as well as the discrete function model [21], [26], our model does not make any assumption about the failure location and radius, which are usually difficult to obtain due to the uncertainty of the disaster failures. Our model is the generalization of the previous deterministic failure models [20], [25] (which require the knowledge of the failure radiuses) and SRLG related models [6]–[11] (which require the knowledge of the failure locations).

The distribution function $f(r)$ of the destructive natural regional failures, such as earthquakes, usually follows the power-law distribution [27], as illustrated in Fig. 2. The typical sizes of these failures can be found in [28] and can be used to determine $f(r)$. The probability of each point being an epicenter of some natural disasters can be defined by risk (hazard) maps [29].

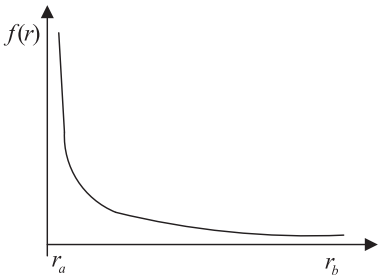


FIGURE 2. Distribution of region radius r.

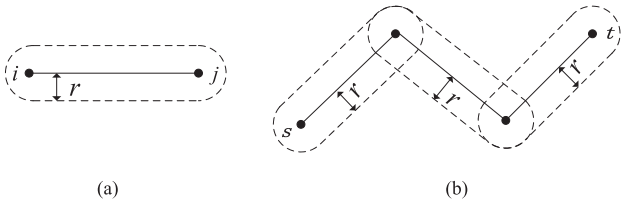


FIGURE 3. Vulnerable zone: The union of points that are located no more than r distance from the network components. Any regional failure occurs in the vulnerable zone will break the network component. (a) Vulnerable zone of link e_{ij}. (b) vulnerable zone of path x_{st}.

C. VULNERABLE ZONE OF A LINK AND OF A PATH

According to the definition of regional failures, a disaster region can be in any shape with arbitrary size and located anywhere in the plane. As a result, there are infinite number of regional failures to be considered. Our first problem is to find a proper statistical metric to evaluate the impact of regional failures.

Definition 2 (*Vulnerable Zone $Z_{e_{ij}}$ of a Link e_{ij}*): is a region sub-area around e_{ij} such that any regional failure with radius r whose epicenter falls within $Z_{e_{ij}}$ will always cause the corruption of the given link.

Given a regional failure with radius r, a link e_{ij} fails if it intersects with the failure region. Thus, if a disaster with radius r happens and its epicenter distance from e_{ij} is less than r, e_{ij} will be broken. Dually, we can say that a generic point $p \in D$ belongs to $Z_{e_{ij}}$ if: p is epicenter (denote such an event by P_{epi}), the disaster has radius r (denote such an event by F_r) and the distance $d_{pe_{ij}}$ between p and e_{ij} is less or equal to r. Thus the probability that p belongs to $Z_{e_{ij}}$ is:

$$\Pr\{p \in Z_{e_{ij}}\} = \Pr\{d_{pe_{ij}} \le r \cap P_{epi} \cap F_r\}.$$

In the general case, this probability is difficult to compute. By applying the conditional probability formula, we have:

$$\Pr\{p \in Z_{e_{ij}}\} = \Pr\{(d_{pe_{ij}} \le r \cap F_r) | P_{epi}\} \cdot \Pr\{P_{epi}\}.$$

Assume that p is the epicenter of disaster of radius r, we can greatly simplify the general problem:

$$\Pr\{p \in Z_{e_{ij}}\} = \Pr\{(d_{pe_{ij}} \le r \cap F_r) | P_{epi}^r\} \cdot \Pr\{P_{epi}^r\}.$$

By P_{epi}^r we denote the event that point p is the epicenter of disaster of radius r. Since p can be any point of the plane D,

the first term in the right member is actually deterministic, and thus:

$$\Pr\{p \in Z^r_{e_{ij}}\} = g(d_{pe_{ij}}) \cdot \Pr\{P^r_{epi}\}$$

where

$$g(e_{pe_{ij}}) = \begin{cases} 0 & \text{if } d_{pe_{ij}} > r \\ 1 & \text{if } d_{pe_{ij}} \leq r. \end{cases}$$

Thus, limited to a previous selection of r, we may redefine:

Definition 3 (*Vulnerable Zone $Z^r_{e_{ij}}$ of a Link e_{ij}*): is the region around e_{ij} which consists of all points whose shortest distance to link e_{ij} is less or equal to r (the "hippodrome" in dash line represented in Fig. 3 (a)).

Let $w^r(x, y)$ be the probability density function that a point $p(x, y) \in D$ is the epicenter of a disaster of radius r, then the failure probability of the link e_{ij} is:

$$\mathrm{P}^r_{e_{ij}} = \frac{\iint_{Z^r_{e_{ij}}} w^r(x, y)\mathrm{d}x\mathrm{d}y}{\iint_D w^r(x, y)\mathrm{d}x\mathrm{d}y}. \tag{2}$$

$w^r(x, y)$ can be defined by risk (hazard) maps [29]. This is a further generalization of our problem which can accommodate some unevenly distributed regional failures, for example, tsunamis, which only affects only the near sea network components. In the following of this paper, we will consider the special case of uniform distribution of disasters over the deployment region. In this case, Eq. (2) becomes $|Z^r_{e_{ij}}|/|D|$. where $\frac{|Z^r_{e_{ij}}|}{|D|}$ is the geometrical area of $Z^r_{e_{ij}}$ normalized to the area of deployment region.[1] All what's said before related to a link e_{ij} can be easily extended to a path x_{st}.

Definition 4 (*Vulnerable Zone $Z^r_{x_{st}}$ of a Path x_{st}*): is a region sub-area around x_{st} such that any regional failure with radius r whose epicenter falls within $Z^r_{x_{st}}$ will always cause the corruption of the given path.

The vulnerable zone of a path x_{st} includes the union of the vulnerable zones of links on the path, i.e., $Z^r_{x_{st}} = \cup_{e_{ij} \in x_{st}} Z^r_{e_{ij}}$, as shown in Fig. 3 (b), and thus it is all points whose shortest distance to x_{st} are less than r. We denote the path failure probability of x_{st} by $P^r_{x_{st}}$.

D. AREA ESTIMATION BY MONTE CARLO RANDOM SAMPLING

Our method is based on the integration of a scalar 2-D function area regions in a plane (as the calculation of areas when $w^r(x, y)$ is uniform). The shapes of such regions may be quite irregular. Therefore, we adopt the Monte Carlo random sampling technique to estimate the $|Z^r_{x_{st}}|$.

Concretely, we randomly and uniformly sample n points from the deployment area D and we count n', the number of points falling within $Z^r_{x_{st}}$. To do this, for each sampled point p and all the edges $e_{uv} \in x_{st}$, and test if the distance from p to at least one e_{uv} is less than r. If so, we increment n'. Then $|Z^r_{x_{st}}|$ can be estimated as $\frac{n'}{n}|D|$. If $w^r(x, y)$ is not uniform, then

$$|Z^r_{x_{st}}| \approx [\sum_{\forall p \text{ increments } n'} w^r(p) / \sum_{\forall p \text{ sampled}} w^r(p)]|D|.$$

The estimation accuracy is provided by the Estimator Theorem [30]. The theorem states that the number of Monte Carlo samples n needed to have the estimation relative error below ϵ with probability $(1 - \delta)$ must be:

$$n \geq \frac{4}{\epsilon^2 \rho} ln \frac{2}{\delta}, \quad \text{where } \rho = \frac{|Z^r_{x_{st}}|}{|D|}. \tag{3}$$

IV. RISK MINIMIZATION ROUTING UNDER REGIONAL FAILURE

This section first defines the RMR problem. We demonstrate the problem is dependent on the failure radius r. After some observations, we propose a local search algorithm.

A. RMR (RISK MINIMIZATION ROUTING) PROBLEM

The conventional shortest path problem is to find a path that minimizes the total length between two end nodes. By considering the failure probability of routing path, our goal is to find a path x_{st} with minimal failure probability (i.e., vulnerable zone) between two end nodes s, t.

Definition 5 (*Risk Minimization Routing Problem*): given a source-destination pair (s, t) on G, a failure radius r, the risk minimization routing problem RMR^r is to find a simple path from s to t with the minimal expected vulnerable zone, i.e., $|Z^r_{x_{st}}|$ is minimal among all paths from s to t.

When considering the risk of a routing path, the shortest path in terms of length may be different from the most robust path (minimal risk) with respect to regional failures. In Fig. 4(a), the lower path is shorter than the upper path, however the upper path is more robust to a regional failure since it has less vulnerable area than the lower path. It is notable that S. Neumayer et al. also figured out this phenomena at the last part of [16], [31]. However, they did not investigate further into this case and provide any solution to this problem.

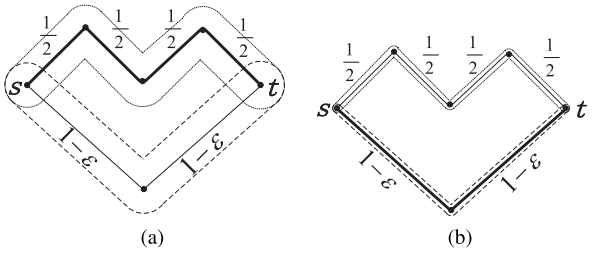


FIGURE 4. The most robust path is not necessarily the shortest path and is dependent on r. They are the upper path in Fig. 4(a) and the lower path in Fig. 4(b) respectively. (a) A big failure radius. (b) A small failure radius.

Another interesting property is that the most robust path is dependent on the failure radius r. For example, in Fig. 4(a) and Fig. 4(b), the shortest paths are always the lower paths, but the most robust paths are the upper path in Fig. 4(a) and the lower path in Fig. 4(b) respectively. Because the risk

[1] Considering this special case does not prevent the method from being generalizable to non-uniform distributions, as shown by Eq. (2)

zone is dependent on r, it's not easy to get the exact minimal expected vulnerable zone path.

A natural approach to solve *RMR* is to decompose the vulnerability zone of the path x_{st} into the vulnerability zones of its links:

$$Z^r_{x_{st}} = \cup_{e_{ij}\in x_{st}} Z^r_{e_{ij}}.$$

Unfortunately the computation of $|Z^r_{x_{st}}|$ from $|Z^r_{e_{ij}}|$ of the link components is not easy, because of the overlapping zones of the links. Let us consider a planar graph G and a simple path x_{st}. If we assume that overlappings of more than two link zones have negligible area, $|Z^r_{x_{st}}|$ can be expressed as $\sum_{e_{ij}\in x_{st}} |Z^r_{e_{ij}}| - \sum_{e_{ij}\in x_{st}} \sum_{\substack{e_{uv}\in x_{st} \\ e_{uv}\neq e_{ij}}} Z^r_{e_{ij}} \cap Z^r_{e_{uv}}|$.

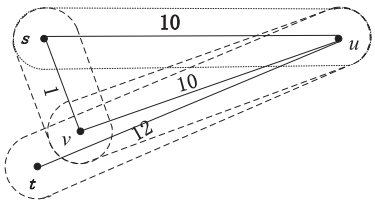


FIGURE 5. Sample network showing the properties of LSA (see the text).

One may wonder can we solve the problem of RMR by using the same idea of shortest path algorithms. We apply an example of Dijkstra to show that it is not able to find the optimum with respect to the regional failure. Let us consider the example in Fig. 5. The path x_{st} minimizing $P_{x_{st}}$ is $s \to v \to u \to t$ ($P_{x_{st}} = 13$, assuming that $|Z^r_{vu} \cap Z^r_{ut}| = 10$). Along $s \to v \to u \to t$, the distance of node u from s is $d_u = 11$. Thus: $d_u > d_s + |Z^r_{su}|$ violating the complementary slackness (CS) condition [32], therefore, for instance, Dijkstra does not guarantee optimality.

Lemma 1: When G is a planar graph (can be drawn on the plane in such a way that its edges intersect only at their endpoints) and the failure radius $r \to 0$, the most robust path is the shortest path between node s and t.

Proof: Denote the edge length of e_{ij} by L_{ij}. Then $|Z^r_{e_{ij}}| = 2L_{ij}r + \pi r^2$. Since the vulnerable zone of edges intersect only at their endpoint when $r \to 0$, $|Z^r_{x_{st}}|$ can be expressed as $\sum_{e_{ij}\in x_{st}} |Z^r_{e_{ij}}| - \sum_{e_{ij}\in x_{st}} \sum_{\substack{e_{uv}\in x_{st} \\ e_{uv}\neq e_{ij}}} Z^r_{e_{ij}} \cap Z^r_{e_{uv}}|$. We assume, the cubic and higher terms equal to zero. It's easy to see that the above expression can be reduced to a sum of linear terms and square terms of r. With $r \to 0$, the square terms become negligible compared to the linear terms. The linear terms dominate the expression indicating the most robust is the shortest path.

B. LSA (LOCAL SEARCH ALGORITHM) FOR RMR^R

As illustrated above, there is the need of defining a heuristic routing algorithm that operatively finds the minimal risk path at least in an approximate way. This motivates us to design an algorithm based on the Dijkstra's algorithm [33] to find the most robust path from s to all other nodes in the graph $G(V, E)$. The algorithm is shown in Algorithm 1. A labeling procedure is carried out at each iteration. These

Algorithm 1 Local Search Algorithm

Input: Graph $G = (V, E)$, source s, destination t and failure radius r
Output: The minimum vulnerable area, $|Z^r_{x_{st}}|$, and the path x_{st}

```
begin
    for i ← 1 to |V| do
        L(i) := ∞
        prev(i) := −1
    L(s) := 0 and S := ∅ ∪ {s}
    while t ∉ S do
        u := a node in V − S, who has the minimal L(u)
        among V − S, and is connected by a link to a
        node in S
        S := S ∪ {u}
        for all nodes v not in S do
            if e_uv exists and |Z^r_{x_su} ∪ Z^r_{e_uv}| < L(v) then
                L(v) := |Z^r_{x_su} ∪ Z^r_{e_uv}|
                prev(v) := u
    return L, and x_st constructed from prev
```

labels are the vulnerable area of the most robust path, i.e., the path with the minimum area of vulnerable zone. Similar to Dijkstra's algorithm, the algorithm proceeds through multiple iterations. Once a node is added to the labeled set, we update the label of each node not in this set so that its label is the area with the minimum vulnerable area. Let S denote this set. We begin with $S = \{s\}$. The set is formed from S by adding a vertex u not in S with the smallest label (line 7). The updates of the labels are in line 10-12. Note that $|Z^r_{x_{su}} \cup Z^r_{e_{uv}}|$ is performed by applying the Monte Carlo random sampling on the path $s \to u \to v$. The path $s \to u \to v$ is inferred from each nodes' predecessor. The procedure will end when the destination t is added to the labeled set, and its label is the vulnerable area of the most robust path from s to t. By $prev(i)$ we denote the predecessor node of i on the most robust path from source s to node i. By $L(i)$ we denote the label of node i. The algorithm is shown below.

Observation 1: In contrast to the conventional shortest path, the most robust path from s to t obtained by Algorithm 1 may be different from the one obtained from t to s. One example is shown in Fig. 5. First consider the most robust path from s to t. Algorithm 1 first labels v so that the most robust path from s to v is $s \to v$. Then u is labeled that the most robust path from s to u is $s \to u$. After that, t is labeled from u that the most robust path from s to t is $s \to u \to t$. However, when considering the most robust path from t to s, Algorithm 1 yields the output $t \to u \to v \to s$. This can be avoided by first running Algorithm 1 from s to t and then running it again from t to s. Choose the more robust path as the path from s to t.

The computational complexity of Algorithm 1 is bounded by $\mathcal{O}(|V| + |V|^2 + |E|^2)$, where n is the number of sampled

points as explained in Section III-D. Line 1 to 4 iterates on all the nodes, the complexity of which is $\mathcal{O}(|V|)$. The complexity of line 6 to 12 consists of two parts, i.e., accessing nodes and edges. Each node is accessed two times, one in the outer loop, the other in line 7 to get the minimal $L(u)$. The complexity is $\mathcal{O}(|V|^2)$. Each edge is accessed maximum $|E|^2$ times in line 10, the complexity of which is $\mathcal{O}(|E|^2)$. Note that when accessing an edge in line 10, $|Z^r_{x_{su}} \cup Z^r_{e_{uv}}|$ is achieved by iterating on n sampled points, and counting the number of which falls within $Z^r_{x_{su}} \cup Z^r_{e_{uv}}$ on the plane D. Since n is a constant, the total complexity of accessing edges is still $\mathcal{O}(|E|^2)$.

C. DISCUSSION FOR RMR$^{F(R)}$

We solved the RMR^r with a fixed failure radius r. Now we turn to solve the RMR problem on the continuous function $f(r)$, i.e., $RMR^{f(r)}$. There are two main obstacles. First, as mentioned in Section IV-A, the most robust path is dependent on the failure radius r. Thus the expression of the area of the vulnerable zone of a path is ambiguous. Second, even if the expression of a path is not ambiguous, the computation with respect to the continuous function $f(r)$ requires high complexity.

A possible approach can be to select a discrete set of values of r and route the connections solving RMR^r for each of the selected values. In this way, we obtain a set of possible routing paths for each connection among which to choose the actual paths. Criteria for this final selection, that goes beyond the scope of this paper, should take $f(r)$ into account. For the preplan of routes to minimize the risk of correlated failures that are hard to predict, please refer to [34].

If however, $f(r)$ is a function of the type represented in Fig. 2, we can route the connections using a single value of the radius r' that dominates or is typical [28]. The reason for choosing such a dominating r' is as follows. Considering the whole range of r is unnecessary, because failures with very big radius rarely happen (due to the long tail feature). Wasting valuable network resources for such very rarely happening events gives us very limited gain. Thus we only consider the left part of the distribution of r that dominates.

V. FAIR BACKING UP RMR PROBLEM UNDER REGIONAL FAILURE

In this section, we introduce the fair backing up RMR problem. In contrast to a single link or node failure, a regional failure will always break multiple primary paths. How to reroute these broken primary paths will raise a fairness issue which remains yet unexplored. We first define a metric to quantify the fairness. Then by considering the joint failure probability of the primary path and the backup path as a constraint, we propose an ILP to formulate this problem.

A. FAIR BACKING UP RMR PROBLEM

When finding a backup path y_{st} for the primary path x_{st}, the criterion is usually minimizing the deployment cost (path length) or minimizing the joint failure probability [24] to maximize survivability. After a regional failure, it's notable that the number of disconnected end nodes is large since the geographically-correlated failures generated will always break multiple primary paths. Thus it will lead to a large number of reconnections for the disconnected end nodes. How to properly protect the primary paths to avoid a situation where some nodes undertake exceedingly more reconnections (overloaded) than others is not considered in the previous literature. For the nodes that bear exceedingly more rerouting paths, it will have a bad influence to its own services, and lead to an obvious service degradation. We focus on how to allocate the backup paths so that the fairness degree is maximal in face of a regional failure.

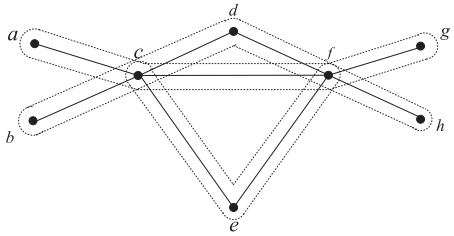


FIGURE 6. An example of the routing fairness under the region-disjoint constraint after a regional failure broke e_{cf}. Node d bears too much reroute paths which lead to the unfairness of d.

TABLE 1. Primary paths and backup paths.

End node pair	Primary path	Backup path
(a, g)	$a \to c \to f \to g$	$a \to c \to d \to f \to g$
(a, h)	$a \to c \to f \to h$	$a \to c \to d \to f \to h$
(b, g)	$b \to c \to f \to g$	$b \to c \to d \to f \to g$
(b, h)	$b \to c \to f \to h$	$b \to c \to d \to f \to h$

An example is shown in Fig. 6. The primary and backup paths are shown in Table. 1. The primary paths of end node pair (a, g), (a, h), (b, g) and (b, h) all pass through link e_{cf}. Assume that a regional failure breaks link e_{cf}. Since all the backup paths pass through $x_{c\to d\to f}$, node d is responsible for reestablishing the connections for the corrupted primary paths that pass through e_{cf}, which makes d to bear a very degraded service due to large number of rerouted paths. On the other hand, node e bears no obvious service degradation since $x_{c\to e\to f}$ is not chosen as any path's backup path. This scenario is not fair for node d compared to node e.

B. PARTIAL REGION-DISJOINT PATHS

Given a primary and backup path (x_{st}, y_{st}), they are totally region-disjoint if $Z^r_{x_{st}} \cap Z^r_{y_{st}} = \emptyset$. We first relax the requirement of region-disjointness to partial region-disjointness. Total region-disjointness may be not necessary and may lead to significantly longer path stretch (Fig. 7). Besides, when the failure radius is sufficiently large, there are no region-disjoint paths in the network. Other than region-disjoint paths [24], we bound the joint failure probability of x_{st} and y_{st} to θ, i.e., $|Z^r_{x_{st}} \cap Z^r_{y_{st}}| \leq \theta$ (we consider here only the special case when $w^r(x, y)$ is constant). This partial region-disjoint requirement expands the candidate set of backup path y_{st} and

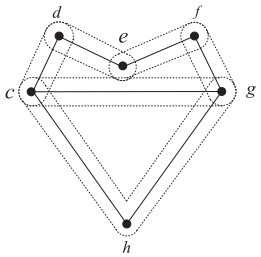


FIGURE 7. Node e only intersects little with link e_{cg}. The partial region-disjoint paths are $c \to d \to e \to f \to g$ and $c \to g$. The region-disjoint paths are $c \to h \to g$ and $c \to g$. The region-disjoint paths are significantly longer than the partial region-disjoint paths, while the difference in risk is very limited.

give us more flexibility. θ may be set according the service level agreement (SLA) between the network service provider and the customer.

C. ROUTING FAIRNESS

To measure the fairness of a protection routing after a regional failure, we first define a metric UD (Unfairness Degree) as follows,

Definition 6 (*Unfairness Degree*): given a network graph $G'(V', E')$ after a regional failure (with failure radius r), and a reconnection request matrix $\mathcal{RM}$ on G', the unfairness degree is the load difference between the most and the least loaded node in the network, where the load of a node is the number of primary and rerouted paths passing it, i.e.,

$$UD = |(P_u + R'_u) - (P_v + R'_v)|_{max}, \quad \forall u,\ v \in V'.$$

By P_u (P_v) we denote the number of primary paths that pass u (v). By R'_u (R'_v) we denote the number of the rerouted paths that pass u (v) based on $\mathcal{RM}$ after a regional failure. Here, we consider the primary resource and the protection resource separately on each router, and we assume that even if the primary path for a particular node pair is corrupted, the primary resource assigned to it cannot be used by other node pairs.

We define our FBRMR problem as follows,

Definition 7 (*Fair Backing up RMR Problem*): given a network graph $G(V, E)$, and the primary paths $x_{st}, \forall s, t \in V$, the fair backing up RMR problem is to find y_{st} for each x_{st} such that after an arbitrary regional failure (with failure radius r), the unfairness degree UD is minimal.

The main difficulty to solve this problem is that a regional failure can happen at anywhere with any size due to its intrinsic uncertainty. Thus exhaustively enumerating all the failure scenarios to trace all the elements in $\mathcal{RM}$ will lead to serious scalability problems. Instead we bound the worst case post failure scenario using the configuration we have before the failure happens. This is based on the following inequality,

$$UD \le (P_u + R'_u)_{max} \le (P_u + B_u)_{max}. \tag{4}$$

By B_u we denote the backup (i.e., protection) paths u undertakes before a regional failure. R'_u is always less than B_u. Thus we aim to minimize the maximal $(P_u + B_u)$ (the sum of primary and backup paths u undertakes before a regional failure) to bound the UD, i.e., in a min-max fairness fashion.

D. ILP FORMULATION OF FBRMR PROBLEM

We now present an ILP formulation of the FBRMR problem. We define the following 0-1 variables for all $e_{ij} \in E$ and for all $s, t \in V$:

$$x_{st}^{ij}(y_{st}^{ij}) = \begin{cases} 1 & \text{if } e_{ij} \text{ is on path } x_{st}\ (y_{st}) \\ 0 & \text{o.w.} \end{cases}$$

Once the RMR problem is solved, the variable x_{st}^{ij} of the primary path is determined. The FBRMR problem is formulated as follows,

$$\min \max_{1 \le i \le |V|} \sum_{\forall s,t \in V} \sum_{e_{ij} \in E} (y_{st}^{ij} + x_{st}^{ij}) \tag{ILP1}$$

$$\text{s.t. } y_{st} \textit{ is a routing path} \tag{1a}$$

$$\sum_{e_{uv} \in x_{st}} \sum_{e_{pq} \in y_{st}} |Z^r_{e_{uv}} \cap Z^r_{e_{pq}}| x_{st}^{uv} y_{st}^{pq} \le \theta, \quad \forall s,\ t \in V \tag{1b}$$

$$y_{st}^{ij} \in \{0, 1\}, \quad \forall e_{ij} \in E, \quad \forall s,\ t \in V \tag{1c}$$

Since $\sum_{e_{ij} \in E} y_{st}^{ij}$ corresponds to $B(i)$ and $\sum_{e_{ij} \in E} x_{st}^{ij}$ corresponds to $P(i)$, the objective function in Eq. (ILP1) minimizes the maximal $(P_i + R_i)$ on node $i (1 \le i \le |V|)$. The constraint in (1a) ensures that y_{st} is a routing path as defined in Section III-A. Constraint (1b) ensures the intersection vulnerable area of x_{st} and y_{st}, i.e., the joint failure probability of x_{st} and y_{st} is below the certain user risk tolerance threshold θ (as explained in Section V-B). Constraint (1c) ensures that all y_{st}^{ij} are 0-1 variables. Referring to the Principle of Inclusion-Exclusion, the considered intersection vulnerable area of path x_{st} and y_{st} can be expressed as follows,

$$\begin{aligned} |Z^r_{x_{st}} \cap Z^r_{y_{st}}| = & \sum_{e_{uv} \in x_{st}} \sum_{e_{pq} \in y_{st}} |Z^r_{e_{uv}} \cap Z^r_{e_{pq}}| \\ & - \sum_{e_{uv} \in x_{st}} \sum_{\substack{e_{pq} \in x_{st} \\ e_{pq} \ne e_{uv}}} \sum_{e_{mn} \in y_{st}} |Z^r_{e_{uv}} \cap Z^r_{e_{pq}} \cap Z^r_{e_{mn}}| \\ & - \sum_{e_{uv} \in y_{st}} \sum_{\substack{e_{pq} \in y_{st} \\ e_{pq} \ne e_{uv}}} \sum_{e_{mn} \in x_{st}} |Z^r_{e_{uv}} \cap Z^r_{e_{pq}} \cap Z^r_{e_{mn}}| + \cdots \end{aligned}$$

The above expression consists of the intersection vulnerable area of two edges, one from x_{st} and one from y_{st} minus the intersection vulnerable area of three edges, one from y_{st} and the other two from x_{st}, etc. The accurate expression of the intersection vulnerable area of x_{st} and y_{st} requires a lot of terms as shown in the above expression. We approximate it by reducing the high order terms to (1b). Under the condition that path x_{st} is given as the optimization input (x_{st}^{ij} is known), the formulation is an Integer Linear Programming (ILP) problem and can be solved using commercial solvers, such as IBM CPLEX [35].

We propose the ILP2 as the benchmark of ILP1. The input of ILP2 is also x_{st} (i.e., x_{st}^{ij} is known). The main concern is minimizing the path length (deployment cost) of the backup

path instead of routing fairness. The problem is formulated as follows,

$$\min \sum_{\forall s,t \in V} \sum_{e_{ij} \in E} c_{ij} y_{st}^{ij} \quad \text{(ILP2)}$$

$$\text{s.t. } y_{st} \textit{ is a routing path} \quad \text{(2a)}$$

$$\sum_{e_{uv} \in x_{st}} \sum_{e_{pq} \in y_{st}} |Z_{e_{uv}}^{r} \cap Z_{e_{pq}}^{r}| x_{st}^{uv} y_{st}^{pq} \leq \theta, \quad \forall s,\ t \in V \quad \text{(2b)}$$

$$y_{st}^{ij} \in \{0, 1\}, \quad \forall e_{ij} \in E, \quad \forall s,\ t \in V \quad \text{(2c)}$$

c_{ij} is the cost (length) of e_{ij}. The objective function in Eq. (ILP2) minimizes the cost (path length) of backup path y_{st}. Constraint (2a) ensures that y_{st} is a routing path. Constraint (2b) ensures that the joint failure probability of x_{st} and y_{st} is below the certain user risk tolerance threshold θ. This is similar to Constraint (1b). Constraint (2c) ensures that all y_{st}^{ij} are 0-1 variables. In Section VI, we evaluate the two ILPs by setting θ to the same value.

VI. NUMERICAL RESULTS

This section evaluates the proposed algorithms in Section IV and the fairness of routing introduced in Section V.

TABLE 2. Topology summary.

Name	Nodes	Edges	Avg. Degree
Rand50	50	137	5.48
Rand100	100	287	5.74
Janos-us	26	42	3.23
Germany backbone	50	88	3.52
Exodus (US)	91	180	3.95
Ebone (Europe)	111	234	4.22

A. EVALUATION SETUP

In order to collect reliable results, we use both realistic topologies from Rocketfuel dataset [36] and random topologies generated from the graph generator of LEMON [37]. The main parameters of the topologies are reported in Table. 2. The deployment area is 1200 x 1200 (arbitrary units) for all the cases. For the Monte Carlo estimation of a path's vulnerable area, we randomly sample $100k$ points in the deployment area. This number guarantees a worst-case error (on the minimum area to be measured) of about 20% with a statistical confidence $(1 - \delta) = 95\%$ (see Eq. (3)). One connection is requested by each node pair of the network.

Comparsion Metrics. We use the following metrics to quantify the results.

- *Vulnerable area*. As defined in Section III, the vulnerable area of a path corresponds to its failure probability in face of a regional failure.
- *Path stretch*. The detail definition can be found in [38]. Generally, a path with longer stretch requires more network resources.
- *Unfairness degree*. As defined in Section V-C, it quantifies the unfair degree of a routing after a regional failure.

For the vulnerable area and path stretch, we compare the results of the LSA algorithm to the shortest path algorithm, Dijkstra. For the routing fairness, we use CPLEX [35] to obtain the backup routes. All the results are averaged on all the node pairs in the network.

B. VULNERABLE AREA

We consider the failure radius from 10 to 200. We show the vulnerable area savings of the LSA compared to the shortest path algorithm, Dijkstra in Fig. 8.

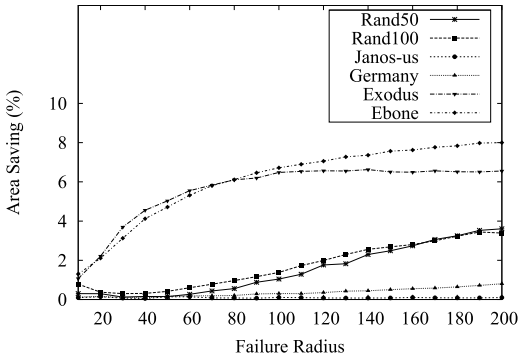


FIGURE 8. Vulnerable area savings.

The length of the conventional shortest path problem is only determined by its constituting edges' weights. Different from that, the vulnerable area of a path is determined by two factors, the constituting edges' vulnerable areas and their geographical layouts. Intuitively, in a denser graph, the most robust path is more likely to be different from the shortest path. For example, in Fig. 8, the vulnerable area saving is higher in Ebone than in Janos-us.

It's also notable that the decrease of vulnerable area compared to the shortest path tends to be stable, after the failure radius reaches a certain point (the turning points of the curves). Actually, the curve of the LSA cannot descend infinitely. Imaging an extreme case that the failure radius is larger than the length (width) of the deployment area D, then a single edge's vulnerable area is equal to the deployment area, $|D|$. Any path's vulnerable area is also equal to $|D|$. In this case, the vulnerable area saving will be zero. However, such a scenario in which a major failure disrupt all the components of the network rarely happens thus is omitted in the figures.

C. PATH STRETCH

Path stretch is adopted as the average path length ratio compared to the shortest path routing, Dijkstra. The path stretch is particularly important when the network resource or the deployment cost is very expensive. The shortest path is not necessarily the most robust path. So the length of the most robust path can be larger than that of the shortest path. We also consider the failure radius from 10 to 200. The increase in stretch is normalized based on the shortest path length of Dijkstra. Fig. 9 shows a similar trend that, with the failure region radius r increasing, the path stretches all tend to increase. This is because that, in general, the more robust path will be more ''zigzagged'', since edge zones are more

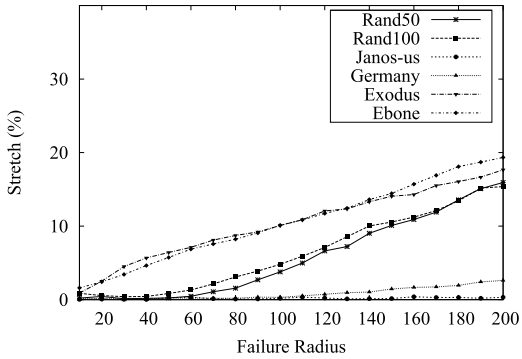


FIGURE 9. Path stretch.

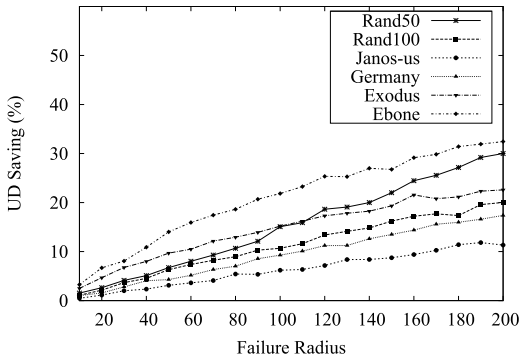


FIGURE 10. UD savings.

overlapped and the union of the vulnerable areas can be more likely to be reduced. When the failure radius grows, this trend tends to be more obvious, which leads to a longer path length. Even so, the path stretch obtained by LSA is not very large, around 20% even when the failure radius reaches 200.

D. ROUTING FAIRNESS

We first find the most robust primary paths with failure region radius setting to 50. Then we run ILP1 and ILP2 with the same user requirement θ (e.g., 0.05 for failure radius 50). To simulate the post regional failure states, for each failure radius r ranging from 10 to 200, we randomly generate failures, then measure the UDs and average them.

In Fig. 10, the UD savings of ILP1 compared to ILP2 are shown. Compared to the result of ILP2, the result of ILP1 has a reduction up to about 30%. The results show that, with the failure radius increasing, the gap between ILP1 and ILP2 increases. The UD saving in a dense graph is more significant than in a sparse graph. For example, the UD saving is more obvious in Ebone (with Avg. Degree 4.22) than in Janos-us (with Avg. Degree 3.23).

Not only the UD saving increases with the failure radius, but also the absolute value of UD increases as well. As shown in Fig. 11, both UDs of ILP1 and ILP2 increase with the failure radius in the Germany backbone (the results in other graphs are similar and thus omitted). This is because with the failure radius increasing, the number of failed primary paths increases as well, and it becomes more difficult to guarantee the routing fairness in face of a larger regional failure.

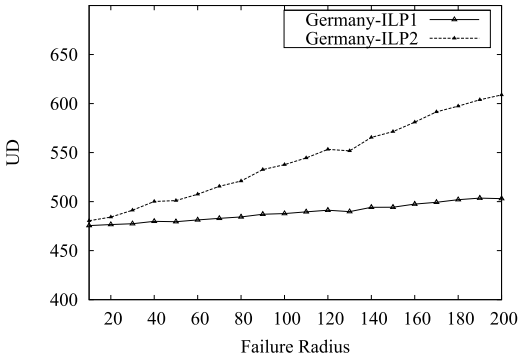


FIGURE 11. UD on the Germany backbone.

However, with the worst case scenario bounded by ILP1, the result in Fig. 11 shows that UD of ILP1 increases less significantly than ILP2.

VII. CONCLUSION

We first studied the Risk Minimization Routing (RMR) problem to mitigate the impact of geographically correlated failures on the end-to-end connection. Instead of using the assumptions that the failure scenarios are known in advance, we consider the routing problem with no assumption of the failure location and size. We develop effective heuristic algorithm to find the most robust path between a given node pair. To handle the variability of the failure distribution, we propose to solve it by considering the failure distribution property of regional failures, i.e., power law distribution. The simulation results show that with little higher path stretch, the path can be more robust.

For the network protection of finding backup paths, we mainly consider the fairness issue in face of a regional failure. We address the Fair Backing up RMR (FBRMR) problem and define a metric UD (Unfairness Degree). Then an ILP is proposed to formulate the problem. Instead of enumerating all the failure scenarios after a failure, we concentrate on the fairness before a disaster to bound the worst cases after a failure. Simulations show that current greedy-based protection can lead to a high UD after a regional failure.

This work mainly focuses on the pre-disaster routing protection issue to minimize the impact of potential regional failures. To realize future disaster-resilient networks, the cooperation work like after-disaster restoration is needed.

REFERENCES

[1] S. LaPerrière, "Taiwan earthquake fiber cuts: A service provider view," *NANOG39*, vol. 5, pp. 1–22, Feb. 2007.
[2] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," *Comput. Commun.*, vol. 36, no. 6, pp. 630–644, Mar. 2013.
[3] A. F. Hansen, A. Kvalbein, T. Čičić, and S. Gjessing, "Resilient routing layers for network disaster planning," in *Proc. IEEE ICN*, P. Lorenz, Ed. Springer-Verlag, Apr. 2005, pp. 1097–1105.
[4] S. Neumayer and E. Modiano, "Network reliability under random circular cuts," in *Proc. IEEE GLOBECOM*, Dec. 2011, pp. 1–6.
[5] M. F. Habib, M. Tornatore, M. D. Leenheer, F. Dikbiyik, and B. Mukherjee, "Design of disaster-resilient optical datacenter networks," *J. Lightw. Technol.*, vol. 30, no. 16, pp. 2563–2573, Aug. 15, 2012.

[6] 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.

[7] I. I. W. Group. (Nov. 2001). "Inference of shared risk link groups," *Internet Draft*, p. 17. [Online]. Available: http://tools.ietf.org/html/draft-many-inference-srlg-02

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

[9] P. Datta and A. K. Somani, "Diverse routing for shared risk resource groups (SRRG) failures in WDM optical networks," in *Proc. IEEE 1st Int. Conf. Broadband Netw.*, Oct. 2004, pp. 120–129.

[10] L. Shen, X. Yang, and B. Ramamurthy, "Shared risk link Group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 4, Aug. 2005, pp. 918–931.

[11] B. Wu, P.-H. Ho, J. Tapolcai, and P. Babarczi, "Optimal allocation of monitoring trails for fast SRLG failure localization in all-optical networks," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–5.

[12] N.-H. Bao, D.-Y. Luo, and J.-B. Chen, "Reliability threshold based service bandwidth recovery scheme for post-disaster telecom networks," *Opt. Fiber Technol.*, vol. 45, pp. 81–88, Nov. 2018.

[13] Q. She, X. Huang, and J. P. Jue, "Maximum survivability using two disjoint paths under multiple failures in mesh networks," in *Proc. IEEE GLOBECOM*, Nov./Dec. 2006, pp. 1–6.

[14] A. Tizghadam and A. Leon-Garcia, "On congestion in mission critical networks," in *Proc. IEEE INFOCOM Workshops*, Apr. 2008, pp. 1–6.

[15] D. Turner, K. Levchenko, A. C. Snoeren, and S. Savage, "California fault lines: Understanding the causes and impact of network failures," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 315–326, Aug. 2010.

[16] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. F. Hansen, "Fast recovery from dual link failures in IP networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 1368–1376.

[17] R. Zhang-Shen and N. McKeown, "Designing a fault-tolerant network using valiant load-balancing," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 2360–2368.

[18] M. Kodialam, T. V. Lakshman, J. B. Orlin, and S. Sengupta, "Resilient routing of variable traffic with performance guarantees," in *Proc. IEEE ICNP*, Oct. 2009, pp. 213–222.

[19] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the vulnerability of the fiber infrastructure to disasters," in *Proc. INFOCOM*, Apr. 2009, pp. 1566–1574.

[20] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the impact of geographically correlated network failures," in *Proc. IEEE MILCOM*, Nov. 2008, pp. 1–6.

[21] 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*, Jul. 2011, pp. 164–170.

[22] X. Wang, X. Jiang, A. Pattavina, and S. Lu, "Assessing physical network vulnerability under random line-segment failure model," in *Proc. IEEE HPSR*, Jul. 2012, pp. 121–126.

[23] W. Wu, B. Moran, J. H. Manton, and M. Zukerman, "Topology design of undersea cables considering survivability under major disasters," in *Proc. Int. Conf. Adv. Inf. Netw. Appl. Workshops*, May 2009, pp. 1154–1159.

[24] S. Trajanovski, F. A. Kuipers, P. Van Mieghem, A. Ilić, and J. Crowcroft, "Critical regions and region-disjoint paths in a network," in *Proc. IFIP Netw. Conf.*, May 2013, pp. 1–9.

[25] A. Sen, S. Murthy, and S. Banerjee, "Region-based connectivity—A new paradigm for design of fault-tolerant networks," in *Proc. Int. Conf. High Perform. Switching Routing*, Paris, France, Jun. 2009, pp. 1–7.

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

[27] Y. Y. Kagan, "Earthquake size distribution: Power-law with exponent $\beta \equiv 1/2$?" *Tectonophysics*, vol. 490, nos. 1–2, pp. 103–114, Jul. 2010.

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

[29] F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Minimizing the risk from disaster failures in optical backbone networks," *J. Lightw. Technol.*, vol. 32, no. 18, pp. 3175–3183, Sep. 15, 2014.

[30] R. Motwani and P. Raghavan, *Randomized Algorithms*. London, U.K.: Chapman & Hall, 2010.

[31] S. Neumayer and E. Modiano, "Network reliability under random circular cuts," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–6. [Online]. Available: http://www.mit.edu/ bastian/NRWRCC-Tech-Report.pdf

[32] D. P. Bertsekas, *Network Optimization: Continuous and Discrete Models*, vol. 28. Belmont, MA, USA: Athena Scientific, 1998, pp. 73–75.

[33] D. P. Bertsekas, *Network Optimization: Continuous and Discrete Models (Optimization, Computation, and Control)*. Belmont, MA, USA: Athena Scientific, 1998.

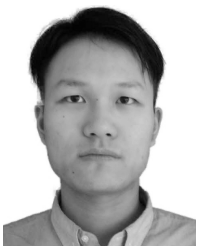
[34] A. Xie, X. Wang, W. Wang, and S. Lu, "Designing a disaster-resilient network with software defined networking," in *Proc. IEEE IWQoS*, May 2014, pp. 135–140.

[35] *ILOG CPLEX: Optimization Software*. Accessed: 2016. [Online]. Available: http://www.ilog.com/products/cplex/

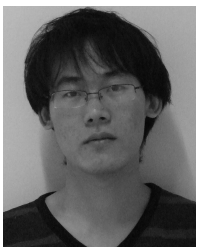
[36] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring ISP topologies with Rocketfuel," *IEEE/ACM Trans. Netw.*, vol. 12, no. 1, pp. 2–16, Feb. 2004.

[37] *Lemon: A C++ Library for Efficient Modeling and Optimization in Networks*. Accessed: 2016. [Online]. Available: http://lemon.cs.elte.hu

[38] X. Wang, X. Jiang, C.-T. Nguyen, X. Zhang, and S. Lu "Fast connection recovery against region failures with landmark-based source routing," in *Proc. 9th Int. Conf. Design Reliable Commun. Netw.*, Mar. 2013, pp. 11–19.



AN XIE received the B.S. degree from Shandong University, in 2012, and the M.S. degree from Nanjing University, in 2015, where he is currently pursuing the Ph.D. degree. He was a Visiting Student with the Hong Kong Polytechnic University, from 2017 to 2018. His research interests include network reliability and SDN/NFV.



XIAOLIANG WANG received the Ph.D. degree from the Graduate School of Information Sciences, Tohoku University, Japan. He was with Nanjing University, China, as an Associate Professor, from 2010 to 2014, where he is currently an Associate Professor with the Department of Computer Science and Technology. He has published over 30 technical papers at premium international journals and conferences, including IEEE TIT, IEEE TCOM, IEEE INFOCOM, USENIX ATC, and USENIX FAST. His research interests include optical switching networks, scheduling algorithm, and datacenter network systems.

SANGLU LU received the B.S., M.S., and Ph.D. degrees from Nanjing University, in 1992, 1995, and 1997, respectively, all in computer science, where she is currently a Professor with the Department of Computer Science and Technology and the State Key Laboratory for Novel Software Technology. Her research interests include distributed computing, wireless networks, and pervasive computing.