On the Vulnerability of Multi-level Communication Network under Catastrophic Events

Pankaz Das*, Mahshid Rahnamay-Naeini†, Nasir Ghani‡ , and Majeed M. Hayat*§
*Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131, USA
†Department of Computer Science, Texas Tech University, Lubbock, TX, USA
‡Department of Electrical Engineering, University of South Florida, Tampa, FL 33620,USA
§Center for High Technology Materials, University of New Mexico, Albuquerque, NM, USA
E-mail: pankazdas@unm.edu; mahshid.naeini@ttu.edu; nghani@usf.edu; hayat@unm.edu

***Abstract*—Various cyber-physical infrastructures such as communication networks and power grids are known to be vulnerable to large-scale stressors ranging from natural disasters to intentional attacks such as those effected by weapons of mass destruction and high-altitude electromagnetic pulses. The stresses instigated by these events can cause damage to critical components of the network infrastructure. In this paper, a general probabilistic model is developed for assessing the vulnerability of a communication network under various catastrophic events. A multi-level scalable network framework is proposed to capture the inter-dependencies across various communication networks in the infrastructure. For a given large-scale stressor, the initial-failure probability of each network component is formulated independently and then by taking into account the failure of the components that it depends upon. This enables the modeling of a shared failure among network components. Detailed simulations of a three-level network model are performed and key network-performance metrics are computed including the total network capacity, the maximum flow and the number of node failures. This work paves the way to model and evaluate the reliability of critical communication networks under massive stressor events.**

***Index Terms*—Network topology, multi-level network, geographically correlated failures, point process, network reliability.**

I. Introduction

The functional reliability of many networks largely depends on the geographical topologies of networks as well as on the locations and impact (geographical extent and severity) of stressors[1] [1]–[3]. For example, in the case of a communication network, various network components such as switches, amplifiers/repeaters, multiplexers and links (fibers, copper cables, antennas, etc.) can fail either directly from the stressor-events or indirectly as a result of damage to the components or systems that support the communication network, e.g., outage of power [4], [5]. Based on the geographical extent and severity of stresses, the functionality of various networks can be impaired at different scales. Clearly, the physical topology of the network and the nature of stressors should be taken into consideration together in the analysis of network reliability.

Modern communication networks are interdependent due to the service or support (both infrastructural and logical) they receive from one another. A *multi-level network* is composed of several interconnected and interdependent sub-networks of varying sizes ranging from small to medium to large, with varying security levels and capacities. Although almost all network infrastructures (military, commercial or private) can be represented by a single topological level concept, it would be precise to model it using the concept of a multi-level network. In this paper, a three-level communication-network architecture is presented that is scalable both in the number of levels as well as the size of the network in each level.

Initial damage from certain stressors, e.g., weapons of mass destruction (WMDs), high-altitude electromagnetic pulses (HEMPs) and natural disasters, may exhibit a high degree of spatial correlation. Similar to an earlier work [6], we assume a Strauss point process to model the correlated locations of multiple stressors that may occur simultaneously. Furthermore, while in [6] the authors only consider a fixed-form Gaussian degradation function, we generalize it to several degradation functions (e.g., linear, circular and Gaussian) to describe different types of stress influences. This function will also be selected probabilistically to capture uncertainty in the types of stressors. A degradation function defines the shape, range and intensity of a stressor over a geographical area.

Inherently, the components of a multi-level communication network possess different types of security and tolerance requirements based on their importance in the network. For instance, a military network or a fiber backbone network has extra security and more robustness to stressors than a commercial network due to the significance of these networks. While taking into account the importance of a network component, we devise a new formulation for calculating the failure probabilities of nodes and links in a network. Moreover, we propose an extended probabilistic shared risk link group (SRLG) formulation that considers inherent connections among network components to calculate their coupled-vulnerabilities to stressors. The advantage of our new SRLG approach is that it does not require any upper layer (e.g., IP layer) information and allows us to compute the failure probability of each component based on failure of components that it depends on. Finally, we provide analytical and simulation results to demonstrate the overall behavior of a realistic multi-level network under different types of correlated stressor events.

[1]By stressors we mean those events that impose physical stresses (intense electromagnetic field, heat, pressure, etc.) over a network and can trigger network component failures. As we are dealing with large-scale stresses in this paper, stressors and attacks/disasters will be used interchangeably.

II. Related Work

Most existing analyzes of network failures start from a given (fixed) network topology and then focus on various stressors [7], [8]. Moreover, many of prior studies on physical stressors were limited to single or geographically-isolated small-size attacks or disasters [9], [10]. The impact of large-scale stressors on networks was first introduced in [3]. Inherently, large-scale stressors lead to geographical-correlation amongst the failures of network components within the stressor's geographical proximity. Geographical correlations among large number of component failures is modeled in [3] based on the geographical proximity of network components from stressor centers. However, the authors only considered a single stressor event at a time, and failure of any network component within the range of stressor was assumed to be deterministic. However, multiple attack/disaster events can occur simultaneously and their effects on network-component failure are not deterministic. A probabilistic failure model with multiple circular stressor events has been proposed in [8]. However, the authors assigned a fixed failure-probability to all network components, which may not be realistic. Further, assumption of only circular-shaped stressors does not completely capture the impacts of various stressors on a network. A more realistic Gaussian shape function for modeling range and intensity of several stressors was used in [6]. In addition, the authors also used a Strauss point process [11] to characterize the geographical correlation among stressors.

There are other works on network failures where SRLG information was used to characterize the correlated link failures in a network [12]. Following a stressor event and by assuming that all components belong to an SRLG will fail with some (fixed) probability, a simple approach to model correlated failures in a network was proposed in [13]. Correlated failures in networks were also studied based on attacks in the logical layers [14], [15].

In contrast to all previous works, we propose a probabilistic model for various stressors with a generalized multi-level framework for the communication network topology. Furthermore, we devise a new formulation to compute the failure probabilities of all components in a communication network considering their coupled vulnerabilities.

III. Multi-level communication network framework

A multi-level communication network framework can be used to represent the physical architecture of many of today's special communication networks. For instance, military communication networks are supported by a wide range of commercial and non-commercial networks. A similar terminology named *multi-level network* is described in [16], where the term *multi-level* implies all five abstract layers of OSI (open system interconnection) model. The authors in [17] have introduced a framework termed *multi-provider network*. Akin to this effort, we have defined each level of our multi-level network as the physical infrastructure of different networks. We also emphasize the infrastructural dependency among

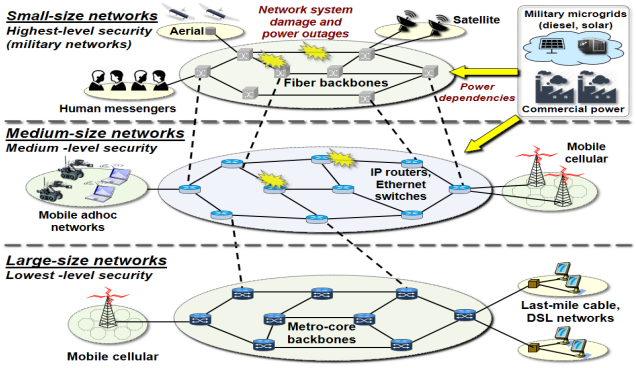

Fig. 1. A physical topology for a multi-level communication network.

different networks for efficient communication following a stressor event.

Figure 1 depicts a prototype of a multi-level communication network of the types described here for military communication. We categorize the physical infrastructure of an interdependent communication system into three scales: small, medium and large. The specifications of each scale are given in Table I. For instance, the small, medium and large networks can be military networks, wide area networks and commercial networks, respectively. In this paper, we do not consider failures in other infrastructures, such as the power grid, supplying electricity for the communication network, which is not true in reality.

TABLE I
Specifications of each level in a multi-level network

Parameter \ Network size	Small	Medium	Large
Number of nodes	~ 100	~ 1000	~ 10000
Bandwidth	low	high	high
Security	high	low	low

Mathematically, the multi-level network can be represented as a graph. Specifically, a finite undirected graph $G =< V, E >$ can be used to represent the multi-level communication network with $N = |V|$ nodes and $M = |E|$ links, where $|\cdot|$ denotes cardinality of a set. Here, $v_i \in V, i = 1, ..., N$, denotes the ith node, and $(v_i, v_j) \in E$ represents a link that connects nodes v_i and v_j, $i, j \in 1, 2, ..., N$.

IV. Probabilistic model for communication network-component failures

The goal of this section is to map the spatial distributions of various stressors to a probability distribution for the network components being functional while considering their coupled vulnerabilities.

A. Modeling correlated stressors

In general, multiple stressors can occur simultaneously either in one geographical location or they can spread over different locations depending upon the nature of stressors.

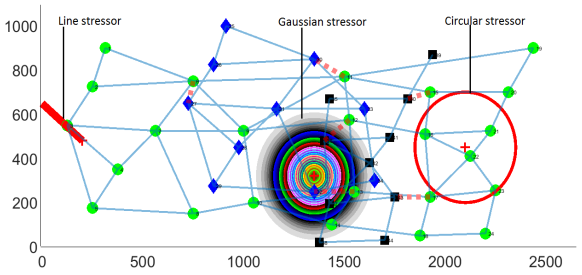

Fig. 2. Three types of stressors on a simulated multi-level communication network. Nodes with three colors represent physical nodes of three communication networks which are placed on a (2500 $\times$ 1000) plane.

Akin to the work done in [6], we have used the Strauss point process to represent spatially-inhomogeneous and spatially-correlated stressor centers. The Strauss point process enables us to model multiple stressor events simultaneously. The locations of these stressors are spatially correlated with each other on a geographic plane [11].

The spread and intensity of these stressors can be different depending upon the inherent shape and strength of stressors. For instance, a tornado yields different geographical impact than a nuclear attack or an earthquake. Based on literature survey, we have found three degradation functions, namely Gaussian [6], circular [18] and linear [7], that may reasonably characterize various real-world stressors. Figure 2 depicts one realization of these three types of degradation functions. A brief description of them is provided below.

Gaussian: Gaussian stressor intensity degrades according to the Gaussian function as the spatial distance from the location of occurrence increases. The variance of the Gaussian function specifies the range and intensity of the stressor on a geographic plane. Many real-world attacks and disasters exhibit a Gaussian nature approximately [6].

Circular: Given a stressor center, a circular degradation function is completely described by two parameters: radius of the circle and intensity of the stressor at the center. Intuitively, the only network component residing within the circle is affected and the intensity at any location is inversely proportional to its distance from the stressor-center.

Linear: We observed from the statistics of tornadoes that it can occur in any geographical location in USA. Typically, a tornado has a radius of 80 meters and length of 3 kilometers [19]. We consider the Poisson point process to model the locations of occurrence of the stressors. Unlike other disasters, a tornado has almost equal strength over the region it spreads. Hence, a uniform intensity all over the line is assumed.

B. Mapping stressor intensities to the network component failure distributions

We denote the stressor(s) event by $W = w$. We adopt the following assumption from [6]: **Assumption 1.** *Upon occurrence of a catastrophic stressor event (e.g., WMD, HEMP, natural disaster, etc.), the initial failure of any network component does not depend on other components.* Due to Assumption 1 and given a stressor event $W = w$, the joint failure probability of all network components can be written as the product of their individual failure probabilities. For nodes we have $p(v_1, v_2, ..., v_N|W = w) = \prod_{i=1}^{N} p(v_i|W = w)$ and for links we have $p((v_1, v_2), ..., (v_{N-1}, v_N)|W = w) = \prod_{(v_i,v_j)\in E} p((v_i, v_j)|W = w)$, where $p(v_i|W = w)$ and $p((v_i, v_j)|W = w)$, denote the failure probability of the ith node and the (v_i, v_j) link, respectively.

Next we find the failure probability of each network component using the following procedure. Clearly, the likelihood of network component failure increases with the intensity of stressor and decreases with component's internal tolerance. Hence, we define the failure probability of ith node as

$$p(v_i|W = w) = \min\left(\frac{I_w(x_i, y_i)}{I_{v_i}(r, c)}, 1\right), \tag{1}$$

where $I_w(x_i, y_i) \geq 0$ captures the aggregated intensity of stressor at node v_i's location (x_i, y_i), and $I_{v_i}(r, c) > 0$ is the internal node tolerance. We define $I_{v_i}(r, c)$ by taking into account two realistic physical attributes of a node: $I_{v_i}(r, c) := r + c$, where $r \in (0, r_{max}]$ is a parameter to capture the resistance (e.g., shielding against HEMP [4]) assigned to a node based on its importance (e.g., higher node-degree or a backbone node) in the network. In addition, $c \in (0, c_{max}]$ captures the security requirement of a node being a network component in the multi-level network. The values of r and c can be estimated from the historical data. Note that, $I_w(x_i, y_i)$ is non-negative due to the fact that stressor intensity can only be positive or zero. Intuitively, all network components possess some resistance to the physical stressors that indicate $I_{v_i}(r, c)$ is a positive quantity. Hence, we have $0 \leq p(v_i|W = w) \leq 1$, thus $p(v_i|W = w)$ is a probability.

In order to find the link failure probability, we first find the stressor intensities over all points on the link. Then we take the maximal stressor intensity to consider maximum impact of the stressor to that link. Since a link can have an infinite number of points, we have taken $L_{(v_i,v_j)}$ number of points on the (v_i, v_j) link to find the maximum stressor intensity. The link failure probability for the (v_i, v_j) link can be written as

$$p((v_i, v_j)|W = w) = \min\left(\frac{\max\limits_{l\in\{1,...,L_{(v_i,v_j)}\}} I_w(x_l, y_l)}{I_{(v_i,v_j)}(r, c)}, 1\right), \tag{2}$$

where (x_l, y_l) is the location of the lth point on (v_i, v_j) link. $I_{(v_i,v_j)}(r, c)$ is the tolerance of the (v_i, v_j) link that we define as the average of internal tolerances of the two nodes connected by the link: $I_{(v_i,v_j)}(r, c) := \frac{I_{v_i}(r,c)+I_{v_j}(r,c)}{2}$. The averaging of node tolerances in calculating the link tolerance is realistic. For example, if two nodes are very important then the link connecting them is assumed to have a great importance.

C. Characterizing coupled vulnerabilities among network components

We model the coupled vulnerabilities among network components using a variation of SRLG. First note that the functional vulnerability of a node directly affects the functionality

of all links connected to it. Clearly, if a node fails then the links attached to it cannot be used anymore for communication. Therefore, for a stressor event $W = w$, by taking into account the coupled vulnerabilities between nodes and links, we find the failure probability of (v_i, v_j) link as

$$\begin{aligned} &p_{srlg}((v_i,v_j)|W=w) = \mathbf{P}((v_i,v_j) \cup v_i \cup v_j | W=w) \\ &= p((v_i,v_j)) + p(v_i) + p(v_j) - p((v_i,v_j))p(v_i) - \\ &p(v_i)p(v_j) - p((v_i,v_j))p(v_j) + p((v_i,v_j))p(v_i)p(v_j), \end{aligned} \tag{3}$$

where the last line follows from Assumption 1. For simplicity of notation, conditioning on the stressor event $W = w$ is removed from the second line. We summarize the link-failure as **Observation 1:** *The increase in failure probability of a communication node increases the failure probability of all links attached to it.* Similarly, link failures can cause node failures as well. For example, a HEMP wave that hampers a link can be carried through the link to the nodes connected to it. We can express the failure probability of the ith node considering all associated link failures as

$$\begin{aligned} &p_{srlg}(v_i|W=w) = \mathbf{P}(v_i \cup (\bigcap_{j\in\mathbb{N}}(v_i,v_j))|W=w) \\ &= p(v_i) + p(\bigcap_{j\in\mathbb{N}}(v_i,v_j)) - p(v_i)p(\bigcap_{j\in\mathbb{N}}(v_i,v_j)), \end{aligned} \tag{4}$$

where $\{j \in \mathbb{N} : v_j \in \text{Neighbor}(v_i)\}$ is the index set of the neighbors of node v_i. Again, conditioning on a stressor event $W = w$ is dropped from the notation. We now have **Observation 2:** *The increase in failure probability of all links attached to a node elevates the failure probability of that node.*

V. Performance Measures

In this section, we define several parameters to evaluate the performance of network under different stressor scenarios.

Definition 1. Total expected capacity (TEC) of network: This metric measures the accumulated average (expected) capacity of all network links. Total capacity of a communication network: $C = \sum_{(v_i,v_j)\in E} C_{ij}$, where C_{ij} is the capacity of the (v_i, v_j) link. C_{ij} is a random variable that we define as

$$C_{ij} = \begin{cases} c_{ij}, & \text{with probablity } p(c_{ij}) = 1 - p((v_i,v_j)|W=w), \\ 0, & \text{with probablity } p(0) = p((v_i,v_j)|W=w), \end{cases}$$

where c_{ij} is the true capacity of the (v_i, v_j) link. We find the TEC of a network by taking conditional expectation ($\mathbf{E}[\cdot|\cdot]$) over C given a stressor $W = w$:

$$TEC = \mathbf{E}[C|W=w] = \sum_{(v_i,v_j)\in E} c_{ij}\left(1 - p((v_i,v_j)|W=w)\right).$$

Definition 2. Total expected number of node failures: Since the number of functional-nodes is an important parameter for any network, we calculate the total expected number of node failures among N nodes after the occurrence of a stressor event. We define a random variable that captures the functionality of the ith node as follows

$$X_i = \begin{cases} 1, & \text{if the } i\text{th node fails with probablity } p(v_i|W=w) \\ 0, & \text{if the } i\text{th node is functional.} \end{cases}$$

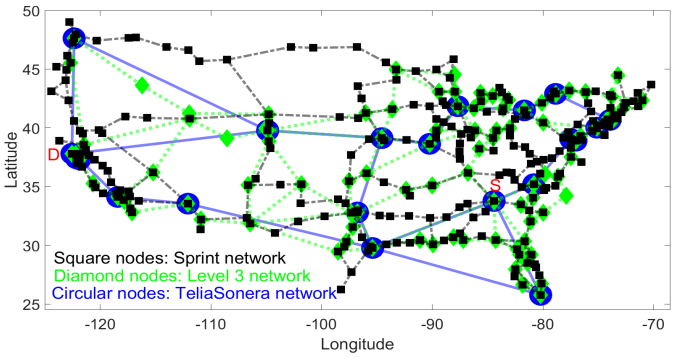

Fig. 3. A physical topology of a multi-level communication network composed of three real networks: TeliaSonera, Level 3 and Sprint.

The total number of node failures can be expressed as $X_T = \sum_{i=1}^{N} X_i$. Then the total expected number of failed nodes is $\mathbf{E}[X_T|W=w] = \sum_{i=1}^{N} p(v_i|W=w)$.

Definition 3. Max-flow between two nodes [3]: This parameter allows us to find the maximum data rate possible between any two fixed nodes in a network.

VI. Simulation Results

Figure 3 depicts a prototype of the physical infrastructure of a multi-level communication network, which is composed of three real networks: TeliaSonera, Level 3 and Sprint. The physical topology dataset of these three networks are available in [20]. Note that each of TeliaSonera, Level 3 and Sprint networks consists of 21, 99 and 264 nodes, respectively, which are located all over USA. Three connections from both Level 3 and Sprint network are made with the TeliaSonera network based on the geographical distance between nodes and their associated node degrees. We have evaluated the performance of the multi-level communication network under different types of stressor scenarios. For each scenario we have generated 500 random samples with 2 stressor events. All links have a capacity of 1 Gbps (Gigabits per second) and intermediate point distance on links is approximately 10 miles. Node tolerances are assigned uniformly in (0, 2]. Moreover, the radius of the circular stressor is assumed to be 200 miles. For a line stressor, the line-direction is considered to be a free parameter within 0-360 degrees, since the line stressor can move to any direction after its occurrence.

Figures 4 and 5 depict the total expected number of node failures and the TEC of the multi-level network, respectively, for three different types of stressors. As expected, the TEC decreases and the total expected number of node failures increases with the increase of the parameter value of stressor. Depending on the stressor, the horizontal axis (*parameter of the stressor*) refers to the variance of the Gaussian stressor or the intensity at the center for circular stressor or the length of line for linear stressor. Notice that the network performance becomes worse for all scenarios while we consider the effect of SRLG among the network components. This is because one component failure contributes to the increase of failure probability of other components (Observations 1 and 2). For

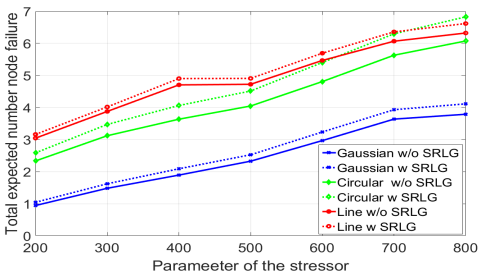

Fig. 4. Total expected number of failed nodes in the network under different types of stressors with (w) and without (w/o) SRLG effects.

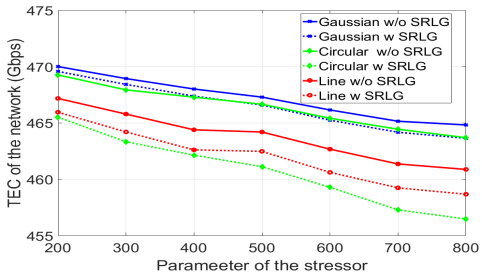

Fig. 5. TEC of the network under various stressors with and without SRLG.

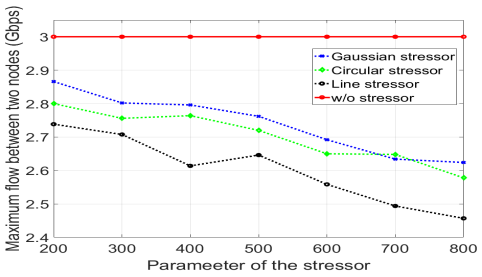

Fig. 6. Maximum flow between two fixed nodes with SRLG.

the particular parameter values assumed in simulation, the multi-level communication network is less vulnerable under Gaussian stressor; however, different parameter values may yield different results, which is intuitive.

Figure 6 illustrates the Max-flow between two arbitrary fixed nodes (denoted by S and D in Figure 3) in the network following a stressor. Here we have directly calculated the Max-flow considering the SRLG. Clearly, Max-flow achievable between these two nodes under normal operation is 3 Gbps, but due to the impact of stressors some nodes/links fail, thus the actual Max-flow between these two nodes is reduced.

VII. Conclusions and Future Work

The reliability of a network is largely affected by the catastrophic attacks and natural disasters. We have presented a multi-level communication architecture to capture the physical infrastructure of the existing communication networks. We have described different types of correlated stressors that can potentially degrade the reliability of a communication network. We have also calculated the coupled-vulnerabilities among network components using a realistic SRLG formulation. Simulation results have shown that the inherent coupling among communication-network components notably increases their vulnerabilities to the large-scale stressors.

In the future, the dynamics of network functionality needs to be studied under temporal correlation among different types of stressors and robust techniques need to be devised to minimize the impact of catastrophic stressors on the network.

Acknowledgment

This work was supported by the Defense Threat Reduction Agencys Basic Research Program under grant No. HDTRA1-13-1-0020.

References

[1] E. K. Çetinkaya *et al.*, "Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach," *Telecommunication Systems*, vol. 52, no. 2, pp. 751–766, 2013.

[2] H. Haddadi *et al.*, "Network topologies: inference, modeling, and generation," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 48–69, 2008.

[3] S. Neumayer *et al.*, "Assessing the vulnerability of the fiber infrastructure to disasters," *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1610–1623, 2011.

[4] C. Wilson, "High altitude electromagnetic pulse (hemp) and high power microwave (hpm) devices: Threat assessments," DTIC Document, Tech. Rep., 2008.

[5] J. Borland, "Analyzing the internet collapse," *ABC News*, 2008.

[6] M. Rahnamay-Naeini *et al.*, "Modeling stochastic correlated failures and their effects on network reliability," in *Proceedings of Int. Conference on Computer Communications and Networks*. IEEE, 2011, pp. 1–6.

[7] S. Neumayer and E. Modiano, "Network reliability with geographically correlated failures," in *Proceedings INFOCOM*. IEEE, 2010, pp. 1–9.

[8] P. K. Agarwal *et al.*, "Network vulnerability to single, multiple, and probabilistic physical attacks," in *Proceedings MILCOM*. IEEE, 2010, pp. 1824–1829.

[9] A. Narula-Tam, E. Modiano, and A. Brzezinski, "Physical topology design for survivable routing of logical rings in wdm-based networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 8, pp. 1525–1538, 2004.

[10] E. Modiano and A. Narula-Tam, "Survivable lightpath routing: a new approach to the design of wdm-based networks," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, pp. 800–809, 2002.

[11] D. J. Strauss, "A model for clustering," *Biometrika*, vol. 62, no. 2, pp. 467–475, 1975.

[12] D. Papadimitriou *et al.*, "Inference of shared risk link groups," *IETF Draft, OIF Contribution, OIF*, vol. 66, p. 2001, 2001.

[13] H.-W. Lee, E. Modiano, and K. Lee, "Diverse routing in networks with probabilistic failures," *IEEE/ACM Transactions on networking*, vol. 18, no. 6, pp. 1895–1907, 2010.

[14] Z. Kong and E. M. Yeh, "Resilience to degree-dependent and cascading node failures in random geometric networks," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5533–5546, 2010.

[15] D. Magoni, "Tearing down the internet," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 6, pp. 949–960, 2003.

[16] J. P. Sterbenz *et al.*, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[17] E. K. Cetinkaya *et al.*, "Multilevel resilience analysis of transportation and communication networks," *Telecommunication Systems*, vol. 60, no. 4, pp. 515–537, 2015.

[18] S. Neumayer and E. Modiano, "Network reliability under random circular cuts," in *IEEE Global Telecommunications Conference*. IEEE, 2011, pp. 1–6.

[19] "Tornado: National oceanic and atmospheric administration: Storm prediction center and wikipedia," http://www.spc.noaa.gov/, accessed: 2016-06-12.

[20] J. P. Sterbenz *et al.*, "Ku-topview network topology tool," http://www.ittc.ku.edu/resilinets/maps/, The University of Kansas, 2010.