Hindawi
Journal of Computer Networks and Communications
Volume 2018, Article ID 4134878, 13 pages
https://doi.org/10.1155/2018/4134878

Review Article

Network Restoration for Next-Generation Communication and Computing Networks

B. S. Awoyemi,[1] **A. S. Alfa**,[1,2] **and B. T. Maharaj**[1]

[1]*University of Pretoria, Pretoria, South Africa*
[2]*University of Manitoba, Winnipeg, MB, Canada R3T 2N2*

Correspondence should be addressed to B. S. Awoyemi; awoyemibabatunde@gmail.com

Received 8 January 2018; Revised 27 February 2018; Accepted 5 March 2018; Published 3 April 2018

Academic Editor: Ignacio Soto

Network failures are undesirable but inevitable occurrences for most modern communication and computing networks. A good network design must be robust enough to handle sudden failures, maintain traffic flow, and restore failed parts of the network within a permissible time frame, at the lowest cost achievable and with as little extra complexity in the network as possible. Emerging next-generation (xG) communication and computing networks such as fifth-generation networks, software-defined networks, and internet-of-things networks have promises of fast speeds, impressive data rates, and remarkable reliability. To achieve these promises, these complex and dynamic xG networks must be built with low failure possibilities, high network restoration capacity, and quick failure recovery capabilities. Hence, improved network restoration models have to be developed and incorporated in their design. In this paper, a comprehensive study on network restoration mechanisms that are being developed for addressing network failures in current and emerging xG networks is carried out. Open-ended problems are identified, while invaluable ideas for better adaptation of network restoration to evolving xG communication and computing paradigms are discussed.

1. Introduction

Current and emerging communication and computing networks are expected to provide high reliability by achieving near-instantaneous restoration in the event that one or more network elements fail. This requires that network restoration plans be put in place such that in the event of failures, the network can immediately adjust, regroup, and/or revert to an alternative arrangement, usually in terms of a reroute, to continue and complete the given communication task [1]. Hence, developing network restoration models to cater for sudden failures, thereby improving the efficiency and reliability of our telecommunications and computing networks, is an imperative. Network (or routing) restoration (or recovery) is the field that describes the design and implementation of appropriate mechanisms and/or models for achieving desirable network reliability by creating proper backup plans for networks in the event of preconceived or unexpected failures [2].

The main goal of network restoration is to seek to instantaneously make available new routes once one or more network elements (e.g., links or nodes) fail, thereby avoiding disruption to network traffic. The new routes are usually either computed immediately at the point of failure or are usually preplanned even before such failure occurs. Generally, in research works that involve developing appropriate network restoration mechanisms for protection against failures, several factors have to be put into consideration. The most important factors are the cost of network infrastructure, length of rerouting paths, amount of the total capacity that has to be reserved for restoration or recovery from failure, and the time taken to achieve such network restoration. The design goal is always to achieve optimal productivity for the network with as much less resource and cost as possible over the shortest amount of time. Network restoration models are built around this goal. The restoration capacity problem, for instance, is designed to place the minimum amount of spare capacity needed in the network to restore a part of lost connections [3].

Several works have been carried out and more works are still being done in addressing network restoration problems, particularly for communication and computing networks. This paper provides a comprehensive study on common failures types and peculiar restoration mechanisms that are being developed for addressing both current and newly evolving next-generation (xG) communication and computing network paradigms.

The main contributions of this paper are summarised thus:

(i) An up-to-date analysis of network restoration solutions that are being developed and applied for current and emerging communication and computing networks is carried out.

(ii) An exploration of the key aspects of network restoration for xG communication and computing networks that still require further investigations is carried out. Furthermore, invaluable insights on how such investigations can be successfully achieved based on the peculiarities and promises of xG communication and computing networks are provided.

The remainder of this paper is organised as follows: Section 2 describes different failure types in communication and computing networks, Section 3 establishes the categorisation of the various network restoration mechanisms for communication and computing networks, Sections 4 and 5 provide a review of network restoration models being employed for addressing failures in both current and emerging communication and computing networks, Section 6 discusses some examples of practical models of network restoration for emerging communication and computing networks, Section 7 gives some observations and future directions of network restoration for emerging networks, and finally, Section 8 provides the concluding remarks.

2. Failures in Communication and Computing Networks

Modern communication and computing networks are designed using network models. A network model is an interconnectivity of active devices, switches, equipment, and so on developed to drive telecommunication and computing needs. In simple description, the devices and other equipment that make up the network are represented as nodes, while the connections between them (either wired or wireless) are referred to as links. The direction in which data transmission flows or in which traffic is routed is called a path. Figure 1 gives a general depiction of a network model for a typical communication or computing network. The nodes are labelled from A to G. Two paths are indicated; P_1 is a path from A to G and P_2 is a path from A to D.

One shared experience for all communication and computing networks is the possibility and/or occurrence of network failures. A network failure can be defined as a forced temporary modification of a network, usually as a result of disruption to actual design of flow or traffic, which results in the capacity of certain links in the network to decrease, possibly to zero [4]. Network failures in communication and computing networks are broadly classified into the following categories:

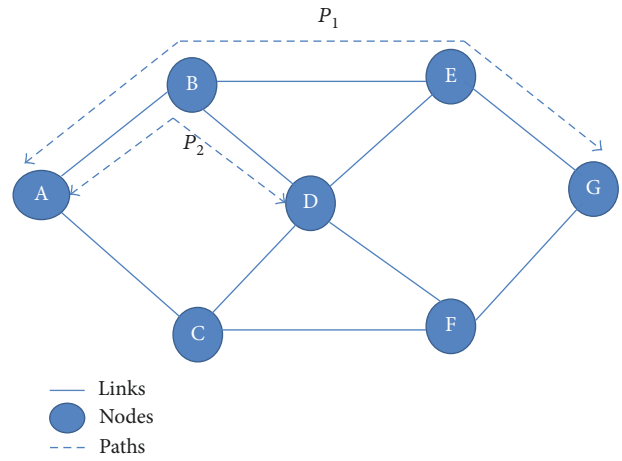

Figure 1: An architectural depiction of a communication or computing network model with 7 nodes, 10 links, and 2 paths shown.

(i) Link failures: a link failure occurs when a link component in a network fails [5]. Solving a link failure problem can be achieved by adding a new link or by redirecting and redistributing the traffic of the failed link to other still functional links with enough capacity to carry the additional traffic from the failed link.

(ii) Node failures: a node failure occurs due to the failure of an equipment at the nodes of the network such as a switch or a router [6]. A node failure can also be considered as the simultaneous failure of all the adjacent links to a node. One way of protecting against node failure is by installing alongside one or more redundant equipment that can immediately replace an active equipment acting as a node.

(iii) Single failures: a single failure occurs in a network when only one equipment, node, or link fails at a time [7]. To protect networks from single failures, network restoration models are developed to offer protection for individual or single elements in the network, with the assumption that multiple, near-simultaneous failures are a rare and/or improbable event.

(iv) Multiple failures: multiple failures in a network can occur when more than one equipment, node, or link fail at the same time [8]. To protect networks from multiple failures, network restoration models are developed to offer protection for two or more elements in the network, with the understanding that such multiple, near-simultaneous failures, though rare, are not entirely impossible occurrence(s).

Good communication and computing networks are designed to quickly restore networks to full activity and/or capacity when failures occur. In the next section, the various types of network restoration mechanisms designed to

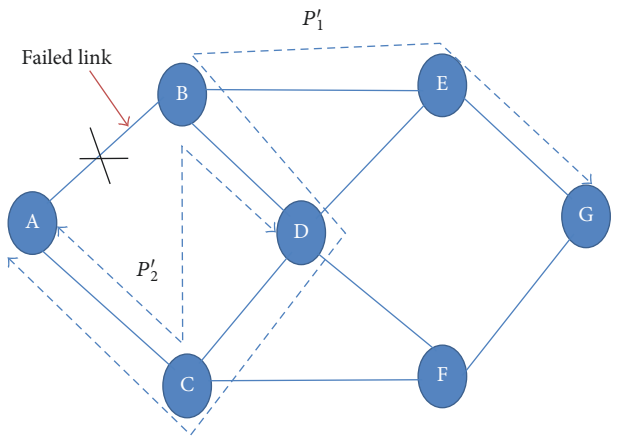

Figure 2: A depiction of a link failure and a corresponding line restoration.

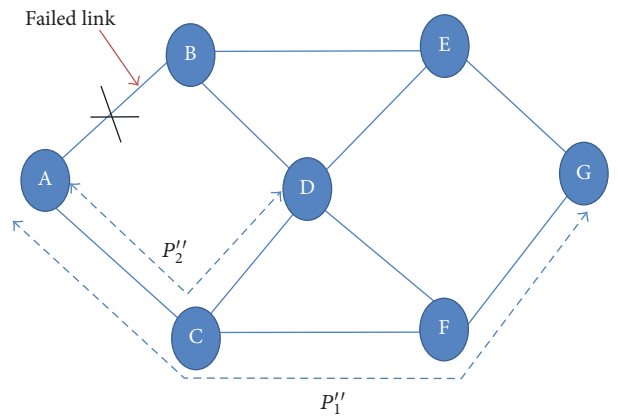

Figure 3: A depiction of a link failure and a corresponding path restoration.

address failures in modern communication and computing networks are discussed.

3. Types of Network Restoration for Communication and Computing Networks

Network restoration seeks to instantaneously find the best alternative route to transmit network traffic when a failure occurs. Network restoration in communication and computing networks can be classified into the following categories:

3.1. Line Restoration. In line restoration (also referred to as link restoration), the traffic carried on the failed link is rerouted from its tail node to its head node. Thus, the original route for traffic that uses the failed link is only slightly modified by replacing the failed link with an alternate route that connects its end nodes [9]. Usually, the end nodes of the failed link are made to participate in a distributed algorithm to dynamically discover a new route. The design of networks under line restoration requires limited information, that is, link loads and capacities, but it does not require source-destination traffic information. Moreover, restoration can be executed very quickly since there is no need to backtrack individual connections to their corresponding ingress nodes [10]. Figure 2 is a follow up on Figure 1 but now gives a pictorial representation of a link failure and a line restoration approach for recovering the network. In Figure 2, when link A-B fails, then

(i) link A-B is replaced by line A-C-D-B, and hence path P_1 is replaced with path P_1';

(ii) link A-B is replaced by line A-C-B, and hence path P_2 is replaced by P_2'.

3.2. Path Restoration. In path restoration, the traffic routed on a failed link is backtracked to its ingress nodes and new, perhaps totally disjoint, alternate routes are selected for restoring the traffic for all affected source-destination pairs. This implies that a completely new path is used as the alternate path [11]. Path restoration schemes have dedicated backup reserves (spares) that are used as backup routes for particular demands. Path restoration often requires less restoration capacity resources than line restoration at the expense of more complex signalling and larger execution time. Path restoration was employed in [12], for example, in providing adequate spare capacity in a telecommunications network environment. Figure 3 is a follow up on Figure 1 but now gives a pictorial representation of a link failure and a path restoration approach for recovering the network. In Figure 3, when link A-B fails, then

(i) path P_1 is replaced with path P_1'';

(ii) path P_2 is replaced by P_2''.

3.3. Reactive Restoration. In reactive restoration schemes, alternate routes are only calculated after the actual failure has occurred [13]. In these schemes, data packets are flooded into the network after the occurrence of failure to look for free capacity and to setup the new path. These restoration schemes are also referred to as real-time restoration approaches and they are mostly applicable in scenarios where traffic changes very frequently in the network.

3.4. Proactive Restoration. In proactive restoration schemes, alternate routes are always precalculated way before the failure happens. In the event of a failure, the connection is simply rerouted to the previously designed route [14]. These schemes are also called preplanned restoration approaches and are faster in execution than the reactive or real-time restoration approaches, even though they usually give poorer capacity utilisation than the real-time approaches.

Network restoration models are most often classified into the abovementioned categories. Generally, communication and computing networks are designed using either the centralised or the distributed architecture. In some instances, therefore, restoration mechanisms are usually classified based on these architectural representations.

3.5. Centralised Restoration. In centralised schemes, there is usually a central controller that performs computations and

sends information about the current state of the network as well as restoration decisions to all components of the network [15]. Centralised schemes are capacity efficient but have single points of failure. They may also have communication overhead and scalability issues.

3.6. Distributed Restoration. In distributed schemes, there is usually no central hub that directs network decisions and information dissemination but rather, individual components of the network are empowered to understand situations in the network and immediately make decisions to enhance network reliability and quick recovery after failures [16].

In the next two sections, we study the utilisation of the various types of network restoration mechanisms described in this section: first in current communication and computing networks, and then in emerging xG communication and computing networks.

4. Network Restoration in Current Communication and Computing Networks

In this section, a review of works in which the various types of network restoration have been developed and employed in addressing network failures in present-day communication and computing networks is carried out.

4.1. Path Restoration

4.1.1. Path Restoration for Teletraffic Networks. In [17], the authors developed a mathematical model for determining transmission network restoration capacity for wide area teletraffic networks. Two path restoration models were developed. The models were called connection-based restoration and load-directed restoration. The connection-based restoration model was designed to restore as many connections as possible in the transmission network for every affected or failed link based on the available built-in reconnection capacity. The idea behind the load-directed restoration model was to make even better use of the reconnection capacity depending on the time of failure, since loads vary from time to time in the course of the day. Network simulation showed that the load-directed approach outperformed the connection-based approach for network restoration when failure occurs in a dynamic call-routing teletraffic network.

The authors in [18] developed an on-line distributed multicommodity flow approximation algorithm for path restoration in circuit-switched telecommunication network. The restoration algorithm developed ran on a number of iterations. Each iteration consisted of two phases—an explore phase and a return phase. The explore phase was started by the source nodes of the disrupted paths. The return phase was started by the destination nodes of the disrupted paths. The return phase started after the explore phase ended. In the return phase, the paths traversed by the explore messages were retraced by the return messages. The return phase ended when the return messages have reached the sources. The return phase helped to resolve the contention for spare capacity in the network.

4.1.2. Path Restoration for Optical Communication Networks. In [19], the authors proposed an adjacent shortest cycle backup path as the restoration method whenever a link in an optical communication network using wavelength division multiplexing (WDM) fails. The shortest path was calculated using an ant colony optimisation algorithm. Adjacent cycles were updated using the restoration method developed. The authors established that the proposed method can survive link failure and theoretically provide better performance than existing restoration methods.

4.1.3. Path Restoration for Mesh Networks. In [20], the authors argued that dual-failure availability is an important metric for a reliable network where the restoration of all single failures is fully satisfied. Hence, an algorithm to evaluate network dual-failure availability for shared backup path protection mesh networks with the existing multiflow design model was developed. The authors created four network families, while each network family has eleven networks. From the algorithm developed, it was revealed that the values of network dual-failure availability increase first and then drops mildly when the average nodal degree of network increases.

4.1.4. Path Restoration for Computing Networks. In [21], the authors proposed the allocation of a backup path as a restoration model for failure in a computing network. The proposed model addressed the problem of the possibility of the backup path being disjoint from the original path at the Internet protocol or overlay layer but sharing the same physical links on the physical layer, meaning that if the failure occurred on the physical link, the failure could affect both the original and the backup paths simultaneously. The proposed solution was to find a route for the backup path that minimised the joint path failure probability between the original and the backup paths.

4.2. Line Restoration

4.2.1. Line Restoration for Teletraffic Networks. In [22], the authors developed network restoration models for scenarios where there is uncertainty in the traffic matrix (i.e., traffic demands can change on varying time scales) and the network topology is also dynamic (i.e., network topology can change when links fail). The models investigated included a restoration strategy that allowed the traffic to be arbitrarily rerouted in order to obtain an optimal utilisation on the modified network, a restoration strategy that is end-to-end and which allowed all affected flow paths to be arbitrarily rerouted and finally, a restoration strategy that reroutes only the affected flows by bypassing around the failed link rather than end-to-end. The models developed provided useful performance

Table 1: Summary of network restoration models employed in current communication and computing networks.

Number	Type of network restoration model	Type of failures addressed	Applicable networks	References
(1)	Path restoration, for example, shortest cycle backup path, minimal joint failure probability, and end-to-end restoration.	Link failures (single and multiple links) and node failures	Teletraffic networks, optical communication networks, mesh networks, and computing networks	[17–21]
(2)	Link (or line) restoration	Link failures (single or multiple failures) and node failures	Teletraffic networks	[22]
(3)	Proactive restoration, for example, connection-based and load-directed restoration models	Node failures and joint link failures	Optical communication networks and computing networks	[23, 24]
(4)	Reactive restoration	Link failures and node failures	Mesh networks	[25]

guarantees both on the original network and on the network after one or more links failed.

4.3. Proactive Restoration

4.3.1. Proactive Restoration for Optical Communication Networks. The authors in [23] considered the possibility of two links failing one after another in any given order in an optical WDM network and developed a restoration model for such occurrence. Three types of proactive restoration methods were developed and a heuristic was used to solve the recovery problems that ensued. A one hundred percent recovery from double link failures that occur immediately one after another was achieved with a slight increase in backup capacity.

4.3.2. Proactive Restoration for Computing Networks. The authors in [24] established the need for routing mechanisms which describes how information is transferred between network nodes for one computer to find another in a network. A route was explained as the sequence of network nodes through which it is possible to transmit information from source node to destination node. To increase reliability in a computer network, the restoration model must establish sufficiently fast routes on or before a failure is detected in the network device. Furthermore, once data cannot be transferred on the main route due to a failure, the source node must immediately switch to the backup route without it taking time on the calculation of a new route. The authors therefore proposed a proactive backup scheme of routes for dynamic changes in the structure and configuration of the network which allowed reducing the recalculation time of optimal routes and thereby increasing the efficiency of the routing mechanism.

4.4. Reactive Restoration

4.4.1. Reactive Restoration for Mesh Networks. The authors in [25] studied the relationship between failure localisation and the properties of available link restoration algorithms in a mesh network topology. From the study, it was discovered that the topological constraints on restoration paths required by algorithms that embed rings within mesh networks resulted in significant degradation in the ability to localise failures. Hence, the use of proactive restoration schemes, as opposed to reactive restoration, had a negative impact, although not as significant as the topological effect. Algorithms that make use of the mesh topology and dynamically route around existing failures using reactive restoration came close to an inherent limit imposed by the complexity of additional algorithmic advances.

Table 1 gives a summary of the various types of network restoration that are being developed and employed for protecting networks against failures in present-day communication and computing networks, as discussed in this section.

5. Network Restoration for Emerging Communication and Computing Networks

Network restoration models are currently being developed for emerging xG communication and computing paradigms. A review of works in which the various types of network restoration models have been developed and employed for addressing network failures in emerging xG technologies is carried out in the following subsections.

5.1. Path Restoration

5.1.1. Path Restoration for Software-Defined Networks. Software-defined networks (SDNs) are the immediate future of telecommunication networks [26]. In SDNs, the part that handles the decision-making process of network traffic (called the control plane) is separated from the part that transmits or relays the data traffic (called the data plane or physical plane) [27]. This makes it possible for intelligence to be carried out in the control plane, thereby easing network management while also enabling dynamic networks configuration. In [28], the authors developed a network failure recovery solution for software-defined optical networks using cognitive mechanisms for achieving the restoration. The authors established that SDN-based networks, in their architecture, enable administrators to simplify the network management and to efficiently detect network failure; hence, they are being considered for application in optical networks. The SDN-based solution developed had a centralised controller which allowed the network to make more efficient failure detection, effectively isolating the affected forwarding elements, and immediately remedying abnormal operations in optical networks.

5.1.2. Path Restoration for Wireless Sensor Networks. Wireless sensor networks (WSNs) are an example of an already developed technology but which is currently evolving for xG applications. Hence, network restoration for WSN is gaining attention. Particularly, occurrences of failure are more prominent in WSN than in most other communication technologies because of the adverse conditions in which those sensor nodes are deployed and for which they are intended to work. WSN nodes are also extremely resource-constrained. It is thus imperative to develop resourceful network restoration models for WSN. The authors in [29] developed a failure recovery model for WSN based on grade diffusion. The model also used the saved shortest path approach to figure out the best recovery path with minimal energy consumption for WSN. The grade diffusion method kept the sensors working for the longest period possible, thus increasing the lifetime of the network. The authors argued that the grade diffusion, enhanced by the shortest path approach which uses routing tables with saved shortest paths, was able to quickly identify faulty nodes and to recover the network in good time.

5.2. Line Restoration

5.2.1. Line Restoration for Mission-Critical or Emergency Networks. The authors in [30] developed a failure recovery model that deals with the problem of efficiently restoring sufficient resources in a communication network to support the demand of mission-critical services after a large-scale disruption like a natural disaster has occurred. The goal was to sufficiently recover the communication network infrastructure in the shortest time and with minimum interventions when massive disasters happen. The problem was modelled as a demand graph which takes into account the demand increase that occurs during such incidents. The graph defined a set of demand flows on the communication network of which a major disruption has made it unable to meet the capacity requirements of demand flows. The extra demand flows were to be accommodated by means of the recovery actions or by deploying new links and nodes. The recovery problem was developed as a mixed integer linear programming problem. The idea was to look for the best strategy that recovers the damaged infrastructure and deploys new links and nodes in order to minimise the cost of the recovery actions under the constraints on network capacity and demand flows satisfaction.

5.2.2. Line Restoration for Expansive Networks. In [31], the authors investigated a network recovery mechanism when a network has experienced massive failures from which recovery could take a long time and may involve several stages before the network can be fully back to its original state. The authors established that unlike in cases of minimal, predictable failures for which network can be quickly restored by preplanning redundant components and/or alternative paths, large-scale failures actually require gradual recovery of traffic. This can only be achieved by repairing failed components and reorganizing logical path connectivity over partial physical resources. It therefore has to be determined which physical components have to be repaired first and what logical paths should be reestablished over the partial recovered network components to realise a fast and effective restoration of traffic flow. The recovery model developed attempted to balance the requirement between maximising the total amount of traffic on all logical paths (i.e., the total network flow) and maximising traffic demand of each logical path. This problem was formulated as an optimisation problem and a heuristic algorithm called grouped-stage recovery (GSR) was introduced to solve the problem with a large number of damaged components in practical time.

5.3. Proactive Restoration

5.3.1. Proactive Restoration for Software-Defined Networks. The authors in [32] investigated a fast failure discovery and network recovery mechanism for dynamic networks using SDN. In the model, a central controller monitored the connectivity so that if a link got broken, the network is instantly reconfigured to restore the end-to-end connectivity for all paths and thus maintain connectivity between nodes. A failure detection scheme that used per-link bidirectional forwarding detection sessions was developed. The per-link detection was said to be better than per-path detection because it reduced detection time, decreased message complexity, and removed false-positive alarms. More so, its recovery time did not depend on the network size and path length. In the design, after detection of a failure, the controller selected a preconfigured backup path to restore the network. The proposed design was said to be a relatively simple way to reduce the recovery time in a dynamic network.

In [33], the authors developed a failure recovery model for data traffic in SDNs. In the model, a controller directs network flow around a failed link or node using preconfigured alternative paths. To significantly reduce recovery time, the developed model used virtual local area network tags to aggregate flow disruptions/failures, and based on the information gathered, a well-developed proactive recovery scheme was invoked to help recover the network from the failure.

The authors in [34] developed a failure recovery mechanism for a hybrid network where traditional Internet protocol routers coexisted and worked alongside SDN switches. In the recovery model, by redirecting traffic on a failed link to SDN switches through preconfigured Internet protocol tunnels, the proposed approach was able to react to failures very fast in order to guarantee traffic reachability in the presence of single link failures. Also, with the help of coordination among SDN switches, multiple backup paths were designed for the failure recovery. The proposed approach was said to avoid potential congestion in the post-recovery network by choosing proper backup paths.

5.3.2. Proactive Restoration for Fifth-Generation Networks. The design of fifth-generation (5G) wireless communication

networks is currently evolving very rapidly. 5G is the soon-to-be wireless communication standard. In [35], the authors established that in carrier cloud, which is one major tool for driving and achieving the goals of this newly developing 5G technology, service resilience could be heavily impacted by a failure of any network function that runs on a virtual machine. Hence, a framework was built which used efficient and proactive restoration mechanisms to ensure service resilience in carrier cloud. Two mechanisms were proposed; the first mechanism was based on bulk signalling whereby only one single message was created to replace a certain number of signalling messages in a bulk, while the second one created message profile which reduced the signalling message header by replacing repetitive information element by a profile identification. An analytical model based on Markov chain was used to evaluate the performance of the mechanisms developed.

5.3.3. Proactive Restoration for Internet-of-Things Networks. Internet-of-things (IoT) network is the emerging computer networking paradigm that makes the interaction between humans and nonhuman elements or objects more realistic and provides the connection among different existing networks. In [36], the authors argued that the current fault detection algorithms, usually designed for specified networks, are not suited for the complex communication environment of IoT, whose transmission is usually through hierarchical networks. Hence, a layered fault management scheme was proposed for IoT, with uniform observation points set around. In order to distinguish between the real fault and false alarm, fuzzy cognitive maps theory was introduced to setup the monitoring model. By adjusting the weighting rules in the model, it was possible for different observing points to achieve flexible judgement of the link failure risk in their authorities. After locating the fault roots, original recovery methods for individual networks were then employed to rescue the broken transmission.

5.3.4. Proactive Restoration for Dependency Networks. The authors in [37] investigated a recovery mechanism for networks in which, when a node fails, other neighbouring nodes that depend on such failed node are adversely affected and they could fail too. Such networks are called dependency networks. In dependency networks, the recovery of a node depends on the state of its dependent nodes. For this kind of networks, the dependency model is that the nodes depending on each other form a dependency group. This dependency group fails only when more than a certain fraction of nodes in the group fails. Obviously, in this model, there exists a fraction of nodes whose failure has no effect on the function of dependency of the group and the failed nodes can be recovered due to dependency relations among nodes. This recovery mechanism is referred to as dependency recovery mechanism. The authors therefore proposed a cascading process model to investigate the failure propagation of such dependency networks with a recovery mechanism. In the work, a fraction of network nodes was chosen randomly to form the dependency groups, while all the other nodes in the complementary fraction did not belong to any dependency group. By means of randomly removing a fraction of nodes and their links, the cascading failure on dependency networks was studied.

5.3.5. Proactive Restoration for Scalable Networks. In [38], the authors developed a coding-based failure recovery mechanism which used diversity coding to achieve quick network restoration over any type of arbitrarily large network. The authors established that coding-based recovery techniques improved capacity efficiency of proactive protection/restoration schemes by making the dedicated paths share the spare resources using coding operations. In the developed model, connection demands in each traffic vector were partitioned into coding groups and an advanced diversity coding technique was employed to achieve the recovery. It is also interesting to note that classical optimisation techniques (column generation and integer linear programming), and not the more generally used approach of developing heuristics, were used in solving the network restoration problem in this work.

5.4. Reactive Restoration

5.4.1. Reactive Restoration for Wireless Sensor Networks. In [39], the authors proposed a restoration method to deal with the failure of an articulation node (a node whose failure may result in the network being broken into different segments that are isolated from each other) in a multichannel WSN scenario. The problem was formulated as a multiobjective optimisation problem. In the centralised solution approach developed, the sink carried out the entire recovery procedure from failure detection to the reallocation of channels after the connectivity has been restored. The recovery solution developed used graph theory heuristics such as graph colouring and Steiner points to rearrange the nodes around the failed node and to recover from the network partitioning and restore network connectivity.

The authors in [40] proposed an energy-efficient failure recovery scheme for WSN. The model used a coverage preserving failure recovery mechanism to achieve energy-efficient network restoration when failure occurs. The authors argued that the proposed scheme was able to diagnose failures with very low false alarming rate and was also able to recover failures by maintaining coverage above a given acceptable threshold value.

5.4.2. Reactive Restoration for Fifth-Generation Networks. In [41], the authors proposed that 5G would have baseband units that are connected to remote radio heads via high-speed fronthaul links. Hence, failure of any 5G cell site fronthaul would imply the loss of hundreds of gigabits or even terabits of data. The authors therefore presented a novel cell outage compensation approach using new self-healing radios added to each cell site in the 5G network. The self-healing radios are being designed to operate only in cases of fronthaul/backhaul failures of any cell site in the network.

Table 2: Summary of network restoration models employed in emerging xG communication and computing networks.

Number	Type of network restoration model	Type of failures addressed	Applicable networks	References
(1)	Path restoration	Link and node failures, single and multiple links failures	Software-defined networks, wireless sensor networks	[26–29]
(2)	Link (or line) restoration	Link and node failures , single and multiple links failures	Mission-critical or emergency networks, expansive networks	[30, 31]
(3)	Proactive restoration	Link and node failures, single and multiple links failures	Software-defined networks, fifth-generation networks, internet-of-things networks, dependency networks, scalable networks	[32–38]
(4)	Reactive restoration	Link and node failures, single and multiple links failures	Wireless sensor networks, fifth-generation networks, internet-of-things networks	[39–43]

The authors then developed a new software-defined controller to handle the self-healing procedures. Finally, a high-level simulation study was carried out to assess the proposed approach. The simulation results confirmed the advantages of the proposed approach in terms of the degree of recovery from failures.

5.4.3. Reactive Restoration for Internet-of-Things Networks. In [42], the authors addressed the reliability of IoT under emergency situations. The authors argued that the reliability of IoT under such emergency or crisis situations could only be guaranteed when the network is self-adaptive and resilient to errors by providing efficient mechanisms for information distribution, especially in the multihop scenario. The restoration mechanism developed to achieve this reliability used the implicit acknowledgements that objects in the network usually receive to detect transmission errors. The mechanism then used a routing metric to designate the best link, thus minimising packet loss probability.

The authors in [43] developed a distributed and dynamic fault-tolerant mechanism for IoT whereby an object with a failed service could be taken over by another service peer without the involvement of other users, including developers and installers. The restoration mechanism used strips to store a list of duplicated services, with each service peer maintaining a consistent view of duplicated services in the strip. In combination with the heartbeat protocol, recovery from failure was achieved by manipulating strips in a distributed manner, and results obtained showed that failures could be recovered within few seconds without administrator or developers in the loop.

Table 2 gives a summary of the various types of network restoration that are being developed and employed for protecting networks against failures in emerging xG communication and computing networks, as discussed in this section.

6. Practical Examples of Network Restoration for Emerging Communication and Computing Networks

In this section, two practical examples where network restoration models have been employed for addressing failures in emerging xG communication networks are discussed. The first example describes a link failure scenario with a proactive restoration plan being designed to restore the network. The second example describes a node failure scenario with a reactive restoration plan being developed to achieve the network restoration.

6.1. An Example of Link Failure with Proactive Restoration Plan. The link failure recovery plan understudied in this section is the work carried out in [33]. The work is chosen because it describes a good model of link failure recovery in xG communication using an SDN platform. The outstanding characteristics of SDN that makes it a preferred network for the immediate future were highlighted as follows: SDN makes use of a centralised network intelligence platform, SDN separates its network data from its control planes, and finally, SDN abstracts network infrastructure from it general applications. In the developed network restoration model of [33], the goal was to investigate how SDN can be deployed for very high network reliability communication prototypes (otherwise referred to as carrier-grade networks (CGNs)). Failures at the data plane were introduced in the form of link or switch failures which could result in problems such as network instability, degrading quality of service, and packet loss. The aim of the proactive scheme developed was to achieve recovery without overwhelming the network with control traffic and dependence on the controller. The developed scheme relied on the protection mechanism to achieve rapid recovery of the data plane failures. Alternate backup paths were preconfigured for every link. Virtual local area network (VLAN) tagging was used to aggregate disrupted flows. The proactive scheme effectively reduced the dependence on the controller. The recovery scheme investigated is represented in a pictorial form in Figure 4.

In the model presented in Figure 4, nodes (switches) A, B, C, D, E, and F are interconnected through links AE, AB, AF, and so on. If one of the nodes or links (e.g., switch B or link AB in Figure 4) fails, switch A detects the failure, tags the flows with the ID of failed core switch, and autonomously detours the two disrupted flows from link AB to their destined 2-hop neighbours via the preconfigured alternate paths. The VLAN ID field of the detoured packets of various disrupted flows is matched against the preconfigured

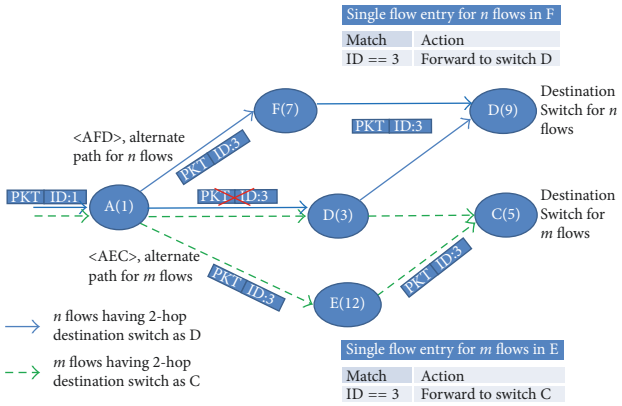

FIGURE 4: Link failure recovery model for SDN [33].

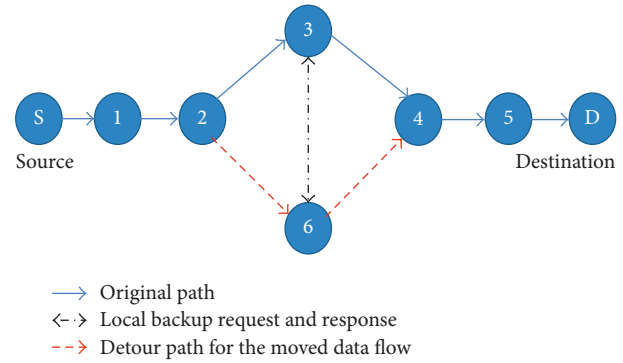

FIGURE 5: An illustration of local traffic distribution for node failure recovery model in MCWNs [44].

alternate path flow rules from switch F which then forwards the packets to the alternate path's next switch. All the preconfigured alternate paths are identified by a unique identifier of the network component (core switch or an edge link) that it is protecting. In the case of a failure, the detoured flows on the alternate path are matched against the identifier of the failed network component and forwarded to the next switch of the backup path or destination 2-hop neighbour of the detour switch.

The developed model was experimented using the xG backbone network topology being developed by AT&T. The network contained 25 switches and 52 links with virtualised rings on the Mininet virtualisation environment. In the experiment, the total recovery time for the developed recovery scheme was calculated by varying the number of flow rules to recover. The aim was to study the total time required to recover from a core network component and edge link failure. Additionally, the experiment was carried out to examine the effect of a number of disrupted flows on the overall recovery time. The failure was triggered by shutting down a switch while the flows passing through it were rerouted to achieve the recovery. The overall failure recovery time was calculated as a time difference between the time that the last disrupted flow occurred and the time in which it was successfully detoured after each failure. The disrupted flows were aggregated into one single flow. With this single group entry modification, it was possible to redirect all disrupted flows to the backup path. The results obtained showed that with the proactive plan, the recovery time was completely unaffected by the number of disrupted flows. Furthermore, the recovery scheme successfully achieved the failure recovery of about 3-4 ms, which means that it successfully fulfilled the carrier-grade recovery requirement of 50 ms time interval.

6.2. An Example of Node Failure with Reactive Restoration Plan. The reference work for this example is [44]. It is a good example of how to address node failure in broadly general xG communications. The xG communication network that was employed in the work is called multichannel wireless networks (MCWNs). In MCWNs, wireless nodes are equipped with multiple wireless network cards or radios to take the advantage of channel diversity. This makes MCWNs very useful in emerging technologies such as WSNs, IoT, and 5G because end-users are enabled to access the Internet at a low cost, with ease of deployment and configuration and flexibility of construction. The model investigated in [44] developed a recovery (backup) scheme that improved the robustness of MCWNs against random failures. At its core, the scheme was equipped with a local traffic load redistribution scheme that identified local traffic load changes in order to maximise the recovery possibility while also minimising the possibility of congestion generation.

In the model developed in [44], the recovery scheme searches for feasible local-to-end rerouting plans which generate new paths to avoid the faulty area, based on any given routing and channel assignment algorithm. Then, by considering current network settings as constraints, the scheme redistributes the traffic load in the local area to satisfy the quality of service requirement of each data flow. In the design for an efficient node failure backup scheme, the aim is to fully explore the capacity of the surviving network components in order to find new paths that do not overload the neighbours of the failed node which reduces the probability of generating congestion. The backup process involves failure testing/identification, deciding feasible routing plan, satisfying quality of service requirements, local traffic redistribution, and backup decision. An illustration of the local traffic distribution is provided in Figure 5.

In the analysis of the model, the achievable capacity (or throughput) of each link is affected by two factors—transmission capacity and channel occupancy ratio (COR). When a single link uses the entire capacity, COR is represented by α_i^r which was given as

$$\alpha_i^r = \frac{L_i^r}{\tau_i^r}, \tag{1}$$

while the aggregated COR when multiple links share the capacity of one channel, represented by β_i^r, was given as

$$\beta_i^r = \sum_j \left(\frac{L_j^r}{\tau_j^r}\right) \quad j = 1, 2, \ldots, \tag{2}$$

where L_i^r is the traffic load on radio r of router $v_i$and τ_i^r is the transmission capacity on radio r of router v_i. The achievable link capacity C_i^r was therefore

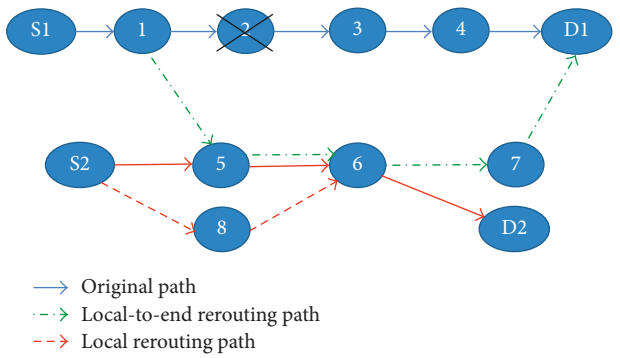

Figure 6: Solution approach for node failure recovery in WSN [44].

$$C_i^r = \left(1 - \beta_i^r\right) \times \tau_i^r. \quad (3)$$

If the achievable capacity of the neighbour node C_i^r was enough for the requested backup stream C_{req} (i.e., if $C_{\text{req}} < C_i^r$), it accepts the backup stream. Otherwise, the local traffic redistribution will be triggered. In that case, a new capacity $C_i^{r'}$ was calculated thus:

$$C_i^{r'} = C_i^r + \left(R_i\right)^{(-l)} \times L_i^r, \quad (4)$$

where l is the level parameter and R_i is the number of radios of the node. If $C_i^{r'} > C_{\text{req}}$ and satisfied quality of service requirements, backup stream was accepted. Otherwise, the backup stream was dropped. After all the backup paths for the affected data flows have been built or refused, the backup process stops. This process is illustrated in Figure 6.

7. Observations and Future Directions for Network Restoration Solutions

From the study on failures and network restoration for current and emerging communication and computing networks, the following general observations are made:

(1) From the review of current literature on network restoration, it is observed that a lot more work has been done on link failure detection and restoration than on node failure detection and restoration, especially for emerging xG communication and computing networks. The reason for this, it seems, is that link failures are a lot easier to understand and analyse. Hence, it is easier to study and develop restoration models for link failures than for node failures. However, exploring node failure problems and developing restoration models for them are equally critical for emerging communication and computing networks. Therefore, a lot more attention has to be dedicated to addressing node failures, especially in xG communication and computing networks.

(2) It is also observed that most of the network restoration problems have been solved by the use of heuristics. While this, in itself, is not a bad idea, solutions through heuristics may not always be the best because they are usually problem-specific, suboptimal, and nontransferable. In other words, since heuristics are usually only based on logical reasoning and not on numerical or analytical basis, they therefore cannot be easily transferred to solving other problems or addressing similar or not-so-similar failure recovery problems. A lot more work has to be done in developing optimal, practicable, and transferable solutions for the failure and network restoration problems in xG communication and computing networks.

From the study and observations already provided, it is clear that there are some aspects of network restoration for emerging xG communication and computing networks that still require further investigation, if the expectations and promises of xG technologies are to be fully realised. The most important areas of network restoration that still requires further studies are highlighted.

7.1. Specific Adaptation of Network Restoration to WSN. While modern WSN is an integral part of emerging xG communication and computing networks, it has its own peculiar characteristics that network restoration can exploit. For instance, a good WSN design can still be effective even when a number of nodes have failed, as compared to most other emerging network paradigms where a single node failure may be catastrophic, and could possibly result in the near collapse of the entire system. More so, in modern WSN designs, some nodes are deliberately put to sleep in order to conserve energy and battery life. This, in some way, may be viewed as those nodes "failing," even though these sleeping nodes have not failed in reality and can still be employed in the network at some later time frame. Another important aspect of WSN is the speed with which data have to be transmitted, especially for xG networks such as in IoT applications. It is imperative therefore to develop network restoration models that specifically identify the peculiarities of WSN and that are built to cater for such peculiarities in their adaptation to and application for IoT and other xG network designs. The authors are currently working on some new network restoration models for practical WSN applications in IoT and other similar xG networks.

7.2. Need for Improved Network Restoration Models That Address Emerging xG Communication and Computing Peculiarities. xG communication and computing prototypes have high promises in terms of speed, reliability, coverage, and so on that would require the application of high-speed failure detection, isolation, and network restoration models for them to be adequately equipped to achieve their goals. Even though research work in this regard is currently on-going, as already established in this study, it is still very inadequate. There are lots of research gaps that still need to be filled, open-ended problems that are still up for investigation, and practical issues (such as scalability and computational complexity) that still require to be addressed. Therefore, there is need for more research work on network restoration for emerging xG communication and computing technologies if the research gaps are to be filled.

7.3. Experimental Implementation of Network Restoration Models in Emerging Technologies. Most recent works on network restoration for emerging xG technologies are still focussed on mathematical and simulation modelling and not on actual implementation of the ideas and models being developed, whether on experimental or deployment basis. The reason construed for this is that many of these emerging xG technologies are themselves still in their early stages of development and fine-tuning, making it difficult to find actual test-beds or experimental models for carrying out the necessary experimentation on network restoration. What we believe can be done in this regard is to create opportunities to implement the network restoration models being developed alongside the experimental developments for these emerging technologies as much and as quickly as possible.

7.4. Developing xG Network Restoration Models for Reliable Disaster Management and Emergency Services. The expectation of remarkable interconnectivity, fast speed, high data rates, wide coverage, and so on that xG networks promise is also its major albatross in case of large-scale disasters and emergency needs. This is because, the impact of such disasters on the network can be extreme, leading to massive numbers of equipment, nodes, links, and so on failing simultaneously. It is important to develop network restoration strategies for emerging xG networks that can provide an acceptable level of reliability and survivability of the network in times of network disruptions as a result of sudden colossal disasters, either natural or man-made.

7.5. Improving Network Security of Emerging Technologies through Network Restoration. One important aspect of emerging xG networks where network restoration can be very useful is in improving network security. A good example is the use of network restoration in tracking down malicious activities by intruders or detecting compromised elements in a network. In such a case, by developing and incorporating the right network restoration models in the system, the activities of malicious nodes can be minimised, if not completely eliminated. More so, reports provided through the network restoration models can be used in identifying and isolating already compromised nodes. However, not much work has been done in this regard yet, making it an important area for active research.

8. Conclusion

Current and emerging xG communication and computing networks, in their design, must be robust against failures and be built with swift network restoration capacities in order to achieve their promises in terms of capacity, latency, speed, and so on. While failures are inevitable, it is important to study existing network restoration models so as to discern the applicability of these models to both present and emerging technology paradigms. In this study, the most impressive network restoration types and models that have been and/or are being developed for recent and xG communication and computing technologies are identified, with their properties and proficiencies also investigated. Important observations on network restoration for xG communication and computing networks are made, and suggestions on improvement and practical adaptation are discussed. Finally, directions for further work in the area of developing network restoration models that meet the needs and peculiarities of emerging xG communication and computing networks are provided.

Conflicts of Interest

The authors declare that there are no conflicts of interest for this paper.

Acknowledgments

This research is funded by the Advanced Sensor Networks SARChI Chair program, cohosted by the University of Pretoria (UP) and Council for Scientific and Industrial Research (CSIR), through the National Research Foundation (NRF) of South Africa.

References

[1] W. Lau and S. Jha, "Failure-oriented path restoration algorithm for survivable networks," *IEEE Transactions on Network and Service Management*, vol. 1, no. 1, pp. 11–20, 2004.

[2] R. Dighe, Q. Ren, and B. Sengupta, "A link based alternative routing scheme for network restoration under failure," in *Proceedings of the Global Telecommunications Conference*, vol. 3, pp. 2118–2123, Singapore, November 1995.

[3] G. Shen and W. Grover, "Capacity requirements for network recovery from node failure with dynamic path restoration," in *Proceedings of the OFC 2003 Optical Fiber Communications Conference*, pp. 775–777, Atlanta, GA, USA, March 2003.

[4] P. H. Franklin, I. Tavrovsky, and R. Ames, "A strategy for optimal management of spares," in *Proceedings of the 2016 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–6, Reno, NV, USA, January 2016.

[5] X. Zhang and Z. Zhang, "Link fault identification using dependent failure in wireless communication networks," *Electronics Letters*, vol. 52, no. 2, pp. 163–165, 2016.

[6] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "On the impact of node failures and unreliable communications in dense sensor networks," *IEEE Transactions on Signal Processing*, vol. 56, no. 6, pp. 2535–2546, 2008.

[7] W. Grote, A. Arenas, and A. Zapata, "Netfailpac: a single failure protection algorithm with QoS provision for optical WDM networks," in *Proceedings of the Third International Conference on Systems (icons 2008)*, pp. 226–229, Cancun, Mexico, April 2008.

[8] S. Yin, S. Huang, B. Guo et al., "Shared-protection survivable multipath scheme in flexible-grid optical networks against multiple failures," *Journal of Lightwave Technology*, vol. 35, no. 2, pp. 201–211, 2017.

[9] R. Shenai, C. Maciocco, M. Mishra, and K. Sivalingam, "Threshold based selective link restoration for optical wdm mesh networks," in *Proceedings of the Fourth International Workshop on Design of Reliable Communication Networks, 2003 (DRCN 2003)*, pp. 31–38, Banff, AB, Canada, October 2003.

[10] H. Luss and R. T. Wong, "Survivable telecommunications network design under different types of failures," *IEEE*

Transactions on Systems, Man, and Cybernetics–Part A: Systems and Humans, vol. 34, no. 4, pp. 521–530, 2004.

[11] S. Hegde, S. G. Koolagudi, and S. Bhattacharya, "Path restoration in source routed software defined networks," in *Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 720–725, Milan, Italy, July 2017.

[12] J. Veerasamy, S. Venkatesan, and J. C. Shah, "Spare capacity assignment in telecom networks using path restoration," in *Proceedings of the 3rd Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS '95)*, pp. 370–374, Durham, NC, USA, January 1995.

[13] N. Haider, M. Imran, N. M. Saad, and M. A. Zakariya, "Performance analysis of reactive connectivity restoration algorithms for wireless sensor and actor networks," in *Proceedings of the 2013 IEEE 11th Malaysia International Conference on Communications (MICC)*, pp. 490–495, Kuala Lumpur, Malaysia, November 2013.

[14] M. Dzida, M. Zagozdzon, M. Zotkiewicz, and M. Pioro, "Flow optimization in ip networks with fast proactive recovery," in *Proceedings of the Networks 2008-The 13th International Telecommunications Network Strategy and Planning Symposium*, pp. 1–15, Budapest, Hungary, September 2008.

[15] J. Perell, S. Spadaro, F. Agraz et al., "Experimental evaluation of centralized failure restoration in a dynamic impairment-aware all-optical network," in *Proceedings of the 2011 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference*, pp. 1–3, Piscataway, NJ, USA, March 2011.

[16] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed restoration path selection for shared mesh restoration," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 761–771, 2003.

[17] D. Medhi and R. Khurana, "Optimization and performance of network restoration schemes for wide-area teletraffic networks," *Journal of Network and Systems Manangement*, vol. 3, no. 3, pp. 265–294, 1995.

[18] S. Venkatesan, M. Patel, and N. Mittal, "A distributed algorithm for path restoration in circuit switched communication networks," in *Proceedings of the 24th IEEE Symposium on Reliable Distributed Systems (SRDS'05)*, pp. 226–235, Orlando, FL, USA, October 2005.

[19] Mallika and N. Mohan, "Link failure recovery in WDM networks," *International Journal of Computer Science and Electronics Engineering*, vol. 1, no. 5, pp. 1–4, 2013.

[20] W. Wang and J. Doucette, "Dual-failure availability analysis for multi-flow shared backup path protected mesh networks," in *Proceedings of the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pp. 127–133, Halmstad, Sweden, September 2016.

[21] W. Cui, I. Stoica, and R. H. Katz, "Backup path allocation based on a correlated link failure probability model in overlay networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*, pp. 236–245, Paris, France, November 2002.

[22] D. Applegate, L. Breslau, and E. Cohen, "Coping with network failures: routing strategies for optimal demand oblivious restoration," *ACM SIGMETRICS Performance Evaluation Review*, vol. 32, no. 1, pp. 270–281, 2004.

[23] H. Choi, S. Subramaniam, and H.-A. Choi, "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*, vol. 2, pp. 808–816, New York, NY, USA, June 2002.

[24] P. D. Alexandrovich and T. I. Yurievich, "Proactive backup scheme of routes in distributed computer networks," in *Proceedings of the 2016 International Siberian Conference on Control and Communications (SIBCON)*, pp. 1–4, Moscow, Russia, May 2016.

[25] S. S. Lumetta and M. Medard, "Towards a deeper understanding of link restoration algorithms for mesh networks," in *Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213)*, vol. 1, pp. 367–375, Anchorage, AK, USA, April 2001.

[26] F. Hao, M. Kodialam, and T. V. Lakshman, "Optimizing restoration with segment routing," in *Proceedings of the IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, San Francisco, CA, USA, April 2016.

[27] A. Ghannami and C. Shao, "Efficient fast recovery mechanism in software-defined networks: multipath routing approach," in *Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 432–435, Barcelona, Spain, December 2016.

[28] X. Zhang, W. Hou, L. Guo, S. Wang, Y. Sun, and X. Yang, "Failure recovery solutions using cognitive mechanisms for software defined optical networks," in *Proceedings of the 2016 15th International Conference on Optical Communications and Networks (ICOCN)*, pp. 1–3, Hangzhou, China, September 2016.

[29] S. Abuelenin, S. Dawood, and A. Atwan, "Enhancing failure recovery in wireless sensor network based on grade diffusion," in *Proceedings of the 2016 11th International Conference on Computer Engineering Systems (ICCES)*, pp. 334–339, Cairo, Egypt, December 2016.

[30] N. Bartolini, S. Ciavarella, T. F. L. Porta, and S. Silvestri, "Network recovery after massive failures," in *Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 97–108, Toulouse, France, June 2016.

[31] K. Genda and S. Kamamura, "Multi-stage network recovery considering traffic demand after a large-scale failure," in *Proceedings of the 2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, Kuala Lumpur, Malaysia, May 2016.

[32] R. Ahmed, E. Alfaki, and M. Nawari, "Fast failure detection and recovery mechanism for dynamic networks using software-defined networking," in *Proceedings of the 2016 Conference of Basic Sciences and Engineering Studies (SGCAC)*, pp. 167–170, Khartoum, Sudan, February 2016.

[33] P. Thorat, R. Challa, S. M. Raza, D. S. Kim, and H. Choo, "Proactive failure recovery scheme for data traffic in software defined networks," in *Proceedings of the 2016 IEEE NetSoft Conference and Workshops (NetSoft)*, pp. 219–225, Seoul, Republic of Korea, June 2016.

[34] C. Y. Chu, K. Xi, M. Luo, and H. J. Chao, "Congestion-aware single link failure recovery in hybrid SDN networks," in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 1086–1094, Hong Kong, China, April 2015.

[35] T. Taleb, A. Ksentini, and B. Sericola, "On service resilience in cloud-native 5G mobile systems," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 483–496, 2016.

[36] X. Li, H. Ji, and Y. Li, "Layered fault management scheme for end-to-end transmission in internet of things," in *Proceedings of the 2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, pp. 1021–1025, Harbin, China, August 2011.

[37] Y. N. Bai, N. Huang, L. N. Sun, and Y. Zhang, "Failure propagation of dependency networks with recovery mechanism," in *Proceedings of the 2017 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–6, Orlando, FL, USA, January 2017.

[38] S. N. Avci and E. Ayanoglu, "Link failure recovery over large arbitrary networks: the case of coding," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1726–1740, 2015.

[39] S. Chouikhi, I. E. Korbi, Y. Ghamri-Doudane, and L. A. Saidane, "Articulation node failure recovery for multi-channel wireless sensor networks," in *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, San Diego, CA, USA, December 2015.

[40] K. P. Sharma and T. P. Sharma, "CPFR: coverage preserving failure recovery in wireless sensor networks," in *Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications*, pp. 284–289, Ghaziabad, India, March 2015.

[41] M. Selim, A. E. Kamal, K. Elsayed, H. M. Abdel-Atty, and M. Alnuem, "Fronthaul cell outage compensation for 5G networks," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 169–175, 2016.

[42] N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, "Reliability for emergency applications in internet of things," in *Proceedings of the 2013 IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 361–366, Cambridge, MA, USA, May 2013.

[43] P. H. Su, C. S. Shih, J. Y. J. Hsu, K. J. Lin, and Y. C. Wang, "Decentralized fault tolerance mechanism for intelligent IoT/M2M middleware," in *Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 45–50, Seoul, Republic of Korea, March 2014.

[44] P. Sun and N. Samaan, "Random node failures and wireless networks connectivity: a novel recovery scheme," in *Proceedings of the 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–6, Vancouver, BC, Canada, May 2016.