photonics

MDPI

Review

Disaster-Resilient Optical Network Survivability: A Comprehensive Survey

Muhammad Waqar Ashraf [1,2], Sevia M. Idrus [1,*], Farabi Iqbal [1], Rizwan Aslam Butt [3] and Muhammad Faheem [4]

1 Department of Electrical Engineering, Universiti Teknologi Malaysia, Johor 81300, Malaysia; wamuhammad4@live.utm.my (M.W.A.); alfarabi@utm.my (F.I.)
2 Department of Computer Engineering, Bahauddin Zakariya University, Multan 60650, Pakistan
3 Department of Telecom Engineering, NED University of Engineering & Technology, Karachi 75270, Pakistan; rizwan.aslam@neduet.edu.pk
4 Department of Computer Engineering, Abdullah Gul University, Kayseri 38080, Turkey; muhammad.faheem@agu.edu.tr
* Correspondence: sevia@fke.utm.my

Received: 30 July 2018; Accepted: 7 September 2018; Published: 12 October 2018

Abstract: Network survivability endeavors to ensure the uninterrupted provisioning of services by the network operators in case of a disaster event. Studies and news reports show that network failures caused by physical attacks and natural disasters have significant impacts on the optical networks. Such network failures may lead to a section of a network to cease to function, resulting in non-availability of services and may increase the congestion within the rest of the network. Therefore, fault tolerant and disaster-resilient optical networks have grasped the attention of the research community and have been a critical concern in network studies during the last decade. Several studies on protection and restoration techniques have been conducted to address the network component failures. This study reviews related previous research studies to critically discuss the issues regarding protection, restoration, cascading failures, disaster-based failures, and congestion-aware routing. We have also focused on the problem of simultaneous cascading failures (which may disturb the data traffic within a layer or disrupt the services at upper layers) along with their mitigating techniques, and disaster-aware network survivability. Since traffic floods and network congestion are pertinent problems, they have therefore been discussed in a separate section. In the end, we have highlighted some open issues in the disaster-resilient network survivability for research challenges and discussed them along with their possible solutions.

Keywords: network survivability; protection; restoration; disaster-aware routing; congestion-aware routing; optical networks

1. Introduction

Optical networks provide high-capacity fiber links for the Information Communication Technology (ICT) access networks and carrying about 99% of the global internet traffic [1]. The level of bandwidth demand is rising continuously thus requires more high capacity optical links [2], which is not an economically viable option. To meet these challenges, the Dense Wavelength Division Multiplexing (DWDM) technology is gaining importance and uses multiple wavelengths in the same optical fiber link to provide multiple virtual channels. Each channel may have a capacity of 100 Gigabits per second or higher, and collectively offer a data rate of Terabits per second over these channels [3]. Network traffic moves through the optical light paths, constituted by high-capacity fiber links, which are established between two network nodes on arriving connection requests. To ensure continuous provisioning of services, survivability of network nodes and fiber links is of prime vitality [4,5].

Network failures could be the result of misconfiguration, hardware failure, ill maintenance, power failures, and/or natural disasters, as shown in Figure 1. In a network, fiber cables are laid down in bundles swathed by a duct where each cable may carry hundreds of fiber strands. Construction or destructive natural events including earthquakes, landslides or ship anchors causes fiber cuts. All the light paths that traverse through failed fiber (fiber cut) will be disrupted and lead to massive data loss. A catastrophic event such as fires or floods can fail the central offices where OXCs are located. This is referred to as node failure which is rare but can impose severe disruptions. Similarly, channels engaged by light paths over optical links can fail due to the failure of transmitter/receiver operating on that channel and are handled either by prompt switching to another idle channel or by treating it as a link failure in absence of an idle channel [6]. Figure 1 also describes the nature of disaster-based failures which can disrupt the function of single or multiple links and/or nodes.

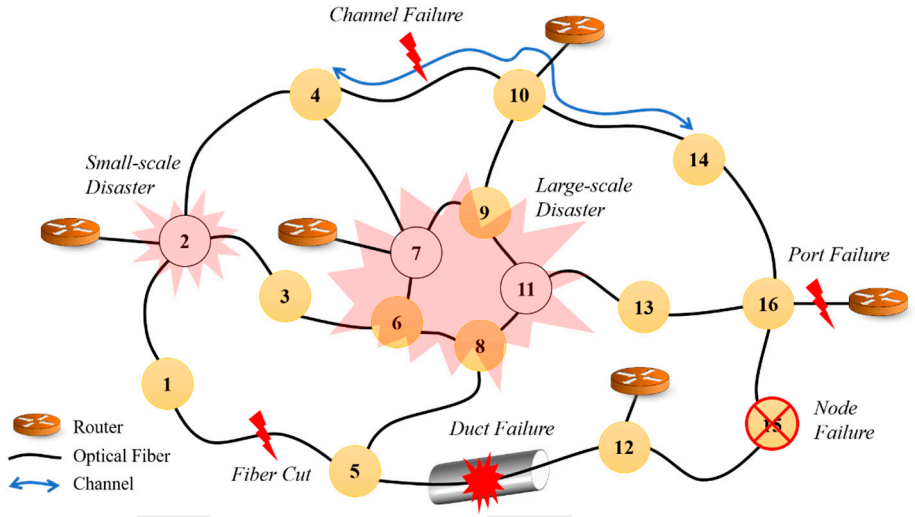


Figure 1. Types of Network Failures.

Disasters can be categorized as natural disasters (e.g., hurricanes & tropical storms, tornadoes, earthquakes, landslides, avalanches, tsunamis, floods, wildfires, animal bites, etc.) and man-made or technological disasters (power service disruption & blackouts, human negligence or errors, anchor drag/drops, EMP attacks, nuclear explosion, sabotage, anti-corporate attacks, cyber-attacks, terrorist attacks, or vandalism). Disaster based failures can have devastating impacts on an optical network by making its services unavailable [7]. For example, the worst disaster in Japanese history was on 11 March 2011, consisting of Great East Japan earthquake of magnitude-9, along with the subsequent tsunami and nuclear accident that destroyed 1500 telecom buildings by the main shock and 700 telecom buildings experienced power outages [8–10]. The Nepal earthquake, in 2015, affected the Rural ICT infrastructure and services by collapsing of the houses, schools, ICT access centers, BTS, transmission towers, fiber backhaul, and microwave links [11,12]. An earthquake of magnitude 7.1 struck central Mexico on 19 September 2017, caused 355 fatalities, 6100 injuries, and collapsed nearly 44,000 buildings, including telecom infrastructure [13]. Some network interruptions appear to be intentional attacks, the motivations of which are hard to observe. A later occurrence including three men associated with scuba diving down to cut off the undersea optical fiber at the bank of Egypt happened in March 2013 [14]. Many specialists feel that deliberate damage of submarine cables is unrealistic or impossible, however undersea-cable bottlenecks have the potential for serious interruptions is causing network providers to search for alternate paths to connect the continents.

Figure 2 provides an overview of disaster-based failure survivability mechanisms in optical networks. Disaster-based failures could cause multi-domain multi-layer failures that span several network domains. Disaster modeling is utilized to assess the risks involved and their corresponding physical and financial impacts. Disasters can be modeled as deterministic or probabilistic, i.e.,

whether the outcomes are precisely determined or undetermined due to the room for random variation. A large-scale disaster could cease to function multiple nodes and links which turn into multi-layer failures that can be modeled as a multilayer network. Following Reference [15–19] presents interesting work on disaster modeling, however, it is out of the scope of this paper. To combat disaster-based failures, intelligent network provisioning schemes are utilized to restore services with a higher priority, known as connection recovery and network recovery. Generally, approaches for connection recovery falls into proactive prevention and reactive compensation considering two factors: Routing and capacity assignment. Protection of connections can be done either by provisioning of backups proactively or by re-provisioning connections reactively after failure (path-based restoration). Protecting a connection over multiple disjoint paths has the advantage of better fault tolerance [20]. Congestion Control Service Provisioning (a basic reactive procedure) has an emphasis on capacity re-arrangement for re-provisioning of disrupted connections. As this method adapts to dynamic network events, it can handle concurrent, cascading failures. Through reactive compensation, limited network resources can re-allocate (re-provision) multiple times for the most effective usage.

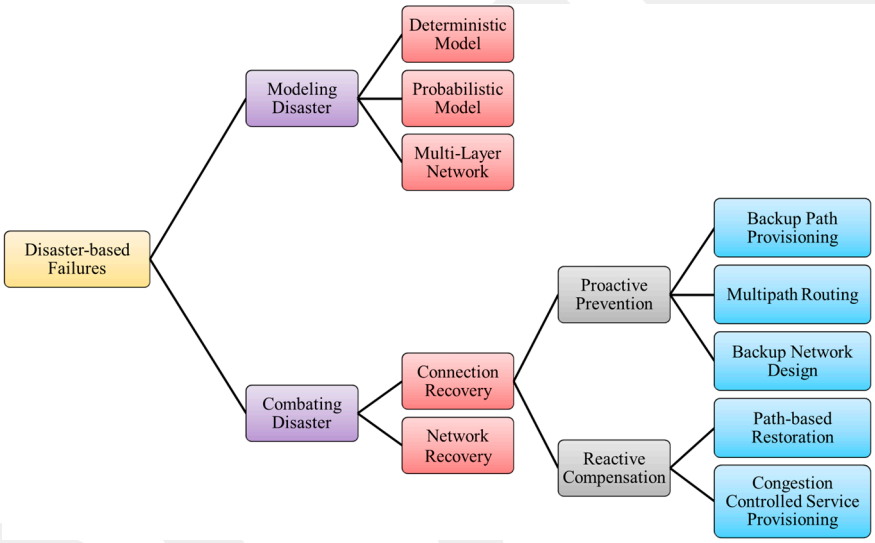


Figure 2. Overview of Disaster-based Failure Survivability Mechanisms [17].

Multiple network components may fail simultaneously due to wide-spread geographical impacts of disasters. The focus of the research community has emerged to large-scale correlated failures with several aspects. For example, Habib et al. in Reference [17] elaborated the classification of research work on disaster survivability as well as disaster impacts on optical networks using their characteristics. They also discussed several ways to combat them. Whereas References [7,21,22] reviewed the work on Resilient Communication services protecting end-user applications from Disaster-based failures (RECODIS). A review on network resiliency against weather-based disruptions and their impacts is provided in References [23,24]. In References [22,25,26], deployment of emergency networks in the event of a large-scale disaster is addressed for post-disaster recovery. This paper is intended to present a survey of fault tolerance and management through protection and restoration, correlated cascading failures, network survivability, and congestion-aware routing in disaster scenarios. It also reviewed the recent techniques and trends adopted for network survivability. A brief review of solutions for survivability techniques regarding fault management, cascading failures, and disaster-aware survivability is presented in Sections 2–4. Section 5 elaborates on some work on congestion-aware routing and spectrum assignment. Open challenges and research directions are given in Sections 6 and 7 concludes this study.

2. Protection and Restoration

Several survivability mechanisms for Wavelength Division Multiplexing (WDM) based optical networks have been studied in References [27–31]. Several recovery techniques for mesh and ring based optical networks are summarized in Reference [27] and Reference [32]. Even a modular suite of algorithms was presented for managing the normal and protection paths in Reference [33]. Protection and restoration [34–36] are implemented either as link-based or path-based to minimize service disruptions at reasonable costs. In the protection scheme, spare capacity is reserved and kept idle until a failure occurs. The use of network capacity is thus not efficient, but recovery speed is guaranteed. However, it has been observed in Reference [37] that the aggregated impact of failures is reduced up to 40% only in backup network design, i.e., protection is not entirely effective. On the other hand, restoration refers to the arrangements where the blocked traffic is rerouted via a dynamically discovered route when some node or link fails. Resources used for recovery do not preserve, but accommodate the available unused capacity of the network. It is more capacity-efficient than a protection scheme but may require a longer recovery time and overhead. The combination of protection and restoration can also be used (known as a hybrid scheme) to take advantage of both schemes [38]. In the hybrid scheme, recovery solution is pre-designed but resources are allocated in real-time. Faults of fiber links and Optical Cross-Connects (OXCs) could cause the channel failure, thus losing a huge amount of data. Ramamurthy et al. [39] studied the distributed protocols for both path restoration and link restoration to examine the protection switching and restoration times. Ramamurthy et al. evaluated the adjustment between capacity utilization and vulnerability to multiple link failures. Protection schemes for different types of networks like SONET-SDH, Multi-Protocol Label Switching (MPLS), Internet Protocol (IP), etc. are proposed in Reference [40]. If a protection scheme is employed in a capacity efficient manner, it will provide much quicker recovery from failure, as proposed by Mohan et al. in Reference [38]. However, path protection results in lower capacity because each path is protected by a dedicated backup path [29,41]. Dedicated protection delivers more reliability in terms of service continuity, QoS, and connection ASR, but cannot provide efficient resource utilization [42]. To mitigate this problem, shared backup path protection technique can be applied in WDM optical networks, however, dedicated protection will take less recovery time, as compared to shared protection [29,43,44].

It is also suggested by Ou et al. [45] to protect the primary path by protecting its vulnerable segments (sub-paths) separately. Sub-path protection delivers faster recovery and higher scalability as compared to path protection at the cost of resource utilization. Link protection can be achieved using link-disjoint backup paths for each link established according to requested connections [46–48]. From the preliminary work, it is observed that most of the studies focused on a single node or single link failure at the given instant. Single-link failures are most likely the cause of dual-link failures and are more tractable than multiple failures. Kim et al., in their technical report [49], studied the impact of two link failures considering of a multi-failure model for different protection schemes and proposed a restoration method for damaged and congested shared path. Kim et al. also computed the capacity cost and survivability for their approach in evaluating the tradeoff. Choi et al. [46] addressed the dual-link failure recovery using a failure model in which two links may fail arbitrarily. With proposed algorithms, Choi et al. suggested that 100% recovery was achieved from double-link failures by increasing backup capacity unassertively. Sivakumar et al. in Reference [50] proposed a combination of protection and restoration techniques for simultaneous dual-link failure to re-establish the connection with the minimum available unused capacity. Lu Ruan et al. proposed a combination of protection and restoration techniques for optical networks considering two link failure [51], such that the second link failure occurs within the recovery span of the first failed link. Primary and backup paths are established using shorter and longer path lengths, respectively. Protection component of the hybrid technique reserves the backup capacity such that affected demands can restore using a pre-planned backup path, and restoration component dynamically finds another path to restore the rest of the affected demands. There have been many p-cycle based techniques proposed to protect the single link failure, however, Feng et al. introduced a p-cycle based Integer Linear Programming (ILP)

model in Reference [52] to mitigate the two link failure recovery problem using static load. Feng et al. also proposed two other algorithms, namely Shortest Path Pair Protection (SPPP) and Short Full Path Protection (SFPP), for dynamic traffic and examined their performance for different traffic loads and capacity. Through simulation results, it is revealed that SFPP is more efficient than SPPP in terms of their capacity for incremental traffic, but has lower blocking probability at high traffic.

In the restoration scheme [28,29,43,53–55], backup paths are provisioned according to update link-state information of nodes and links when a failure arises. It provides higher resource utilization as compared to protection, however, recovery time is more than that of protection as this technique finds the backup path dynamically after failure occurrence. Restoration can be classified as (i) link-restoration; (ii) path-restoration; and (iii) segment-based restoration [28]. Among these restoration schemes, link restoration takes less time for fault recovery whereas path restoration takes the maximum time. Provisioning network connections with the most survivable paths (via appropriate protection and restoration schemes) increases the reliability of network connections, which is crucial to various important network services (banking, big data transfers, etc.).

Yadav et al. [56] proposed a HCA to achieve the efficient restoration in WDM optical networks. The algorithm theme is based on the modified resource allocation to reserve a wavelength, in advance, during the establishment of a connection for a backup light path, but the model is designed to deal with single link failure only. The proactive restoration method is also proposed by Rani et al. in Reference [57] that improves the network resource utilization and reduces the blocking probability. Chen et al. proposed the Dynamic Load Balancing Shared Path Protection (DLBSPP) algorithm in Reference [58], which employed a traffic-aware restoration mechanism to compute link-disjoint backup paths that carry multi-link failure traffic. Jara et al. [59] studied the simultaneous k link-failures on dynamic WDM optical network by proposing a routing and wavelength dimensioning approach named Fault Tolerance Method Based on Cheapest Paths (FTBCP). To avoid longer recovery times, the FTBCP computes the primary and alternate routes off-line, with maximum traffic load, and then these computed routes are assigned, on request, to reduce blocking probability with failures $k \geq 1$.

3. Disaster-Based Correlated Cascading Failures

Disaster-based failures can be correlated or cascading, and sometimes trigger the failures horizontally or vertically within the network [7]. For example, the optical layer in WDM networks provides services to the upper layers (e.g., ATM, SONET-SDH, MPLS, IP) and lacks the restoration of optical layer that may vertically disrupt the services of the upper layers. Today's smart networks are managed through software designs. The complexity level of these software designs is increasing over time. Software bugs could lead to unstable network states. For example, in 2012, a routine update of load balancing software on a Gmail server caused a partial loss of 40% of services for 18 min [60] because this update contained faulty logic. A single node was fully updated to recover this cascading error instead of partially updating all failed nodes at a time. The problem of cascading a disaster was persuasively considered after the event of the Tohoku earthquake in 2011. This problem can be viewed as a chain-sequence of interconnected failures or associated with a cause-and-effect relationship that is a vital feature of most catastrophic events. Pescaroli et al. defined and separated the cascading disasters and cascading effects by reviewing the literature in Reference [61] while considering the dynamics of disasters. Pescaroli et al. analyzed the critical elements responsible to cascade failures and concluded that cascading can be limited in the event of a disaster if vulnerability, critical infrastructure, interdependencies, amplification, and secondary disasters of the network are considered during risk reduction practices.

The nature of disaster failures is much more dynamic and wide-spread than the failures discussed in Section 2. These failures may span in the form of multiple correlated cascading failures either horizontally (within a layer) or vertically (layer to layer), as depicted in Figure 3a [62]. Light paths (shown as a two-sided arrow) in the optical layer are responsible for connecting nodes and data centers of the upper layer, so disaster failures can propagate to upper layers due to functional dependencies.

Erjongmanee et al. [63] address some external factors and their impacts on the telecommunication networks and correlated the natural disaster with the large-scale failures. The existing capacity of the network and bandwidth demand can change pre, trans, or post-disaster events. The possible degradation in a post-disaster network offered bandwidth due to cascading failures, as is illustrated by Figure 3b. It can also be observed that requested bandwidth upsurged in a post-disaster scenario because people intend to use social media, live video streams, and TV news, etc. to get more and more information about the incident, which consequently contributes requested bandwidth in post-disaster and recovery scenarios.

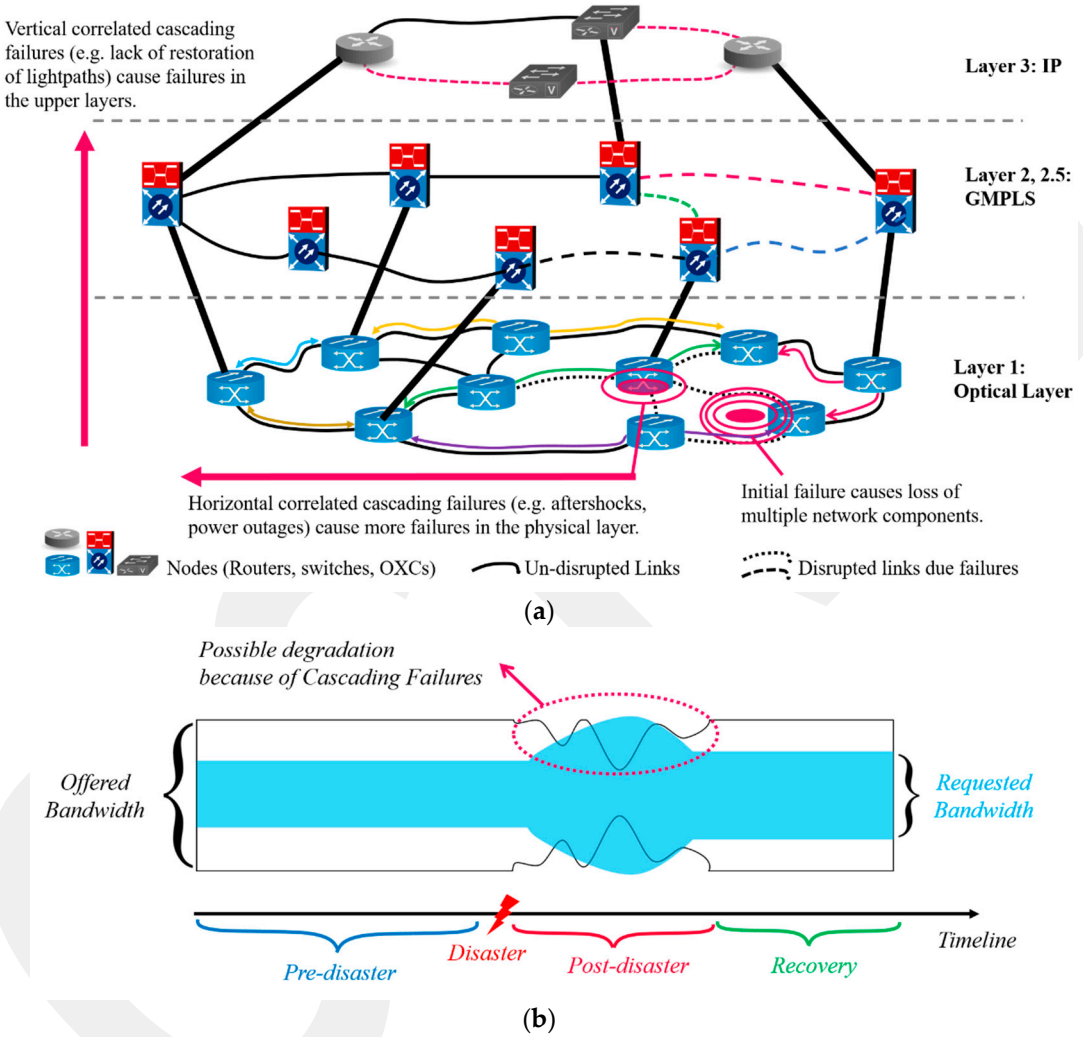


Figure 3. Effects of Correlated Cascading Failures. (**a**) Horizontal and Vertical Correlated Cascading Failures; and (**b**) Pre-Disaster and Post-Disaster Typical Requested and Offered Bandwidths.

Optical backbone networks tend to exhibit complex behavior due to their increasing scale and interconnected components at different layers. Thereby, these networks become more susceptible to local failures, later on, turn into cascading failures. Sometimes we exaggerate the problem more instead of alleviating it in response to our actions taken to mitigate these failures and upsurge other parts of the network. Savla et al. [64] proposed a model for cascading failures that includes network states as flows and the activation of link status. Under the proposed circumstances, an overload condition or disaster disruption can irreversibly inactivate a link. Coupling links can be inactive successively due to cascading failure that may or may not be adjacent. Routing policies can access the network state. An algorithm designed to assess the upper bound on the margin of resilience for directed acyclic

graphs. This algorithm propelled a directing strategy that provably coordinates with the upper bound for a network.

Most of the studies addressed the catastrophic consequences and critical conditions of correlated cascading disruptions. It is essential to have the knowledge of propagation of failures in time and space and the velocity at which failures propagate. Typically, cascading failures propagate with constant velocity from the center of the initial failure. In Reference [65], Zhao et al. studied the propagation behavior of cascading failures on spatially embedded networks, and proposed a theoretical framework to predict propagation velocity. The cross-layer reliability of optical networks has also become an issue of great interest. For example, IP-over-WDM networks comprise the upper IP-logical layer and the lower WDM-physical layer. Link establishment at logical layer correspondingly maps on the path connecting the source-destination pair in the physical layer, such that the logical connection remains established even when physical link fails. Zhou et al. [66] formulated an MILP to assist survivable routing constrained by at least one of the four cross-layer metrics: (1) Newly added logical links to be minimized, (2) maximization of capacity, or (3) connectivity of logical topology after physical link failure, or (4) minimum cross-layer cut to be maximized. Similarly, an ILP formulation is presented in Reference [67] for the joint multi-layer survivability problem. Zhou et al. proposed a proactive restoration scheme for IP-over-EON (Elastic Optical Network) to solve the problem of single optical link failure and/or IP node failure. Dikbiyik et al. [68] proposed a three-fold solution to prevent and recover the connections from disaster failures considering a probabilistic risk model. A metric penalty based on SLA introduced to analyze the disaster-risk-aware provisioning through an ILP formulation. Through reactive traffic engineering solution, disrupted connections and connections under risk of correlated cascading failures are re-provisioned. Disaster impacts and their cascading failures are estimated for specific events of earthquakes, hurricanes, etc. that are occurring in geo-collocated regions.

Attacking the physical layer can cause serious service degradation, loss of data, and revenue. Several physical layer attack methods and optical layer security breaches have been documented in Reference [69–74]. Commonly, link-disjoint primary and backup paths have been proposed in the conventional survivability techniques for construction level failures (misconfiguration, hardware failure, ill maintenance, power failures etc.) that do not consider such scenarios. Furdek et al. [75] introduced a dedicated path protection scheme considering the concept of attack group that helps to established attack-aware disjoint primary and backup paths. Routing and wavelength assignment were handled by a 2-step ILP formulation. Weapon of Mass Destruction (WMD) attacks can also lead to multiple correlated cascading failures. Mukherjee, in his technical report [76], analyzed the existing approaches and developed several novel techniques for the protection of telecom networks and other critical infrastructures against WMD attacks. The primary focus of this report was to prepare the network by considering the risks of WMD attacks in different parts of the infrastructure and recover from them. The techniques applied to mitigate the impacts of the manifold and cascading disruptions were persuaded by large-scale attacks. Mukherjee explored the conceivable target zones in the network, risk-aware routing to decline network failure in case of a WMD assault, multi-path provisioning to give partial protection when there is not sufficient capacity after a WMD-assault, the nature of cascading failures initiated by a WMD attack, and techniques to provide protection in the upper network layers. Additionally, proposed the protection schemes for WMD survivability in cloud networks.

4. Disaster-Aware Network Survivability

Increase in disaster threats as indicated by Reference [77,78] and the rising risks of disasters around the world demand the design of disaster-resilient network against disaster risk constraints [79]. Disaster risk constraints may be reflected as service disruptions caused by natural disasters or intentional attacks. Tools for network planning and management [80] and network optimization [81] are required to mitigate the impact of disaster based failures, and more generally of spatially correlated failures in optical networks. A Geographic Information System (GIS) based fiber tool provides risk-aware new fiber network planning and the seamless management of intact infrastructures [82]. During the

past couple of years, the research community has studied, with diverse perspectives, to address the network disaster vulnerabilities, as discussed below.

Deployed protection schemes cannot cope with disaster-based failures. The risk profile of the network helps to identify all possible network vulnerabilities and determines the networks capability to survive geographically correlated failures. Natural disasters or physical attacks can disrupt multiple network components to function instantaneously as those have a geographic regional impact. The region of a failure can be of a circular geometry of a radius r centered at point O in the network layout. Network elements enclosed within this region can malfunction, as illustrated in Figure 4. Wang in Reference [83] proposed two algorithms: (1) Failure recovery after region failure and (2) network augmentation in the case of a single region failure for providing continuous service against geographically correlated regional failures. He proposed a greedy approximation based on the approximation ratio.

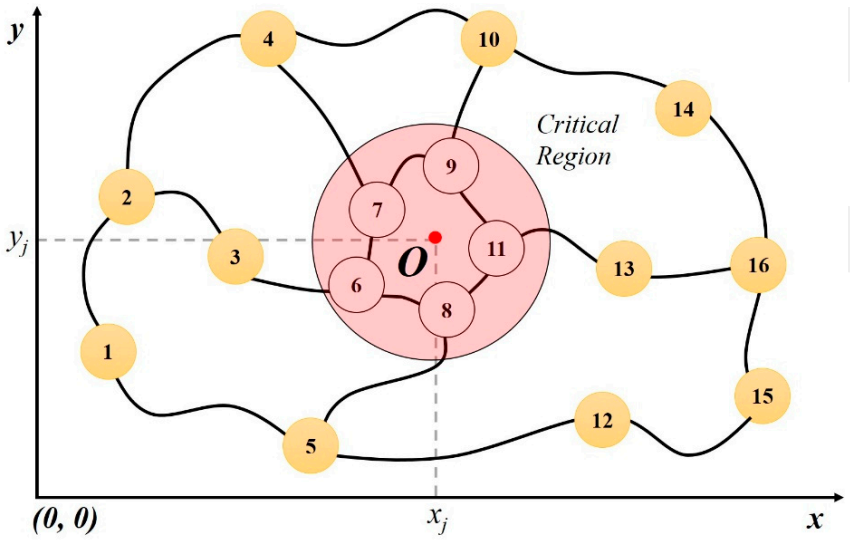


Figure 4. Critical region failures embedded in xy-plane.

Several parameters have been showing up in the literature to enumerate the effects of these failures. For instance, weighted spectrum formulated in Reference [84] as $WS(G,N) = \sum_i (1-\lambda_i)^N$ based on the Eigenvalues of the normalized Laplacian of a graph. Long et al. [85] used this parameter to assess the network survivability in the event of geographically correlated failures. Additionally, they solve an optimization problem to determine the most vulnerable geographic nodes and cuts, and conduct a comparative analysis using other common survivability measures with weighted spectrum.

Cheng et al. [86] considered the regionally correlated failures and attacks to be a threat to optical network communication and proposed a model to identify the critical region. The model described its effectiveness in finding most vulnerable regions at fiber-level network using both weighted and unweighted topologies. The obtained results are used to enhance the performance of routing using GeoDivRP. As networks are installed geographically, having areas posed by different disasters, it leads to complications in protecting the network. Iqbal et al. [87] proposed a model to identify affected areas for several disasters with different shapes and sizes characterized by temporal distribution. They also introduced two metrics: (1) Region Betweenness-Centrality to represent the region importance in terms of all-nodes pairs shortest paths passing through that region and (2) Risk Impact to enumerate the threat posed by disasters within a region and analyzed the effect of link existence and disaster area size on these metrics.

Network geography describes the impact of failure events on a network's services and capacity. Gardner et al. [88] explained the geographic vulnerabilities as a geographic region that is based on the radius of effected proximity such that when nodes and their incident links fail, then the network will

become disconnected. Geographic region depending on the radius of threat will reduce the search space. Similarly, Trajanovski et al. [89] formulated a polynomial-time algorithm to decline the impact of regional failures on the region-aware network. Trajanovski et al. proved the problem of provisioning region-disjoint paths as non-deterministic polynomial time problem (i.e., NP-hard) and proposed a heuristic as a solution to this problem. Geometric probability can also be used for the geography of disasters. Saito et al. [90] proposed a geometric model based on the geometric probability for a physical network affected by a disaster. Performance metrics such as connection maintainability and network design rule are evaluated to make the network robust against disasters. Saito in Reference [91] has also analyzed the network survivability against earthquake by introducing spatial network design rules, whereas Tran and Saito [92] extended the work in Reference [91] by proposing an algorithm that determines the new additional links to enhance the network robustness against earthquakes.

Disasters tend to display spatiotemporal characteristics and consequently links availability change instantly. If the spatiotemporal impact of the disaster (such as the path of a hurricane see Figure 5) can be predicted, then preventative measures can be taken to mitigate the disaster impacts on the network. Iqbal et al. [93] presented the spatiotemporal network resilience based on a grid-based risk profile depicted in Figure 6. Where each grid rectangle g contains an availability value representing the probability that g is free from failure for a particular time interval. The availability of a link computed as the product of the availability values of all grid rectangles it crosses. The availability of a path is the product of the availability values of its links. The most risk-averse path obtained via the shortest path algorithm, using as weights the –log of the link availabilities.

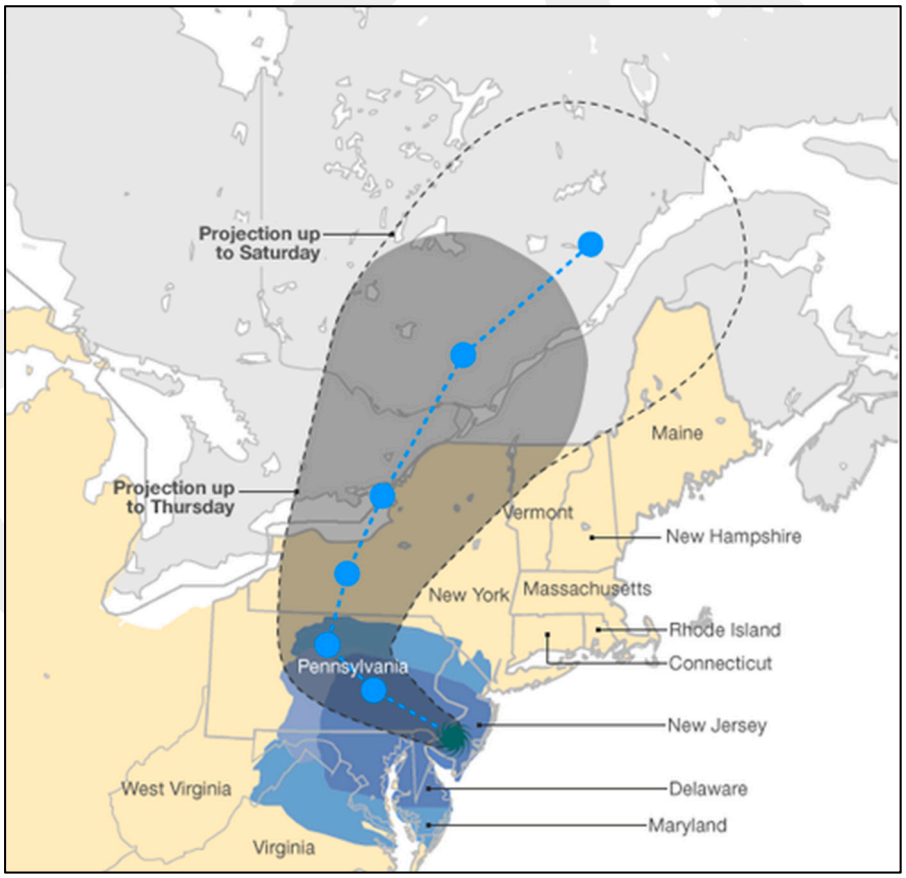
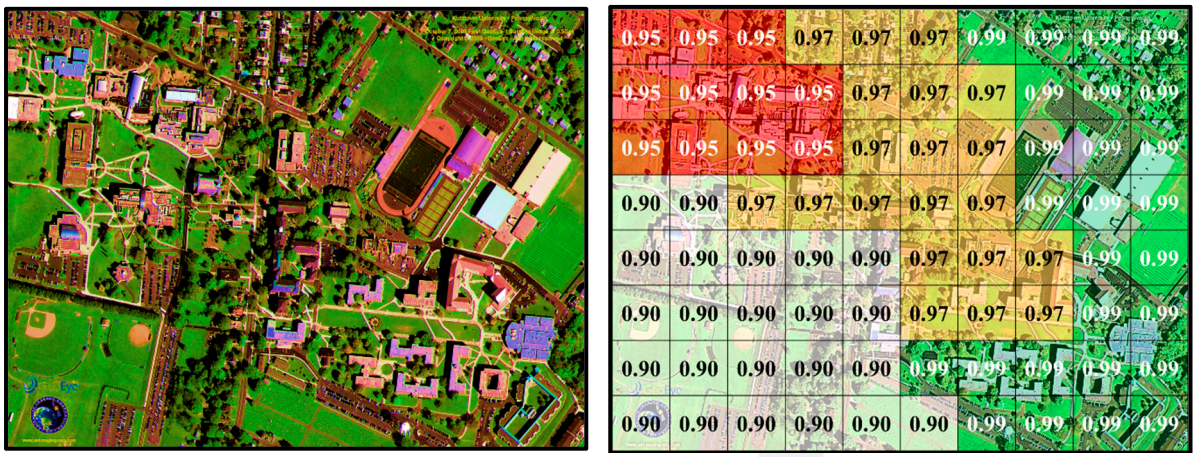


Figure 5. Projected path of Hurricane Sandy 2012 (Source: National Oceanic and Atmospheric Administration).



(**a**) (**b**)

Figure 6. Grid based Spatiotemporal Impact as Risk Profile. (**a**) Network Area; and (**b**) Grid Model.

Network elements (nodes and links) contain geographical information. Spatially close links (e.g., along a bridge) have a higher chance of simultaneous failure. Previous models proposed for network resilience assumed that all links installed as straight lines, whereas links are deployed with irregular geometry because of geographical constraints, cost-effectiveness, and government rules. Figure 7 illustrates the fiber-link as a concatenation of multiple link segments of varying lengths where each link-segment is a straight line connecting two points of known geodetic locations. In Reference [94], Iqbal et al. considered the geography of links (as indicated in Figure 7) to detect spatially close fibers using data structures like kD-tree and R-tree. The minimum separation distance between the links was constrained by a value α to represent the construction-level and large-scale failures. They also proposed a polynomial algorithm based on R-tree to identify the spatially close risk groups using the minimum number of Distinct Risk Group (DRG). Extending the work of Reference [94], Ashraf et al. in Reference [95] proposed a polynomial-time algorithm to find the spatially-disjoint pair of light paths between two network nodes using kD-tree processing and kNN (k-nearest neighbors) search algorithm. Running time and optimality of the proposed algorithm can be controlled via a heuristic K (required number of shortest paths). Awaji et al. proposed a novel technique in Reference [96] to boost the network robustness against natural disasters like mega quakes and tsunamis. They outlined the solutions for two imperative facets: Survivability against damages in broad-area networks and quick network recovery in confounded areas. They proposed an integrated approach of optical packet switching and circuit switching for more survivable broad-area networks, while emergency optical networks and hierarchical topologies are elaborated for quick network recovery in devastated areas. In Reference [97], Al Mamoori et al. formulated an ILP model which minimizes the network resources (wavelength links) needed to handle requests for communication in data center networks. They analyzed the model for different numbers of data centers, multiple disasters, and optical reach.

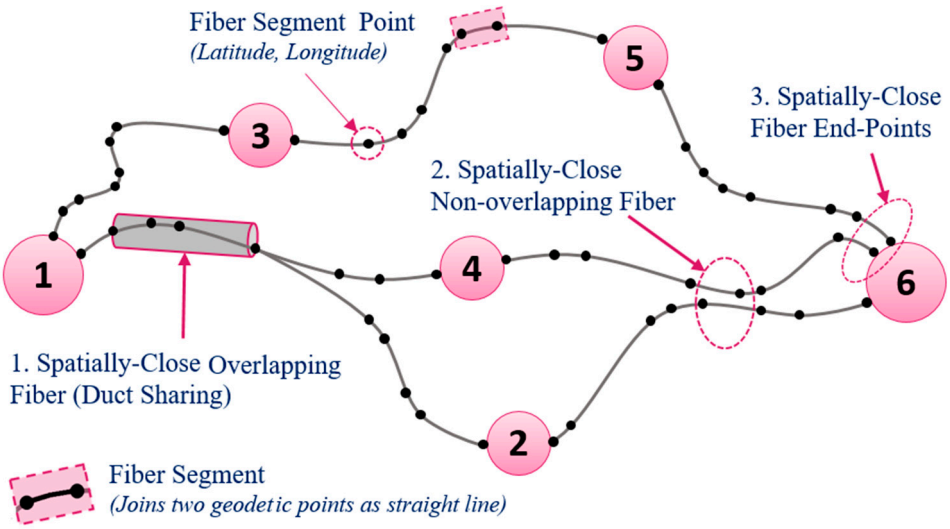


Figure 7. Link Representation and their Minimum Separation Distance.

GeoPath diversification in optical networks is essential to establish reliable, high capacity, and resilient connections between two network nodes. In References [98,99], Cheng et al. introduced GeoPath diversification mechanisms where routing decisions considered to be a physical network topology. Performance of the proposed mechanism and that of Open Shortest Path First (OSPF) compared when the network was subject to area-based challenge. A new metric as compensated Total Geographical Graph Diversity (cTGGD) introduced to distinguish the GeoPath diversity of different network topologies. Sousa et al. [100] proposed an integer linear program which computes a pair of minimum path length such that all intermediary nodes and links are at least D km apart from each other. In this way, a disaster having coverage diameter less than D km cannot influence the backup path and result in terms of network resilience against disaster-based failures. They also consider the vulnerability regions to assess the susceptible components (nodes and/or links) of D-geodiverse paths pair between two network nodes belonging to the same region. Similarly, a geographical location-aware algorithm proposed by Wang et al. in Reference [101] that calculates multiple paths separated by at least a given spatial distance, known as pre-defined distance threshold r. Two variants of the algorithm based on a penalty adjustment are proposed and tested. Wang et al. evaluated the performance using the proximity factor and concurrent failures to measure the resilience of the algorithm. The number of failures depends upon topology and failure generation. The proximity factor is the geographical correlation between paths of the computed pair. Table 1 shows the close comparison of survivability techniques.

Table 1. Close comparison of large-scale attack and disaster survivability techniques.

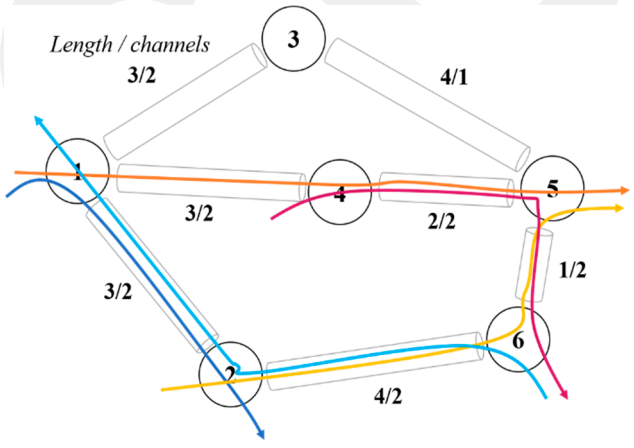
Ref	Techniques/Formulation	Objectives	Assessments/Limitations
[76]	Protection from WMD attacks (a technical report).	Combating the terrorist attacks like WDM to assess the impacts of catastrophic failures on critical infrastructures.	Characterizing the impact of WMD attacks in WDM networks. Re-provisioning algorithms, multi-path routing, data replication, WMD-risk-aware virtual-network mapping & re-mapping and service recovery. Addresses the network preparedness for upcoming attacks.
[83]	Algorithms for network recovery and augmentation under geographically correlated region failures.	Effective connection recovery in the event of regional failures.	Addressed two NP-hard problems and proposed the integer programming formulations as their solutions. Also proposed corresponding greedy algorithms to approximate the optimal solutions.
[85]	Network metrics: weighted spectrum (WS) and network criticality (NC)	To enumerate the network survivability against geographically correlated failures.	Assessed the network survivability in the event of geographically correlated failures. Solved an optimization problem to determine the most vulnerable geographic nodes and cuts in the networks.
[86]	Critical Region Identification Model, GeoDivRP	Finding the most vulnerable regions at fiber-level and enhancing the performance of GeoDivRP.	Considered the regionally correlated failures and attacks and proposed a model to identify the critical region. The effectiveness of the model is evaluated using both weighted and unweighted topologies. The obtained results are used to enhance the performance of routing using GeoDivRP.
[87]	Disaster-affected Region Identification Model Metrics for evaluation of model predicted areas (1) Region Betweenness-centrality (2) Risk Impact	Characterizing the heterogeneous areas affected by different types of disasters. Introduced two metrics RBC to represent the region importance in terms of all-node pair shortest paths and Risk Impact to enumerate the threat posed by disasters within a region.	Proposed a model to identify disaster-affected areas with different shapes and sizes using Poisson distribution, and analyzed the effect of link existence and disaster area size on these metrics.

Table 1. *Cont.*

Ref	Techniques/Formulation	Objectives	Assessments/Limitations
[89]	Polynomial-time algorithm to find the critical region Heuristic to find the region disjoint paths	Finding critical region and region disjoint paths	Determined the vulnerability of a network to the failure of a certain region embedded in a plane. The methodology was applicable to different geometries of the critical region. The critical region may include disconnected pairs of nodes, average shortest path length etc.
[93]	Risk profiling for spatiotemporal characteristics of disasters (link availability values)	Finding risk profile of disasters at different areas of the network at different times.	Preventative measures can be taken if risk profile of spatiotemporal disaster impact is predicted. The most risk-averse path is obtained via the shortest path algorithm using as weights the –log of the link availabilities.
[94]	Polynomial-time algorithms Implementing kD-Tree and R-Tree Data Structures	Detection of spatially close fibers and spatially close risk groups.	Considered the geography of links to detect spatially close fibers. Minimum separation distance relies on α which represent the radius of construction-level and large-scale failures. Identified the spatially close risk groups using the minimum number of DRG.
[97]	ILP Formulation	A robust scheme that minimizes the network resources (wavelength links) needed to handle the requests for communication in data center networks.	Prioritized the minimization of resource utilization and the number of disasters. However, resource utilization increases with the increase in a number of disasters as disasters reduces the capacity.
[99]	Path Geo-Diversification cTGGD	Impact of Path Geo-Diversification on the routing performance	Performance of the proposed mechanism compared with that of when the network was subject to area-based challenge. cTGGD used to distinguish the GeoPath diversity of different network topologies.
[100]	ILP	Path geo-diversification where a demand between two network nodes supported by a pair of geographically separated paths of a minimum distance.	ILP is complex in computation and includes all unnecessary path computations which are time-consuming. Preferably, proposed heuristic algorithms in the literature may provide acceptable solutions of the problem.
[101]	Brute force approach and enhanced K-shortest path algorithm	Geographic aware route selection algorithm to find alternative paths with appropriate geographical separation referred to as the proximity factor.	Work based on the grid-based network and do not consider any real network. Further, PF based on node-to-node separation whereas fiber links should also be considered for alternate/disjoint path computation.

5. Congestion-Aware Routing and Wavelength Assignment

The last, but not least, concerning issue is the traffic congestion that may be induced due to the rerouting of disrupted or blocked traffic in the event of a disaster. The solution proposed in Reference [62], which begins with the thought that telecom networks have some spare capacity to avoid or alleviate traffic congestion. Such capacity can be utilized to give better assurance against disasters. If the network resources are consumed appropriately and the network loaded is distributed evenly over the links, the congestion will be controlled in terms of connection acceptance rate and lower blocking probability. Overloading of network resources is also known as network congestion. It means that the available capacity of the network cannot fulfill the total demand or connection requests. Congestion occurs due to several reasons like low bandwidth, multicasting, bad configuration, too many hosts in the broadcast domain, broadcast storm (can be a busy day for e-commerce or Black Friday sales) or rerouting because of disasters-based network path failures etc. Generally, congestion can be avoided by network segmentation, reconfiguring Transmission Control Protocol/Internet Protocol (TCP/IP) settings, backpressure routing, and prioritizing the network traffic. There are several studies on congestion control techniques [102–112] in which network performance is evaluated under various network conditions and a range of parameters for heterogeneous networking environments. In Reference [113], Wu et al. proposed a model for per link congestion control by balancing network resource allocation considering the current and future demands of light path requests. Figure 8a shows a network of six nodes and bidirectional links with lengths and channels available per link. Five light paths have established upon connection requests on the first-fit rule. Figure 8b summarizes the network traffic over each link. According to the Routing and Wavelength Assignment (RWA) problem, light paths are established considering the path lengths and the channel availability with the lowest blocking probabilities. Taking the current statistics in view, Figure 6a clearly indicates that connection requests between nodes $(1 \leftrightarrow 4)$, $(1 \leftrightarrow 3)$, and $(3 \leftrightarrow 5)$ can be established immediately because of channel availability. If a connection request arrives other than the above-mentioned requests, then it has to wait for a channel to be free which causes a delay or drop in the connection request. In the case connection request $(4 \leftrightarrow 5)$, a light path can be established immediately, however, it incorporates a delay at the cost of path length (i.e., 4→1→3→5 as there is no channel available at 4→5), which introduces a path delay. Hence, it can be concluded that there is a tradeoff between path length and capacity while establishing a connection between two nodes of a network.



(**a**)

Links	Length	Offered Channels	Channels Used
1↔2	3	2	2
1↔3	3	2	0
1↔4	3	2	1
2↔6	4	2	2
3↔5	4	1	0
4↔5	2	2	2
6↔5	1	2	2

(**b**)

Figure 8. Physical network topology with 6 nodes and 7 bidirectional links. (**a**) Network Light path Establishment and (**b**) Network Traffic Table.

Realistic networks have irregular network topologies and connection requests are random. Whenever the traffic load increases, the number of idle channels per link decreases in establishing

the connections. Connection requests start blocking when there zero channels exist over the links and can be measured as blocking probability. Rani et al. [30] proposed a congestion-aware strategy dynamic in nature which seeks to minimize the blocking probability by the proportional distribution of network traffic over the links to enhance resource utilization. Wason et al. in References [114,115] developed a low complexity mathematical model to calculate and reduce the blocking probability of routes and overall network. Authors analyzed blocking probabilities against a number of links, a number of free wavelengths and length of routes. In Reference [116], Wason et al. proposed another mathematical model for wavelength-routed WDM networks to optimize the blocking probability. Authors compared the proposed model with References [114,115] and showed that recent model performs better than earlier models. Singal et al. also address the blocking probability of ring optical networks in Reference [117] considering the total number of wavelengths in the network. They analyzed the blocking probability node by node by varying the number of wavelengths and using wavelength conversion algorithms. Results showed that blocking probability decreases with the increase of a number of wavelengths.

RWA can be treated either as individual problems (i.e., routing problem or wavelength assignment problem) or as a single problem on the basis of scale, size, and other network preferences. Sohal et al. [118] addressed the routing problem in wavelength-routed optical networks. They studied the performance of Dijkstra and least congested path routing algorithms in terms of path lengths and blocking probability. RWA can also be utilized either in a centralized or distributed manner. For small-scale networks, there are a small number of requests; hence, the centralized RWA approach can be used to tackle the problem. However, for large-scale networks where traffic is high with a random pattern should utilize the distributed method. Zanjani et al. [119] proposed a congestion-aware DLA routing algorithm which considered the congestion as a decision point to allocate resources. The end-to-end connectivity assurance and congestion avoidance have raised the need for robust and low latency routing protocols. Stewart et al. presented Congestion Avoidance Shortest Path Routing (CASPaR) algorithm in Reference [120] that pursues to enhance the Packet Delivery Probability (PDP) and reduces the latency. Continuous service availability is the major concern of disaster-resilient all-optical networks. Hu et al. in Reference [121] proposed a new WRT scheme without disrupting the network services to meet the continuity constraints of wavelength and services/data loss. Re-tuning is conducted only on the backup/alternate path in case of failure of the primary path that carries the traffic under normal conditions. Authors also proposed a heuristic version of the same to intact the optimality and performance. Work on congestion-aware RWA is summarized in Table 2.

Table 2. Congestion-Aware Routing and Wavelength Assignment Techniques.

Ref	Techniques	Objectives	Limitations
[30]	Congestion control strategy in WDM networks	Dynamic strategy symmetrically distributes the traffic on the links according to the channels available on the link.	Criteria for most and least used links not defined before distribution of data that may be based on a number of connection requests, connection establishment strategy or path lengths.
[117]	Analysis of blocking performance in Ring optical network	Computing and analyzing the node-by-node blocking performance in the ring optical network using wavelength conversion algorithms	Whole work is based on the 8-node ring network. Results showed that blocking probability decreases with the increase of a number of wavelengths.
[118]	Dijkstra Algorithm and Least Congested Path Routing Algorithm	Studied the performance of these algorithms in terms of blocking probability and path lengths	Only focused on the routing algorithm of the RWA problem.
[119]	LC-DLA routing algorithm	Resource allocation on the decision of network congestion in large-scale networks taking a huge number of connection requests and heavy traffic load in the account.	Proposed LC-DLA provisions least congested lightpaths as compared to other DLA and shortest path algorithms. Existing algorithms may introduce the traffic jam/bottlenecks while accumulating congestion and hence upsurge the blocking probability. It is observed that LC-DLA tries to balance the network congestion and resultantly avoid the traffic jams.

Table 2. *Cont.*

Ref	Techniques	Objectives	Limitations
[120]	CASPaR Algorithm	Pursued to enhance the PDP and reduced the latency by selecting the shortest path.	CASPaR shows improved performance than that of other protocols but in terms of packet delivery only.
[122]	Centralized PCE with STAR (Self-Tuned Adaptive Routing) algorithm	Efficient path computation avoiding underutilization of capacity over links and congestion.	Introduced a novel centralized PCE with STAR algorithm that discovers the paths considering available link capacity and load balancing. Separate path computing and path signaling functions which give operators more control over their network.
[123]	MILP Model to handle capacity exhaustion problem	Investigate post-disaster static traffic floods in several scenarios to reduce traffic blocking.	The arrival of connection requests is random so network traffic and lightpath establishment are also dynamic in real-life networks. Should be investigated with dynamic traffic floods.

All services in optical network finally converge at IP layer and move into the cloud. It is essential for service providers to employ optimized path computation techniques for efficient routing. OSPF and Intermediate System to Intermediate System (ISIS) routing protocols use Dijkstra algorithm to find the shortest path for every source-destination pair. As a result, short weighted links easily congested while other links remained underutilization. Hao et al. in Reference [122] introduced a novel centralized Path Computation Element (PCE) that employs refined path computation algorithm with dynamic link cost metrics to enable network-embedded routing protocols in discovering paths that use available link capacity more efficiently. Further, PCE applies Software-Defined Optical Networking (SDON) [124] paradigms to separate path computing and path signaling functions, which gives operators more control over their network. Hao et al. proposed that centralized PCE with Self-Tuned Adaptive Routing (STAR) algorithm contributes to the efficient consumption of link capacity for load balancing and avoids overloading the links (i.e., to avoid congestion and deadlocks) as well. Overall, single PCE or multiple PCEs in a network results in terms of more revenue-bearing traffic.

The incident of Boston Bombing in 2013 introduced a new problem as capacity exhaustion during a disaster and might affect the ICT services. Unlike considerations used in previous studies to design resilient networks, this issue is relatively different. Human instinct drives him to get more and more information about what is going on during a disaster. This practice has been progressively increased since the introduction of social media, mobile broadband, and several other like services. According to Fraustino et al. [125], two out of three persons use social media in the event of disasters. It is estimated that about 95% people make phone calls (caused semi-shutdown of mobile networks) and 76% use social media to post information regarding the incident [126,127]. Live broadcasts and video streaming (i.e., TV breaking news, user-generated videos etc.) also got attraction [128]. However, ICT's physical infrastructure is not damaged but heavy traffic and a huge number of connection requests overload the access network capacity referred to as capacity exhaustion problem. The core optical network may have the capability to handle such traffic flood as a consequence of natural disasters and human threats so that violation of the SLA is avoided. Post-disaster traffic has a higher influence on the QoT of light paths in all-optical networks and failure of few seconds may cause massive losses both in terms of data volumes and decline of revenue. Nasralla et al. in Reference [123] proposed a MILP to handle capacity exhaustion problem due to post-disaster traffic floods. Authors evaluated the network blocking for single node flooding with different traffic flood sizes. The proposed model has investigated four techniques to maximally serve the traffic floods using rerouting, excess capacity, traffic filtering and differentiated services.

6. Challenges in Disaster-Resilient Optical Network Survivability

With the high frequency of fiber cut and the tremendous traffic loss, network survivability becomes a critical concern in network design and its real-time operation. It is in ultimate need of network operators to design effective methods to recover from failures of network links and nodes.

Most of the research work on survivability in WDM networks focuses on the recovery from a single link or node failure. Multiple (i.e., near-simultaneous) failures are also possible in a realistic network, and appropriate recovery methods can be designed.

In this paper, most of the studies proposed techniques to provision disjoint light path between two network nodes to enhance network resilience against failures and disasters. Large-scale disasters show their impact on the large geographical area. While, disjoint light path are physically disjointed but both light paths (primary as well as backup) may simultaneously fail due to the minimum spatial distance between them. We have shown, in Figure 8, how fibers can be spatially close. Algorithms for detection of spatially close fibers and grouping them using the minimum number of distinct risk groups are proposed in Reference [94]. However, light paths are established against connection requests, which are composed of fiber links in real networks. This work needs to extend from spatially close fibers to spatially close disjoint paths for risk-averse path provisioning. Similarly, Reference [101] presented the geographic proximity-aware route selection algorithm to discover backup paths with appropriate proximity factor. The study is based on a grid-based network, whereas fiber links are deployed in a zig-zag (irregular geometry) manner in real-life networks. Hence, more sophisticated techniques can be investigated.

Current techniques for discovering shortest light paths and alternate light paths do not account for parameters like light path lengths, link capacities, light path capacities, connection requests, and light path establishment at the same time and accommodate one or two of them during provisioning or re-provisioning. In this way, most of the links on popular routes get congested and some remained underutilized or un-used within the network. This can be referred to as inappropriate utilization of network capacity. Un-used links and their stranded capacity of a network should also be considered for optimized utilization of network resources. As in disaster scenarios, network resources face sudden traffic floods and such techniques cannot provide the resilience or survivability to networks. Hence this opens a new research challenge for the research community.

Capacity exhaustion has become an acute problem due to post-disaster traffic floods as indicated in Reference [123]. To deal with the critical demand of ICT services during traffic fluctuations and upsurges, Least-Congested Distributed Light path Allocation (LC-DLA), as proposed in Reference [119] for large-scale networks, should be studied to mitigate capacity exhaustion problem while considering a huge number of connection requests and heavy traffic loads.

7. Conclusions

Optical networks are deployed across the world delivering higher-scale connectivity and huge data transmission. Network component failures particularly fiber cuts are frequent, whereas disaster-based failures are occasional, however, they disrupt the network severely. Large-scale disasters contribute towards geographically correlated failures that can damage a large portion of optical networks. Network survivability emerged from protection and restoration mechanisms to disaster-resilient network survivability techniques to mitigate geographically correlated large-scale disaster impacts. Another factor is network congestion that occurs due to the rerouting of disrupted paths or traffic fluctuations or growth. Network congestion is an inevitable problem like disasters. It is direly needed for network operators that solutions should be designed not only to overcome described network problems, but also eradicate the issues like cascading failures and network congestion. In this paper, we critically studied the solutions for small-scale (network component) failures and large-scale (disaster-based) failures. A framework based on different approaches may provide better protection and survivability from disasters with capacity optimization. This will assist the fault tolerance management to improve network robustness against disasters.

Funding: This work was supported by the Ministry of Higher Education Malaysia (MOHE) FRGS funding vote number 4F961 and the administration of Universiti Teknologi Malaysia through Institute Grant vote number 02K85.

Conflicts of Interest: The authors declare no conflict of interest.

Acronyms

ASR	Availability Satisfaction Ratio
ATM	Asynchronous Transfer Mode
BTS	Base Transceiver Station
CASPaR	Congestion Avoidance Shortest Path Routing
cTGGD	Compensated Total Geographical Graph Diversity
DAL	Distributed Lightpath Allocation
DLBSPP	Dynamic Load Balancing Shared Path Protection
DRG	Distinct Risk Groups
DWDM	Dense Wavelength Division Multiplexing
EMP	Electromagnetic Pulse
FTBCP	Fault Tolerance Method Based on Cheapest Paths
GeoDivRP	Geodiverse Routing Protocol
GIS	Geographic Information System
GMPLS	Generalized Multi-Protocol Label Switching
HCA	Hybrid Connection Algorithm
ICT	Information Communication Technology
ILP	Integer Linear Programming
IP Layer	Internet Protocol Layer
ISIS	Intermediate System to Intermediate System
LC-DAL	Least-Congested Distributed Lightpath Allocation
MILP	Mixed Integer Linear Programming
MPLS	Multi-Protocol Label Switching
OSPF	Open Shortest Path First
OXCs	Optical Cross-Connects
PCE	Path Computation Element
PDP	Packet Delivery Probability
QoS	Quality of Service
QoT	Quality of Transmission
RECODIS	Resilient Communication services protecting end-user applications from Disaster-based failures
RWA	Routing and Wavelength Assignment
SDH	Synchronous Digital Hierarchy
SDON	Software-Defined Optical Networking
SFPP	Short Full Path Protection
SLA	Service Level Agreement
SONET	Synchronous Optical Network
SPPP	Shortest Path Pair Protection
STAR	Self-Tuned Adaptive Routing
WDM	Wavelength Division Multiplexing
WMD	Weapon of Mass Destruction
WRT	Wavelength Retuning

References

1. Agrawal, A.; Sharma, P.; Bhatia, V.; Prakash, S. Survivability improvement against earthquakes in backbone optical networks using actual seismic zone information. *arXiv* **2017**, arXiv:1703.02358.
2. How Much Bandwidth Do We Need? Available online: https://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/ (accessed on 13 April 2017).
3. Saleh, A.A.; Simmons, J.M. Technology and architecture to enable the explosive growth of the internet. *IEEE Commun. Mag.* **2011**, *49*, 126–132. [CrossRef]
4. Awduche, D.; Chiu, A.; Elwalid, A.; Widjaja, I.; Xiao, X. *Overview and Principles of Internet Traffic Engineering*; RFC 3272; IETF: Fremont, CA, USA, 2002.

5. Bouillet, E.; Ellinas, G.; Labourdette, J.F.; Ramamurthy, R. Mesh routing and recovery framework. In *Path Routing in Mesh Optical Networks*; John Wiley & Sons Ltd.: Chichester, UK, 2007; pp. 61–80.
6. Sivalingam, K.M.; Subramaniam, S. *Emerging Optical Network Technologies: Architectures, Protocols and Performance*; Springer Science & Business Media: New York, NY, USA, 2005.
7. Rak, J.; Hutchison, D.; Calle, E.; Gomes, T.; Gunkel, M.; Smith, P.; Tapolcai, J.; Verbrugge, S.; Wosinska, L. Recodis: Resilient communication services protecting end-user applications from disaster-based failures. In Proceedings of the 18th International Conference on Transparent Optical Networks (ICTON), Trento, Italy, 10–14 July 2016; pp. 1–4.
8. Adachi, T.; Ishiyama, Y.; Asakura, Y.; Nakamura, K. The restoration of telecom power damages by the great east japan earthquake. In Proceedings of the IEEE 33rd International Telecommunications Energy Conference (INTELEC), Amsterdam, The Netherlands, 9–13 October 2011; pp. 1–5.
9. Urushidani, S.; Aoki, M.; Fukuda, K.; Abe, S.; Nakamura, M.; Koibuchi, M.; Ji, Y.; Yamada, S. Highly available network design and resource management of SINET4. *Telecommun. Syst.* **2014**, *56*, 33–47. [CrossRef]
10. Okumura, H. The 3.11 disaster and data. *J. Inf. Process.* **2014**, *22*, 566–573. [CrossRef]
11. Seismonepal Website. Available online: http://seismonepal.gov.np/ (accessed on 12 January 2018).
12. Dawadi, B.R.; Shakya, S. Ict implementation and infrastructure deployment approach for rural nepal. In *Recent Advances in Information and Communication Technology*; Springer: Cham, Switzerland, 2016; pp. 319–331.
13. Mexico Earthquake Fact Sheet #5 (29 September 2017). Available online: https://www.usaid.gov/sites/default/files/documents/1866/mexico_eq_fs05_09-29-2017.pdf (accessed on 12 January 2018).
14. Undersea Internet Cables Off Egypt Disrupted as Navy Arrests Three. Available online: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests (accessed on 12 January 2018).
15. Koshimura, S.; Kayaba, S.; Matsuoka, M. Integrated approach to assess the impact of tsunami disaster. In *Safety, Reliability and Risk of Structures, Infrastructures and Engineering Systems*; Taylor & Francis Group: London, UK, 2010; pp. 2302–2307.
16. Lin, Z.; Levy, J.K.; Lei, H.; Bell, M.L. Advances in disaster modeling, simulation and visualization for sandstorm risk management in North China. *Remote Sens.* **2012**, *4*, 1337–1354. [CrossRef]
17. Habib, M.F.; Tornatore, M.; Dikbiyik, F.; Mukherjee, B. Disaster survivability in optical communication networks. *Comput. Commun.* **2013**, *36*, 630–644. [CrossRef]
18. Goścień, R.; Walkowiak, K. Modeling and optimization of data center location and routing and spectrum allocation in survivable elastic optical networks. *Opt. Switch. Netw.* **2017**, *23*, 129–143. [CrossRef]
19. Davis, D.A.; Vokkarane, V.M. Generalized survivability models for many-to-many communication. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 729–735.
20. Zhang, W.; Tang, J.; Wang, C.; de Soysa, S. Reliable adaptive multipath provisioning with bandwidth and differential delay constraints. In Proceedings of the IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
21. Mauthe, A.; Hutchison, D.; Cetinkaya, E.K.; Ganchev, I.; Rak, J.; Sterbenz, J.P.; Gunkelk, M.; Smith, P.; Gomes, T. Disaster-resilient communication networks: Principles and best practices. In Proceedings of the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016; pp. 1–10.
22. Gomes, T.; Tapolcai, J.; Esposito, C.; Hutchison, D.; Kuipers, F.; Rak, J.; de Sousa, A.; Iossifides, A.; Travanca, R.; André, J. A survey of strategies for communication networks to protect against large-scale natural disasters. In Proceedings of the 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016; pp. 11–22.
23. Kmiecik, W.; Rak, J.; Medeiros, C.; Heegaard, P.E.; Mas Machuca, C.; André, J.; Jorge, L.; Musumeci, F.; Voyiatzis, A.; Pasic, A. A survey on network resiliency methodologies against weather-based disruptions. In Proceedings of the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016.
24. Tornatore, M.; André, J.; Babarczi, P.; Braun, T.; Følstad, E.; Heegaard, P.; Hmaity, A.; Furdek, M.; Jorge, L.; Kmiecik, W.; et al. A survey on network resiliency methodologies against weather-based disruptions. In Proceedings of the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016; pp. 23–34.

25. Shiraiwa, M.; Yoshikane, N.; Xu, S.; Tsuritani, T.; Miyata, N.; Mori, T.; Miyabe, M.; Katagiri, T.; Yoshida, S.; Tanaka, M. Experimental demonstration of disaggregated emergency optical system for quick disaster recovery. *J. Lightw. Technol.* **2018**, *36*, 3083–3096. [CrossRef]
26. Shiraiwa, M.; Yoshikane, N.; Xu, S.; Tsuritani, T.; Miyata, N.; Mori, T.; Miyabe, M.; Katagiri, T.; Yoshida, S.; Tanaka, M. First experimental demonstration of disaggregated emergency optical system for quick disaster recovery. In Proceedings of the Optical Fiber Communication Conference, San Diego, CA, USA, 11–15 March 2018; p. Th2A.29.
27. Zhou, D.; Subramaniam, S. Survivability in optical networks. *IEEE Netw.* **2000**, *14*, 16–23.
28. Zhang, J.; Mukherjee, B. A review of fault management in wdm mesh networks: Basic concepts and research challenges. *IEEE Netw.* **2004**, *18*, 41–48. [CrossRef]
29. Mukherjee, B. *Optical WDM Networks*; Springer Science & Business Media: New York, NY, USA, 2006.
30. Rani, S.; Sharma, A.K.; Singh, P. Survivability strategy with congestion control in wdm optical networks. In Proceedings of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET 2007), Dubai, UAE, 18–20 November 2007; pp. 1–4.
31. Zhang, Z.; Li, Z.; He, Y. Network capacity analysis for survivable WDM optical networks. In Proceedings of the International Conference on Instrumentation, Measurement, Circuits, and Systems (IMCCC 2012), Harbin, China, 8–10 December 2012; pp. 291–296.
32. Sengupta, S.; Ramamurthy, R. From network design to dynamic provisioning and restoration in optical cross-connect mesh networks: An architectural and algorithmic overview. *IEEE Netw.* **2001**, *15*, 46–54. [CrossRef]
33. Gupta, R.; Chi, E.; Walrand, J. Different algorithms for normal and protection paths. *J. Netw. Syst. Manag.* **2005**, *13*, 13–33. [CrossRef]
34. Ramamurthy, S.; Mukherjee, B. Survivable wdm mesh networks. Part I—Protection. In Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM'99, New York, NY, USA, 21–25 March 1999; pp. 744–751.
35. Saini, H.; Garg, A.K. Protection and restoration schemes in optical networks: A comprehensive survey. *Int. J. Microw. Appl.* **2013**, *2*, 5–11.
36. Chatterjee, B.C.; Sarma, N.; Sahu, P.P.; Oki, E. Literature survey. In *Routing and Wavelength Assignment for WDM-Based Optical Networks*; Springer: Cham, Switzerland, 2017; pp. 17–34.
37. Gill, P.; Jain, N.; Nagappan, N. Understanding network failures in data centers: Measurement, analysis, and implications. In Proceedings of the ACM SIGCOMM Computer Communication Review, Toronto, ON, Canada, 15–19 August 2011; pp. 350–361.
38. Mohan, N.; Seema. Network protection and restoration in optical networks: A comprehensive study. *Int. J. Res. Eng. Technol. (IJERT)* **2013**, *2*, 50–54.
39. Ramamurthy, S.; Sahasrabuddhe, L.; Mukherjee, B. Survivable WDM mesh networks. *J. Lightw. Technol.* **2003**, *21*, 870. [CrossRef]
40. Vasseur, J.-P.; Pickavet, M.; Demeester, P. *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*; Elsevier: San Francisco, CA, USA, 2004.
41. Maier, G.; Pattavina, A.; De Patre, S.; Martinelli, M. Optical network survivability: Protection techniques in the wdm layer. *Photonic Netw. Commun.* **2002**, *4*, 251–269. [CrossRef]
42. Binti Halida, S.N.F.; Idrus, S.; Farabi, M.; Zulkifli, N. Dedicated protection scheme for optical networks survivability. In Proceedings of the 2011 4th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO), Kuala Lumpur, Malaysia, 19–21 April 2011; pp. 1–5.
43. Bouillet, E. *Path Routing in Mesh Optical Networks*; John Wiley & Sons: Chichester, UK, 2007.
44. Alshaer, H. Dynamic connection provisioning with shared protection in IP/WDM networks. *Int. J. Commun. Syst.* **2014**, *27*, 2832–2850. [CrossRef]
45. Ou, C.; Zang, H.; Singhal, N.K.; Zhu, K.; Sahasrabuddhe, L.H.; MacDonald, R.A.; Mukherjee, B. Subpath protection for scalability and fast recovery in optical wdm mesh networks. *IEEE J. Sel. Areas Commun.* **2004**, *22*, 1859–1875. [CrossRef]
46. Choi, H.; Subramaniam, S.; Choi, H.-A. On double-link failure recovery in wdm optical networks. In Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM, New York, NY, USA, 23–27 June 2002; pp. 808–816.

47. Ramasubramanian, S.; Chandak, A. Dual-link failure resiliency through backup link mutual exclusion. *IEEE/ACM Trans. Netw.* **2008**, *16*, 157–169. [CrossRef]
48. Guo, Y.; Kuipers, F.; Van Mieghem, P. Link-disjoint paths for reliable qos routing. *Int. J. Commun. Syst.* **2003**, *16*, 779–798. [CrossRef]
49. Kim, S.-I.; Lumetta, S. *Multiple Failure Survivability in WDM Mesh Networks*; Report No. UILU-ENG-06-2205; Coordinated Science Laboratory: Urbana, IL, USA, 2006.
50. Sivakumar, M.; Maciocco, C.; Mishra, M.; Sivalingam, K.M. A hybrid protection-restoration mechanism for enhancing dual-failure restorability in optical mesh-restorable networks. In Proceedings of the OptiComm 2003: Optical Networking and Communications, Dallas, TX, USA, 1 October 2003; pp. 37–48.
51. Ruan, L.; Feng, T. A hybrid protection/restoration scheme for two-link failure in wdm mesh networks. In Proceedings of the Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA, 6–10 December 2010; pp. 1–5.
52. Feng, T.; Long, L.; Kamal, A.E.; Ruan, L. Two-link failure protection in WDM mesh networks with p-cycles. *Comput. Netw.* **2010**, *54*, 3068–3080. [CrossRef]
53. Jaumard, B.; Bui, M.; Mukherjee, B.; Vadrevu, C.S. Ip restoration vs. Optical protection: Which one has the least bandwidth requirements? *Opt. Switch. Netw.* **2013**, *10*, 261–273. [CrossRef]
54. Zhao, Y.; Li, X.; Li, H.; Wang, X.; Zhang, J.; Huang, S. Multi-link faults localization and restoration based on fuzzy fault set for dynamic optical networks. *Opt. Express* **2013**, *21*, 1496–1511. [CrossRef] [PubMed]
55. Kadohata, A.; Tanaka, T.; Imajuku, W.; Inuzuka, F.; Watanabe, A. Rapid restoration sequence of fiber links and communication paths from catastrophic failures. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2016**, *99*, 1510–1517. [CrossRef]
56. Yadav, D.S.; Rana, S.; Prakash, S. Hybrid connection algorithm: A strategy for efficient restoration in wdm optical networks. *Opt. Fiber Technol.* **2010**, *16*, 90–99. [CrossRef]
57. Rani, S.; Sharma, A.K.; Singh, P. Restoration approach in wdm optical networks. *Optik* **2007**, *118*, 25–28. [CrossRef]
58. Chen, B.; Zhang, J.; Zhao, Y.; Lv, C.; Zhang, W.; Huang, S.; Zhang, X.; Gu, W. Multi-link failure restoration with dynamic load balancing in spectrum-elastic optical path networks. *Opt. Fiber Technol.* **2012**, *18*, 21–28. [CrossRef]
59. Jara, N.; Rubino, G.; Vallejos, R. Alternate paths for multiple fault tolerance on dynamic wdm optical networks. In Proceedings of the 2017 IEEE 18th International Conference on High Performance Switching and Routing (HPSR), Campinas, Brazil, 18–21 June 2017; pp. 1–6.
60. Brodkin, J. Why Gmail Went Down: Google Misconfigured Load Balancing Servers. Available online: https://arstechnica.com/information-technology/2012/12/why-gmail-went-down-google-misconfigured-chromes-sync-server/ (accessed on 2 February 2018).
61. Pescaroli, G.; Alexander, D. A definition of cascading disasters and cascading effects: Going beyond the toppling dominos metaphor. *Planet@ Risk* **2015**, *3*, 58–67.
62. Mukherjee, B.; Habib, M.; Dikbiyik, F. Network adaptability from disaster disruptions and cascading failures. *IEEE Commun. Mag.* **2014**, *52*, 230–238. [CrossRef]
63. Erjongmanee, S.; Ji, C. Large-scale network-service disruption: Dependencies and external factors. *IEEE Trans. Netw. Serv. Manag.* **2011**, *8*, 375–386. [CrossRef]
64. Savla, K.; Como, G.; Dahleh, M.A. Robust network routing under cascading failures. *IEEE Trans. Netw. Sci. Eng.* **2014**, *1*, 53–66. [CrossRef]
65. Zhao, J.; Li, D.; Sanhedrai, H.; Cohen, R.; Havlin, S. Spatio-temporal propagation of cascading overload failures in spatially embedded networks. *Nat. Commun.* **2016**, *7*, 10094. [CrossRef] [PubMed]
66. Zhou, Z.; Lin, T.; Thulasiraman, K.; Xue, G.; Sahni, S. Cross-layer network survivability under multiple cross-layer metrics. *J. Opt. Commun. Netw.* **2015**, *7*, 540–553. [CrossRef]
67. Papanikolaou, P.; Christodoulopoulos, K.; Varvarigos, E. Joint multi-layer survivability techniques for ip-over-elastic-optical-networks. *J. Opt. Commun. Netw.* **2017**, *9*, A85–A98. [CrossRef]
68. Dikbiyik, F.; Tornatore, M.; Mukherjee, B. Minimizing the risk from disaster failures in optical backbone networks. *J. Lightwave Technol.* **2014**, *32*, 3175–3183. [CrossRef]
69. Prucnal, P.R.; Fok, M.P.; Deng, Y.; Wang, Z. Physical layer security in fiber-optic networks using optical signal processing. In Proceedings of the 2009 Asia Communications and Photonics Conference and Exhibition (ACP), Shanghai, China, 2–6 November 2009; pp. 1–10.

70. Rejeb, R.; Leeson, M.S.; Machuca, C.M.; Tomkos, I. Control and management issues in all-optical networks. *J. Netw.* **2010**, *5*, 132–139. [CrossRef]
71. Kitayama, K.-I.; Sasaki, M.; Araki, S.; Tsubokawa, M.; Tomita, A.; Inoue, K.; Harasawa, K.; Nagasako, Y.; Takada, A. Security in photonic networks: Threats and security enhancement. *J. Lightwave Technol.* **2011**, *29*, 3210–3222. [CrossRef]
72. Fok, M.P.; Wang, Z.; Deng, Y.; Prucnal, P.R. Optical layer security in fiber-optic networks. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 725–736. [CrossRef]
73. Peng, Y.; Sun, Z.; Du, S.; Long, K. Propagation of all-optical crosstalk attack in transparent optical networks. *Opt. Eng.* **2011**, *50*, 085002.
74. Furdek, M.; Skorin-Kapov, N.; Zsigmond, S.; Wosinska, L. Vulnerabilities and security issues in optical networks. In Proceedings of the 2014 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, 6–10 July 2014; pp. 1–4.
75. Furdek, M.; Skorin-Kapov, N.; Wosinska, L. Attack-aware dedicated path protection in optical networks. *J. Lightw. Technol.* **2016**, *34*, 1050–1061. [CrossRef]
76. Mukherjee, B. *Network Adaptability from WMD Disruption and Cascading Failures*; California Univ Davis: Fort Belvoir, VA, USA, 2016.
77. Lamb, S.; Davis, P. Cenozoic climate change as a possible cause for the rise of the Andes. *Nature* **2003**, *425*, 792–797. [CrossRef] [PubMed]
78. Emanuel, K.; Sundararajan, R.; Williams, J. Hurricanes and global warming: Results from downscaling IPCC AR4 simulations. *Bull. Am. Meteorol. Soc.* **2008**, *89*, 347–367. [CrossRef]
79. Ferdousi, S.; Dikhiyik, F.; Habib, M.F.; Mukherjee, B. Disaster-aware data-center and content placement in cloud networks. In Proceedings of the 2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Kattankulathur, India, 15–18 December 2018; pp. 1–3.
80. Das, A.; Sen, A.; Qiao, C.; Ghani, N.; Mitton, N. A network planning and management tool for mitigating the impact of spatially correlated failures in infrastructure networks. In Proceedings of the 2016 12th International Conference on the Design of Reliable Communication Networks (DRCN), Paris, France, 15–17 March 2016; pp. 71–78.
81. Le, Q.; Piarabutr, P.; Sawangving, N.; Mahadthai, P.; Wuttisittikulkij, L.; Vanichchanunt, P.; Saengudomlert, P. Optical network optimization tool with network survivability. *Electron. Eng. Soc. Korea* **2017**, *1*, 228–231.
82. Matrood, Z.M.; George, L.E.; Mahmood, F.H. A simple gis based method for designing fiber-network. *Int. J. Eng. Innov. Technol.* **2014**, *4*, 49–57.
83. Wang, X. Network recovery and augmentation under geographically correlated region failures. In Proceedings of the Global Telecommunications Conference (GLOBECOM 2011), Kathmandu, Nepal, 5–9 December 2011; pp. 1–5.
84. Fay, D.; Haddadi, H.; Thomason, A.; Moore, A.W.; Mortier, R.; Jamakovic, A.; Uhlig, S.; Rio, M. Weighted spectral distribution for internet topology analysis: Theory and applications. *IEEE/ACM Trans. Netw.* **2010**, *18*, 164–176. [CrossRef]
85. Long, X.; Tipper, D.; Gomes, T. Measuring the survivability of networks to geographic correlated failures. *Opt. Switch. Netw.* **2014**, *14*, 117–133. [CrossRef]
86. Cheng, Y.; Sterbenz, J.P. Critical region identification and geodiverse routing protocol under massive challenges. In Proceedings of the 7th International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, 5–7 October 2015; pp. 14–20.
87. Iqbal, F.; Kuipers, F. On centrality-related disaster vulnerability of network regions. In Proceedings of the 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, Italy, 4–6 September 2017; pp. 1–6.
88. Gardner, M.T.; Beard, C. Evaluating geographic vulnerabilities in networks. In Proceedings of the 2011 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), Naples, FL, USA, 10–12 May 2011; pp. 1–6.
89. Trajanovski, S.; Kuipers, F.A.; Ilić, A.; Crowcroft, J.; Van Mieghem, P. Finding critical regions and region-disjoint paths in a network. *IEEE/ACM Trans. Netw.* **2015**, *23*, 908–921. [CrossRef]
90. Saito, H. Analysis of geometric disaster evaluation model for physical networks. *IEEE/ACM Trans. Netw.* **2015**, *23*, 1777–1789. [CrossRef]

91. Saito, H. Spatial design of physical network robust against earthquakes. *J. Lightw. Technol.* **2015**, *33*, 443–458. [CrossRef]
92. Tran, P.N.; Saito, H. Enhancing physical network robustness against earthquake disasters with additional links. *J. Lightw. Technol.* **2016**, *34*, 5226–5238. [CrossRef]
93. Iqbal, F.; Kuipers, F. Spatiotemporal risk-averse routing. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, USA, 10–14 April 2016; pp. 395–400.
94. Iqbal, F.; Trajanovski, S.; Kuipers, F. Detection of spatially-close fiber segments in optical networks. In Proceedings of the 12th International Conference on the Design of Reliable Communication Networks (DRCN), Paris, France, 15–17 March 2016; pp. 95–102.
95. Ashraf, M.W.; Idrus, S.M.; Iqbal, F. Maximally spatial-disjoint lightpaths. In Proceedings of the International Conference on Electrical, Electronics, Communication and Control Engineering (ICEECC), Kuala Lumpur, Malaysia, 5–6 December 2017; UTM: Kuala Lumpur, Malaysia, 2017.
96. Awaji, Y.; Furukawa, H.; Xu, S.; Shiraiwa, M.; Wada, N.; Tsuritani, T. Resilient optical network technologies for catastrophic disasters. *J. Opt. Commun. Netw.* **2017**, *9*, A280–A289. [CrossRef]
97. Al Mamoori, S.; Jaekel, A.; Bandyopadhyay, S. Disaster-aware wdm network design for data centres. In Proceedings of the 18th International Conference on Distributed Computing and Networking, Hyderabad, India, 5–7 January 2017; p. 38.
98. Cheng, Y.; Li, J.; Sterbenz, J.P. Path geo-diversification: Design and analysis. In Proceedings of the 2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Almaty, Kazakhstan, 10–13 September 2013; pp. 46–53.
99. Cheng, Y.; Gardner, M.T.; Li, J.; May, R.; Medhi, D.; Sterbenz, J.P. Analysing geopath diversity and improving routing performance in optical networks. *Comput. Netw.* **2015**, *82*, 50–67. [CrossRef]
100. De Sousa, A.; Santos, D.; Monteiro, P. Determination of the minimum cost pair of d-geodiverse paths. In Proceedings of the 13th International Conference Design of Reliable Communication Networks, Munich, Germany, 8–10 March 2017; pp. 1–8.
101. Wang, J.; Bigham, J.; Phillips, C. A geographical proximity aware multi-path routing mechanism for resilient networking. *IEEE Commun. Lett.* **2017**, *21*, 1533–1536. [CrossRef]
102. Jacobson, V. Congestion avoidance and control. *ACM SIGCOMM Comput. Commun. Rev.* **1988**, *18*, 314–329. [CrossRef]
103. Chiu, D.; Jain, R. Analysis of the increase and decrease algorithms for congestion avoidance in computer networks. *Comput. Netw. ISDN Syst.* **1989**, *17*, 1–14. [CrossRef]
104. Floyd, S.; Jacobson, V. Random early detection gateways for congestion avoidance. *IEEE/ACM Trans. Netw.* **1993**, *1*, 397–413. [CrossRef]
105. Brakmo, L.S.; O'Malley, S.W.; Peterson, L.L. *TCP Vegas: New Techniques for Congestion Detection and Avoidance*; ACM: London, UK, 1994.
106. Mathis, M.; Mahdavi, J. Forward acknowledgement: Refining TCP congestion control. *ACM SIGCOMM Comput. Commun. Rev.* **1996**, *26*, 281–291. [CrossRef]
107. Sisalem, D.; Schulzrinne, H. Congestion control in TCP: Performance of binary congestion notification enhanced TCP compared to Reno and Tahoe TCP. In Proceedings of the 1996 International Conference on Network Protocols, Columbus, OH, USA, 29 October–1 November 1996; pp. 268–275.
108. Stevens, W.; Paxson, V.; Allman, M. *TCP Congestion Control*; RFC 2581; IETF: Fremont, CA, USA, 1999.
109. Floyd, S.; Handley, M.; Padhye, J.; Widmer, J. Equation-based congestion control for unicast applications. *ACM SIGCOMM Comput. Commun. Rev.* **2000**, *30*, 43–56. [CrossRef]
110. Jin, C.; Wei, D.X.; Steven, H. Low FAST TCP: Motivation, Architecture, Algorithms, Performance. In Proceedings of the INFOCOM, Hong Kong, China, 7–11 March 2004.
111. Tang, A.; Wang, J.; Low, S.H. Understanding choke: Throughput and spatial characteristics. *IEEE/ACM Trans. Netw. (ToN)* **2004**, *12*, 694–707. [CrossRef]
112. Zulkifli, N.; Idrus, S.M.; Supa'at, A.S.M.; Farabi, M. Network performance improvement of all-optical networks through an algorithmic based dispersion management technique. *J. Netw. Syst. Manag.* **2012**, *20*, 401–416. [CrossRef]
113. Wu, J.; Zhang, J.; von Bochmann, G.; Savoie, M. Forward-looking wdm network reconfiguration with per-link congestion control. *J. Netw. Syst. Manag.* **2012**, *20*, 6–33. [CrossRef]

114. Wason, A.; Kaler, R. Blocking in wavelength-routed all-optical WDM networks. *Optik* **2010**, *121*, 903–907. [CrossRef]
115. Wason, A.; Kaler, R. Blocking probability calculation in wavelength-routed all-optical networks. *Optik* **2011**, *122*, 1638–1641. [CrossRef]
116. Wason, A.; Kaler, R. Blocking probability optimization in wavelength routed optical wdm networks. *Optik* **2013**, *124*, 3131–3133. [CrossRef]
117. Singal, A.; Kaler, R. Blocking probability of algorithms for different wavelength assignment in optical ring network. *Optik* **2013**, *124*, 147–151. [CrossRef]
118. Sohal, E.S.K.; Kaur, E.S. Blocking probability of dijkstra shortest and least congestion routing algorithm in wavelength-routed WDM network. *Int. J. Recent Innov. Trends Comput. Commun.* **2014**, *2*, 1374–1379.
119. Zanjani, S.B.; Rahbar, A.G. Least-congested distributed lightpath allocation. In Proceedings of the 2010 5th International Symposium on Telecommunications (IST), Tehran, Iran, 4-6 December 2010; pp. 151–156.
120. Stewart, M.F.; Kannan, R.; Dvir, A.; Krishnamachari, B. Caspar: Congestion avoidance shortest path routing for delay tolerant networks. In Proceedings of the IEEE 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, USA, 15–18 February 2016; pp. 1–5.
121. Hu, R.Q.; Hu, W.; Jin, M.; Qian, Y. Wavelength retuning without service interruption in an all-optical survivable network. *Int. J. Commun. Syst.* **2009**, *22*, 719–738. [CrossRef]
122. Hao, F.; Jansen, A.; Kodialam, M.; Lakshman, T.V. Path Computation for IP Network Optimization. Available online: https://insight.nokia.com/path-computation-ip-network-optimization (accessed on 25 November 2017).
123. Nasralla, Z.H.; El-Gorashi, T.E.; Musa, M.O.; Elmirghani, J.M. Routing post-disaster traffic floods in optical core networks. In Proceedings of the 2016 International Conference on Optical Network Design and Modeling (ONDM), Cartagena, Spain, 9–12 May 2016; pp. 1–5.
124. Thyagaturu, A.S.; Mercian, A.; McGarry, M.P.; Reisslein, M.; Kellerer, W. Software defined optical networks (SDONS): A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2738–2786. [CrossRef]
125. Fraustino, J.D.; Liu, B.; Jin, Y. *Social Media Use during Disasters: A Review of the Knowledge Base and Gaps*; National Consortium for the Study of Terrorism and Responses to Terrorism: College Park, MD, USA, 2012.
126. Ungerleider, N. *Why Your Phone Doesn't Work during Disasters—And How to Fix It*; Fast Company: Vineland, NJ, USA, 2013; Volume 17.
127. Baklan, P.; Yamori, K.; Tanaka, Y. Measure of user behaviour before and during disaster congestion. In Proceedings of the 2014 16th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 16–19 February 2014; pp. 135–140.
128. Fukuda, K.; Aoki, M.; Abe, S.; Ji, Y.; Koibuchi, M.; Nakamura, M.; Yamada, S.; Urushidani, S. Impact of tohoku earthquake on R&E network in Japan. In Proceedings of the Special Workshop on Internet and Disasters, Tokyo, Japan, 6–9 December 2011; p. 1.