International Journal of Engineering Technologies and Management Research
December 2025 12(12)
www.ijetmr.com

Original Article

ALGORITHM APPROACHES FOR MINIMAL OPERATION BACKWARD ERROR RECOVERY IN DYNAMIC NETWORK TOPOLOGIES

Aasifa Arabi [1*], **Dr. Nilesh Bhosle** [2]
[1] Research Scholar, India
[2] Research Guide and Associate Professor, Department of Computing, Artificial Intelligence and Machine Learning, NIMS Institute of Computing, Artificial Intelligence and Machine Learning, NIMS University, Rajasthan, Jaipur, India

ABSTRACT

Network survivability is a crucial requirement in high-speed optical networks. Typical approaches of providing survivability have considered the failure of a single component such as a link or a node. In this paper, we consider a failure model in which any two links in the network may fail in an arbitrary order. Three loopback methods of recovering from double-link failures are presented. The first two methods require the identification of the failed links, while the third one does not. However, pre computing the backup paths for the third method is more difficult than for the first two. A heuristic algorithm that pre-computes backup paths for links is presented. Numerical results comparing the performance of our algorithm with other approaches suggests that it is possible to achieve recovery from double-link failures with a modest increase in backup capacity. Current means of providing loop-back recovery, which is widely used in SONET, rely on ring topologies, or on overlaying logical ring topologies upon physical meshes. Loop-back is desirable to provide rapid preplanned recovery of link or node failures in a bandwidth-efficient distributed manner. We introduce generalized loop-back, a novel scheme for performing loop-back in optical mesh networks. We present an algorithm to perform recovery for link failure and one to perform generalized loop-back recovery for node failure. We illustrate the operation of both algorithms, prove their validity, and present a network management protocol algorithm, which enables distributed operation for link or node failure. We present three different applications of generalized loop-back. First, we present heuristic algorithms for selecting recovery graphs, which maintain short maximum and average lengths of recovery paths. Second, we present WDM-based loop-back recovery for optical networks where wavelengths are used to back up other wavelengths. We compare, for WDM-based loop-back, the operation of generalized loop-back operation with known ring-based ways of providing loop- back recovery over mesh networks. Finally, we introduce the use of generalized loop-back to provide recovery in a way that allows dynamic choice of routes over preplanned directions.

Keywords: WDM, Loop-Back, Network Restoration, Mesh Networks.

INTRODUCTION

THE explosive growth of the Internet has fueled intensive research on high-speed optical networks based on wavelength division multiplexing (WDM) technology. WDM technology harnesses the large bandwidth of the optical fiber, which is of the order of several Terabits/s into a few tens of wavelengths, each of which can be operated at electronic rates of a few Gb/s. Point- to-point WDM links with several tens of wavelengths have been deployed by carrier networks. Recent advances in optical routing and switching are

*Corresponding Author:
Email address: Aasifa Arabi (aasifaarabi99@gmail.com), Dr. Nilesh Bhosle (nilesh.bhosle@nimsuniversity.org)

Received: 06 October 2025; **Accepted:** 23 November 2025; **Published** 17 December 2025
DOI: 10.29121/ijetmr.v12.i12.2025.1721
Page Number: 38-46
Journal Title: International Journal of Engineering Technologies and Management Research
Journal Abbreviation: Int. J. Eng. Tech. Mgmt. Res.
Online ISSN: 2454-1907
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

enabling the transition from point-to-point optical WDM links to true optical networking by performing optical routing. In this technique called as wavelength routing, wavelengths can be independently routed from an input port to an output port. With the potential development of optical switches that are capable of dynamically reconfiguring the routing pattern under electronic control, the flexibility provided by the network is dramatically increased. In a dynamically configurable wavelength-routing network, lightpaths or all-optical circuit-switched paths can be provided on a demand basis, depending on traffic requirements. As wavelength-routing paves the way for network throughputs of possibly hundreds of Tb/s, network survivability assumes critical importance. A short network outage can lead to data losses of the order of several gigabits. Hence, protection or dedicating spare resources in anticipation of faults, and rapid restoration of traffic upon detection of a fault are becoming increasingly important. According to Brown et al. (1994), the overall availability requirements are of the order of percent or higher. Survivability is the ability of the network to withstand equipment and link failures. There are several kinds of failures that can disrupt the light path service provided by the optical network. Link failures occur because of fiber cuts that are mostly due to backhoe accidents. Such cuts typically result in all fibers in the bundle to be cut and hence a link failure could lead the failure of hundreds of channels, and therefore need elaborate restoration mechanisms. Node failures occur due to the failure of equipment at nodes such as switches. These equipment are typically protected within the node by redundant equipment (including redundant switches) Doverspike and Wilson (1994). The other type of failure is a channel failure in which the equipment on a single wavelength channel such as transmitter or receiver fails. These failures cause a single light path to fail and typically do not affect the other light paths. In order to recover from channel failures, spare transmitting and receiving equipment must be available at the source and destination nodes. In this paper, we restrict ourselves to the case of link failures. Traditional optical networks have tended to take the form of point-to-point WDM transmission links or rings. Well-known protection mechanisms such as 1+1 and 1:1 protection Ellinas and Stern (1996) are used for point- to-point links. There are two kinds of protection schemes for other networks: link protection and path protection. In link protection, an alternate light path (called as a backup light path) between the end points of each link is pre-computed. Upon the link's failure, all the lightpaths using the link (called as working lightpaths) are switched at the end-nodes of the link to their corresponding backup lightpaths. The portion of the working lightpaths excluding the failed link remains the same. In contrast, path protection entails the rerouting of all working lightpaths that use the failed link along precomputed backup light paths. Here, the entire route of the working lightpaths may be changed. This flexibility in path protection could lead to lower protection capacity but requires that all failed paths effect their recovery independently. On the other hand, link protection may require more protection capacity because of reduced flexibility in rerouting, but requires only local knowledge around the failed link to complete the recovery. In both link and path protection, the protection capacity may be dedicated to a link or path, respectively, or may be shared. Rings (with links in both the clockwise and counterclockwise directions) have been especially attractive because of the availability of exactly one backup path between any two nodes, leading to simple automatic protection switching mechanisms. When a link fails, in link protection, the end-nodes of the link switch to the backup path joining the two end-nodes. In path protection, all affected connections are notified of the link failure, and they switch to the backup paths. Both link and path protection techniques in rings require the reservation of 50% of the total capacity for protection purposes. More recently, attention has focused on mesh networks partly because of the increased flexibility they provide in routing connections, and partly because the natural evolution of network topologies leads to a mesh-type topology. While protection in mesh networks can potentially be more efficient, it is more complex as well because of the multiplicity of routes which can be used for recovery. Approaches for protecting link failures in mesh networks can be found in the recent literature and are briefly reviewed here. One approach is to use ring-like protection mechanisms by embedding cycles on a given mesh topology. Suppose the network is represented by a directed graph (digraph). Recovery from single-link failures requires the graph to be 2-edge connected, 1 so let us assume that a 2-connected digraph is given. In the double cycle cover method of Ellinas et al. (2000), Fan (1992), the links of the digraph are covered by two directed cycles such that each link is covered by a cycle in each direction exactly once. A set of cycles that has this property can be found in polynomial time for planar graphs Fan (1992) (i.e., graphs that can be drawn on a plane without intersecting edges), but no known polynomial-time algorithm is known for non-planar graphs. On each link, exactly half of the fibers are set aside for protection and half are used for working traffic. Consider the undirected link AB (that includes the directed links AB and BA), and suppose that it is a part of two cycles C1 and C2, where C1 is a cycle that includes directed link AB and C2 is a cycle that includes directed link BA . Then, all the working fibers from A to B are backed up by the protection fibers from A to B on cycle C2 , and all working fibers from B to A are backed up by the protection fibers from B to A on cycle C1 . Note that this is fiber-based recovery since whole working fibers are backed up by a set of protection fibers. The advantage of this technique lies in the fact that the protection switches can be pre-configured, and no signaling is required upon failure of a link. Apart from the drawback of not being able to guarantee recovery when the graph is non-planar, the above technique has the disadvantage of requiring wavelength conversion when there is a single fiber in each direction of a link Finn et al. (1997). Accordingly, another method of link protection was presented in Finn et al. (1997). In this method, instead of forming cycles, a 2-connected directed sub graph H that covers all nodes is obtained. Another sub graph H' which is similar to H except that the directions of the edges are reversed is also immediately obtained. On each fiber, half of the wavelengths are working and the other half are reserved for protection. Furthermore, the wavelengths that are reserved for protection in the edges in H are the working wavelengths in H' and vice versa. Then, a failure of an undirected link AB can be recovered as follows. Suppose the working wavelengths on directed link AB belong to H and those on directed link BA belong to H' . The working wavelengths on directed link AB are recovered using

the protection wavelengths on directed path AB in subgraph H' . Similarly, the working wavelengths on directed link BA are recovered using protection wavelengths on directed path BA in subgraph H . This method is applicable to non-planar graphs as well.

Software-defined networking (SDN) separates the control plane from the data plane, i.e., it moves the control logic from the network devices to a central controller. The centralized controller manages the flow of data through a southbound application programming interface (SB-API). Similarly, a centralized management of the networking devices has the advantage that new applications, services, and networking functions can be flexibly deployed with minimum operating and capital expenses. A few survey studies on SDN operation, history, architecture, programmability, and research directions are described in [1–6]. Link failure recovery approaches leverage the SDN unique features of centralized control and the flexibility of programmable data plane for real-time applications such as video conferencing A New Algorithm (1998) and voice over IP (VOIP), which can tolerate a delay of 50 ms in case of recovery. Thus, the quality of service (QoS) can be maintained in case of a link failure to ensure untroubled and constant communication. The reported mean for link and device failures in a traditional data center network per day have been recorded as 40.8 and 5.2 failures per time unit Fournier (1985), respectively, which necessitates the discovery of a method that enables faster recovery of failed links. The study Fournier (1985) also reported that the frequency of link failures is higher than that of the node failures. Therefore, fault-resilient approaches play an important role in tra_c engineering for operator networks to ensure a fast failure recovery, which will ultimately accomplish the requirements of the end-users.

The tight coupling of control and data planes in legacy networks makes them sluggish and complex to manage. Although traditional networks have been adopted universally, their management and configuration are cumbersome Goddyn (1985). because of the following reasons: _ Vendors are hesitant in providing the source code of the protocols to the developer and user community because of being afraid of unverified changes to their devices that can lead to malfunctions in the networks Grover (1992). _ A global view of the network is hard to obtain in the traditional network architecture; hence, only distributed routing protocols can be used, e.g., routing information protocol (RIP) Grover and Stamatelakis (1998) and open shortest path first (OSPF) Häggkvist and Jackson (1985). _ The co-existence of data and control planes also leads to an improper utilization of the bandwidth Itai et al. (1981), as it is shared by both the planes. Thus, the packets are broadcasted to the network, which leads to low link utilization. Similarly, the ball game gets worse as soon as there is a link failure because the system tries to search alternate paths in the network for packet broadcasting, leading to network congestion. In case of a link failure, re-routing is performed for discovering an alternative path to divert the packets from a failed link to the alternative path. However, the implementation of traditional routing protocols hinders the network growth and causes delays owing to several problems, such as flooding of the link-state information, long convergence time of path detection Jackson (1980), deployment complexity of the network Jaeger (1985), and route flaps caused by prefix instability Dravida et al. (1994). Additionally, there may be network destabilization because of routing conflicts owing to the autonomous system (AS) Jan et al. (1993). Consequently, there is a lack of optimum decisions due to the unavailability of the global statistics of the network. These problems exist in traditional internet architecture because of two reasons: First, because implementing changes in the traditional routing protocols is di_cult owing to the software being embedded in the firmware; and second, the internet companies feel at risk and shy away from implementing any new proposals, even if it can increase the performance of the network, as this will also increase the network complexity and, consequently, the maintenance cost. Fast failure recovery within a fixed time interval is vital for providing a service guarantee in next-generation technologies. In literature, several architectures [18–20] have been proposed for enabling the fast recovery of networks. The architecture proposed in Venkatesan et al. (1995) consists of an automatic failure recovery or fault management framework. The research conducted in Médard et al. (1997) leverages 5G, secure Internet-of-Things (IoT), and unmanned aerial vehicle (UAV) swarms to ensure service in mission-critical infrastructures. Likewise, a platform for virtualization of services based on SDN and network function virtualization (NFV) was proposed in [20], which enables the development, implementation, and functioning of media services over 5G networks. Moreover, the nodes may operate in remote and harsh environments with a possibility of frequent failures. Therefore, consecutive changes are essential to discover an alternative path for the nodes that have experienced failure [21]. In addition, the SDN handles the link failures using one of two main approaches, proactive and reactive [22]. In the proactive approach, the alternate paths are preconfigured, and in the case of a link failure, the disrupted flows are forwarded to the backup path. In contrast, in the reactive scheme, the controller is approached for finding an alternative path and the flow rules for the new path are inserted when the controller calculates the path. The SDN controller, which has access to the global topological information, will search the optimum alternative path for the failed link and will push the flow rules to it. Hence, the data plane is not interrupted. Consequently, the packets, are not broadcasted to the network here due to the centralized control architecture, which leads to a performance improvement in the network. However, both schemes have their pros and cons along with a trade-o_ in performance and e_ciency. Link failure recovery in SDN was overviewed in [23,24]. In this survey, we investigate the link failure detection and recovery approaches in SDN. A demonstration of the SDN-based failure recovery with proactive and reactive approaches is presented with pictorial diagrams. We compare the proactive.

REVIEW OF LITERATURE

Methods commonly employed for link protection in highspeed networks can be classified as either dynamic or preplanned, though some hybrids schemes also exist. Dynamic restoration typically involves a search for a free path using back-up capacity through broadcasting of help messages. Overheads due to message passing and software processing render dynamic processing

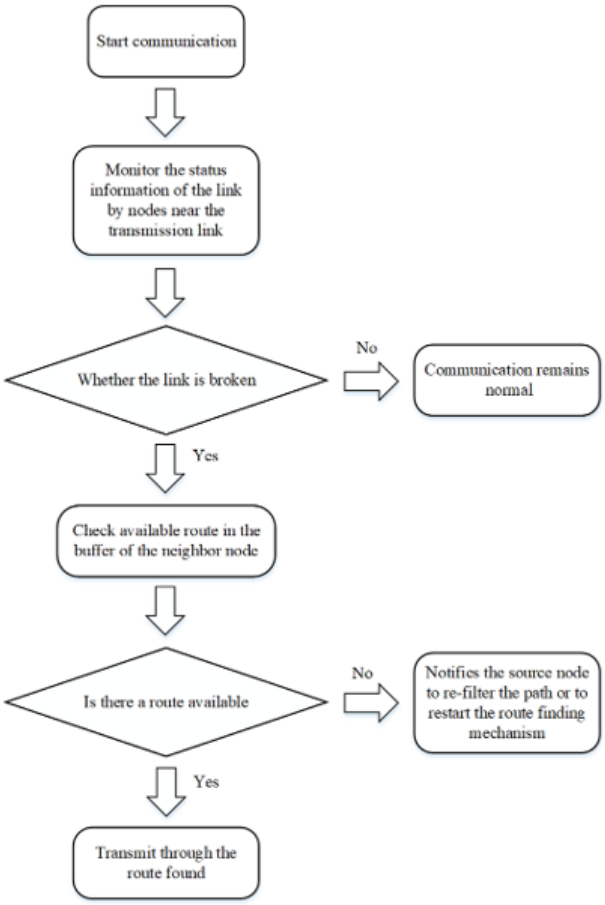
slow. For dynamic link restoration using digital cross-connect systems, a two second restoration time is a common goal for SONET. Preplanned methods depend mostly on lookup tables and switches or add–drop multiplexers. To meet our speed requirement, we consider preplanned methods, even though they may suffer from poorer capacity utilization than dynamic systems, which use real-time availability of back-up capacity. Within preplanned methods, we distinguish between path and link or node restoration. Path restoration refers to recovery applied to connections following a particular path across a network. Link or node restoration refers to recovery of all the traffic across a failed link or node, respectively. Path restoration may be itself subdivided into two different types: live (dual-fed) back-up, and event-triggered back-up. In the first case, two live flows, a primary and a back-up, are transmitted. The two flows are link- disjoint if we seek to protect against link failure, or node-disjoint (except for the end nodes) if we seek to protect against node failure. Upon failure of a link or node on the primary flow, the receiver switches to receiving on the back-up. Recovery is thus extremely fast, requiring action only from the receiving node, but back-up capacity is not shared among connections. In the second case, event-triggered path restoration, the back-up path is only activated when a failure occurs on a link or node along the primary path. Backup capacity can be shared among different paths [36], thus improving capacity utilization for back-up channels and allowing for judicious planning. However, recovery involves coordination between sender and receiver after a failure and action from nodes along the back-up path. This coordination may lead to delays and management overhead. Preplanned link or node restoration can be viewed as a compromise between live and event-triggered path restoration. Preplanned link restoration is not as capacity- efficient as event-triggered path restoration, but is more efficient than live back-up path restoration since sharing of back-up bandwidth is allowed. The traffic along a failed link or node is recovered, without consideration for the end points of the traffic carried by the link or node. Thus, only the two nodes adjacent to the failure need to engage in recovery. The back-up is not live, but triggered by a failure. Overviews of the different types of protection and restoration methods and comparison of the tradeoffs among them can be found in Doverspike and Wilson (1994), Dravida et al. (1994), Venkatesan et al. (1995), [25], [26], and [40]. Link or node restoration also benefits from a further advantage, which makes it very attractive for preplanned recovery: since it is not dependent upon specific traffic patterns, it can be preplanned once and for all. Thus, link or node restoration is particularly attractive at lower layers, where network management may not be aware, at all locations of the network, of the origination and destination, or of the format [39] of all the traffic being carried at that location. Therefore, in this paper, we concentrate on preplanned link and node restoration in order to satisfy our transparency requirement. Moreover, link restoration satisfies the first part of our flexibility goal since restoration is done without consideration for primary routings. For preplanned link restoration, the main approaches have involved covers of rings and, more recently, preplanned cycles Grover and Stamatelakis (1998). The most direct approach is to design the network in term of rings. The building blocks of SONET networks are generally self-healing rings (SHRs) and diversity protection (DP) [32], [31], [38]. SHRs are unidirectional path-switched rings (UPSRs) or bidirectional line-switched rings (BLSRs), while DP refers to physical redundancy where a spare link (node) is assigned to one or several links (nodes) ([38, pp. 315–332]). In rings, such as BLSR, link or node restoration is simply implemented using loop-back, which we explain in Section II. Ring-based architectures may be more expensive than meshes Brown et al. (1994), [35] and, as nodes are added, or networks are interconnected, ring-based structures may be difficult to preserve, thus limiting their scalability [34], [35], [38]. However, rings are not necessary to construct survivable networks [24], [33]. Meshbased topologies can also provide redundancy Jan et al. (1993), [28], [34]. For reasons of cost and extensibility, mesh-based architectures are more promising than interconnected rings. Covering mesh topologies with rings is a means of providing both mesh topologies and distributed ring-based restoration. There are several approaches to covers of rings for networks in order to ensure link restorability. One approach is to cover nodes in the network by rings [31]. In this manner, a portion of links are covered by rings. If primary routings are restricted to the covered links, then link restoration can be effected on each ring in the same manner as in a traditional SHR, by routing the back-up traffic around the ring in the opposite direction to the primary traffic. Using such an approach, the uncovered links can be used to carry unprotected traffic, i.e., traffic which may not be restored if the link that carries it fails. To allow every link to carry protected traffic, other ring-based approaches ensure every link is covered by a ring. One approach to selecting such covers is to cover a network with rings so that every link is part of at least one ring Grover (1992). This approach suffers from some capacity drawbacks. With fiber- based restoration, every ring is a four-fiber ring. A link covered by n rings requires 4n fibers; a link covered by rings requires fibers. Alternatively, the logical fibers can be physically routed through four physical fibers, but only at the cost of significant network management overhead. Minimizing the amount of fiber required to obtain redundancy using ring covers is equivalent to finding the minimum cycle cover of a graph, an NP-complete problem Itai et al. (1981), [30], although bounds on the total length of the cycle cover may be found Fan (1992). A second approach to ring covers, intended to overcome the difficulties of the first approach, is to cover every link with exactly two rings, each with two fibers. The ability to perform loop-back style restoration over mesh topologies was first introduced in Ellinas and Stern (1996) and Ellinas et al. (2000). In particular, Ellinas et al. (2000) considers link failure restoration in optical networks with arbitrary two-link redundant arbitrary mesh topologies and bidirectional links. The approach is an application of the double-cycle ring cover Jaeger (1985), [27], [29]. For planar graphs, the problem can be solved in polynomial time; for nonplanar graphs, it is conjectured that double-cycle covers exist, and a counterexample would have to obey certain properties Goddyn (1985). Node recovery can be effected with double-cycle ring covers, but such restoration requires cumbersome hopping among rings. In Section III-B, we consider double-cycle covers in the context of wavelength-based recovery. In order to avoid the limitations of ring covers, an approach using preconfigured cycles, or -cycles, is given in Grover and Stamatelakis (1998). A p-cycle is a cycle on a redundant mesh network. Links on the p-cycle are recovered by using the -cycle as a conventional BLSR. Links not on the -cycle are recovered by selecting, along the

-cycle, a path connecting the nodes, which are the end-points of the failed link. Note that some difficulty arises from the fact that several -cycles may be required to cover a network, making management among -cycles necessary. A single -cycle may be insufficient because a Hamiltonian might not exist, even in a two-connected graph. Even finding -cycles which cover a large number of nodes, may be difficult. Some results Fournier (1985), Jackson (1980), [41] and conjectures Häggkvist and Jackson (1985), [37] exist concerning the length of maximal cycles in two-connected graphs. The -cycle approach is in effect a hybrid ring approach, which mixes path restoration (for links not on the -cycle) with ring recovery (for links on the -cycle).

Priorwork that is related to our paper falls into two categories: loopback recovery methods for single-link failure protection and path protection techniques for protection from double-link failures. Considering link protection techniques for mesh networks first, one approach is to use ring-like protection mechanisms by embedding cycles on a given mesh topology. Suppose the network is represented by a directed graph (digraph). Recovery from single-link failures requires the graph to be 2-edge connected, 2 so let us assume that a 2-connected digraph is given. In the oriented cycle double cover (OCDC) method of Finn et al. (1997), A New Algorithm (1998), the links of the digraph are covered by two directed cycles such that each link is covered by a cycle in each direction exactly once. A set of cycles that has this property can be found in polynomial time for planar graphs A New Algorithm (1998) (i.e., graphs that can be drawn on a plane without intersecting edges), but no polynomial-time algorithm is known for nonplanar graphs.3 On each link, exactly half of the wavelengths are set aside for protection and half are used for working traffic. Consider the undirected link AB (that includes the directed links AB and BA) and suppose that it is a part of two cycles C1 and , C2 where C1 is a cycle that includes directed link AB and C2 is a cycle that includes directed link BA. Then, all of the working wavelengths from A to B are backed up by the protection wavelengths from A to B on cycle,C2 and all working wavelengths from B to A are backed up by the protection wavelengths from B to A on cycle C1 . The advantage of this technique lies in the fact that the protection switches can be preconfigured, and no signalling is required upon failure of a link.

PROPOSED METHODOLOGIES

Network survivability in high-speed optical systems has traditionally focused on safeguarding against the failure of a single link or node. However, increasing network scale and traffic demand have made it essential to consider more complex failure scenarios, particularly double-link failures that may occur in any arbitrary order. The paper addresses this gap by proposing a set of recovery methods and a heuristic algorithm designed to ensure efficient and rapid restoration under double-link failure conditions.



The proposed strategy builds on preplanned protection mechanisms rather than dynamic recovery. Dynamic approaches—although flexible—are slow due to the need for message broadcasting, signaling, and real-time path computation. Preplanned methods, in contrast, provide recovery using pre-established backup paths or cycles, enabling rapid restoration suitable for high-speed networks where even milliseconds of downtime can result in immense data loss. The proposed method adopts this preplanned strategy to maintain high recovery speed while tolerating more complex failure patterns.

1) Loopback-Based Double-Link Failure Recovery

The authors present three loopback methods, two of which rely on identifying the exact failed links, while the third does not require explicit failure localization. Loopback recovery—widely used in SONET—operates by redirecting traffic from a failed link onto an alternate route arranged in a looped or cyclical structure. This method is extended and generalized for mesh topologies, enabling a more distributed, scalable, and bandwidth-efficient solution.

Traditional loopback is most effective on ring topologies. However, mesh networks, which naturally arise as network size increases, offer more flexibility but complicate the process of establishing predetermined recovery paths. The paper introduces generalized loopback, enabling loopback behavior even on arbitrary mesh networks. This requires designing recovery graphs that guarantee that backup paths remain available regardless of the failed components.

2) Precomputation of Backup Paths Using a Heuristic Algorithm

A crucial contribution of the method is a heuristic algorithm that pre-computes backup paths for every link in the network. Unlike single-link protection schemes that rely on cycle covers or specific ring overlays, this heuristic is designed to handle more complex double-link failures without requiring a perfect cycle cover.

Key characteristics of the heuristic:

- It precomputes alternate paths for each link in advance.
- It avoids reliance on the existence of double-cycle covers, which are difficult to guarantee in non-planar graphs.
- It strikes a balance between protection capability and required backup capacity.
- It ensures that each link has a set of backup routes that remain valid even if another link fails concurrently.

The algorithm aims to identify multiple link-disjoint or partially overlapping alternate routes that maintain connectivity between the two nodes of a failed link. Because double-link failures can occur in arbitrary combinations, the protection paths must not depend on any single alternate path always remaining intact. Thus, redundancy must be distributed intelligently across the network.

3) Advantages Over Earlier Mesh-Based Approaches

Earlier approaches to mesh survivability often relied on:

- **Double cycle covers,** which guarantee each link appears in a protecting cycle in both directions; however, these are difficult to compute for non-planar graphs.
- **p-cycles,** which provide fast restoration but may require multiple cycles to cover an entire network.
- **Ring covers,** which suffer from capacity inefficiency and scalability limitations.

The proposed method avoids these drawbacks by using an algorithmic approach that does not require any rigid topological structure such as rings, cycles, or Hamiltonian paths. This makes it applicable to arbitrary mesh networks, including large-scale and irregular topologies common in modern WDM systems.

4) Generalized Loopback for Node Failures

In addition to link failures, generalized loopback is extended to node failures. Node recovery is often more complex than link recovery because all adjacent links simultaneously lose connectivity. The paper presents an algorithm that isolates the failed node and redirects all its incoming and outgoing traffic across alternate predetermined paths. This is supported by a network management protocol that enables distributed and autonomous operation without requiring centralized decision-making during failure.

EXPERIMENTAL RESULTS

The experimental evaluation demonstrates the efficiency and reliability of the proposed heuristic for double-link recovery. The authors compare their approach with existing algorithms and measure performance in terms of two primary metrics:

- **Restorability (percentage of successfully recovered double-link failures)**
- **Backup capacity required (additional resources reserved for recovery)**

1) Nearly 100% Restorability

The results indicate that the proposed method achieves almost 100% recovery from double-link failures. This is significant because double-link failures represent a more demanding scenario than traditional single-link protection strategies.

Many existing preplanned methods fail to guarantee complete restorability when failures occur at two different points in the network, especially in mesh-based architectures. The heuristic algorithm ensures that backup routes remain available and do not conflict with each other even under such complex failure conditions.

2) Modest Increase in Backup Capacity

A major advantage highlighted in the results is that the method achieves near-total restorability without requiring excessive backup capacity. Traditional ring-based or double-cycle techniques often require reserving 50% or more of the total network capacity for protection. In contrast, the proposed algorithm uses capacity more efficiently.

The numerical simulations suggest that only a modest increase in additional capacity is required to support complete double-link recovery. This makes the method cost-effective for real-world deployment, where bandwidth is an expensive and finite resource.

3) Comparison With Other Approaches

When compared with:

- **Double cycle cover methods,**
- **p-cycle approaches, and**
- **Traditional ring overlays,**

the proposed algorithm demonstrates superior flexibility and lower dependence on specific graph properties. In non-planar or irregular network topologies, the proposed method consistently provides higher recovery success rates.

4) Effectiveness in Both Link and Node Failure Scenarios

The experiments also validate the generalized loopback mechanism for node failures. Even though node failures are more disruptive, the method successfully reroutes traffic around the failed node without excessive delay or capacity requirements.

5) Practical Benefits for Next-Generation Optical Networks

The results are particularly relevant for WDM optical mesh networks, which form the backbone of modern high-speed internet. The ability to recover from double-link failures with minimal capacity overhead ensures:

- Higher service availability
- Reduced downtime
- More resilient communication infrastructure

Given that fibre cuts and equipment failures are common in real-world networks, achieving fast and reliable restoration is essential. The proposed algorithm meets this requirement by enabling rapid, distributed, and preplanned recovery.

CONCLUSION AND FUTURE WORK

Network survivability is a crucial requirement in high-speed optical networks. Typical approaches of providing survivability have considered the failure of a single component such as a link or a node. In this paper, we motivated the need for considering double-link failures and presented some approaches for handling such failures. A heuristic algorithm that pre-computes backup paths for links in order to tolerate double-link failures was then presented. Numerical results comparing the performance of our algorithm with other approaches suggests that it is possible to achieve almost 100% recovery from double-link failures with a modest increase in backup capacity. In this work, we have assumed that any two arbitrary links may fail in any order. Future work may consider other failure models. Pre-computing backup paths that minimize the capacity requirement under double-link failures is another interesting direction of study. Exploring the trade-off between restorability and backup capacity is yet another possible topic for future study.

In the proactive method, the backup paths are calculated in advance. Therefore, when a link fails, the controller forwards the tra_c on the backup path. The method has its pros, such as the controller does not need to recalculate the path as the forwarding rules for the backup path already exist in SDN switches. However, a disadvantage of this approach is that the TCAM space cost of the SDN switches increases. Besides this, the switches have a limitation of 8000 flow entries in the flow tables. In a few cases, the backup path may fail earlier than the original primary path. If the failure occurs early, the performance is a_ected, because the incoming packets are matched with the flow rules due to the redundancy of backup path flow entries in the switches. In the reactive approach, the SDN controller installs the flow rules for the alternative path when a link failure event occurs. The methodology is economical in terms of TCAM space; however, the calculation of an alternative path at run time and the installation of rules for the alternative path incurs an additional delay. To summarize, the critiques of the reactive approach argue that the induced delay incurred by the controller in finding an alternative path cannot meet the minimum delay requirements of the CGNs. However, approaches that have used e_cient routing algorithms and minimum flow operations have achieved the desired results. There is always a space for future researchers in terms of improving the previous works because there is a tradeo_ between flow operations, large-scale SDN, the minimum shortest cost path, complexity of the algorithm, delay, congestion, load balancing, etc. The inter-domain techniques have synchronization, E2E service provisioning, and interoperability problems that hamper failure recovery. Similarly, in the in-band

schemes, the di_erentiation between data and control tra_c is a complex process. Therefore, e_cient solutions with minimum complexity can be proposed with which the innovative features of southbound interface protocols, such as OpenFlow/Netconf, can be combined for achieving effcient results. In the end, we discussed ML-based schemes. There is a high probability of the ML-based schemes being used in the future because of the increase in the internet nodes and users as well as the enormous usage of data. However, the lack of standard datasets for the SDN environment hinders the use of ML in SDN research. The development of ML applications with high accuracy for link failure detection and the formation of versatile datasets should be considered for using ML in SDN in future.

The introduction of SDN for combating link failure recovery is a novel approach that leverages centralized control concepts. In this paper, we described the background and importance of SDN in link failure recovery by explaining the vulnerabilities of the traditional networking architecture. Then, the three SDN planes and their interaction mechanisms were described along with the importance of SDN for link failure recovery. The failure recovery speed is dependent on the time taken in failure detection. Therefore, we described the state-of-the-art approaches for link failure detection with their pros and cons. We described the proactive and reactive approaches. First, we explained the link failure detection and recovery process with proactive failure recovery in SDN. Then, previous schemes using proactive recovery were described in detail. Similarly, we described reactive failure recovery approaches, i.e., the reactive failure recovery mechanism in SDN and its related literature. We compared the e_ectiveness of proactive and reactive failure recovery approaches in SDN from the summaries of previous works. A comparison was performed between the proactive and reactive schemes in terms of latency, scalability, routing updates, TCAM space, flow operations matching, configuration, robustness to backup path failures, routing information access, processing of switches, and the overheads of routing, controller and switches. The inter-domain and intra-domain architectures for link failure recovery were discussed. Finally, the link failure recovery in a hybrid SDN environment, large-scale networks, in-band SDN, and machine learning schemes were discussed. We simulated two application scenarios of the Naval tactical networks and DCN using the ODL controller for proactive and reactive approaches, showing the recovery time and throughput comparison. The experimental results after applying the two schemes show that flow insertion by the SDN controller, in case of the Although we have proposed SRM as a framework that applies to many different applications, we have developed just one such application, wb. Further, because we based the implementation on ALF and deliberately factored many application semantics into the design of the wb transport, it is relatively difficult to extract and re-use wb's network implementation in another application. However, this limitation resulted from our lack of prior experience with ALF-based design and we argue now that an ALF protocol architecture does not necessarily preclude substantial code re-use. Based on our subsequent experience with another ALF architecture | the Real-time Transport Protocol (RTP) [SCFJ94] that underlies the MBone tools vic and vat | we know that the core of an ALF based design can be easily tailored for a range of application types. For ex- ample, we developed a generic RTP toolkit as an object- oriented class hierarchy, where the base class implements the common RTP framework and derived subclasses implement application-specific semantics. Our RTP toolkit sup- ports a wide range of applications including layered video, traditional H.261-coded video, LPC-coded audio, generic audio/video recording and playback tools, and RTP monitoring and debugging tools. Each of these tools shares most of its network implementation with all of the others, yet each still reects its individual semantics through ALF | RTP is not a generic protocol layer. In current work, we are applying these same design principles to both the next generation of the wb protocol as well a new set of SRM-based applications.

ACKNOWLEDGMENTS

None.

REFERENCES

A New Algorithm for Bi-Directional Self-Healing for Arbitrary Redundant Networks (1998).. In Proceedings of the Optical Fiber Communication Conference. IEEE.

Brown, G. N., Grover, W. D., Slevinsky, J. B., and MacGregor, M. H. (1994). An Architecture for Efficient Survivable Networks. In Proceedings of IEEE GLOBECOM (Vol. 2, pp. 471–477). IEEE.

Doverspike, R., and Wilson, B. (1994). Comparison of Capacity Efficiency of DCS Network Restoration Routing Techniques. Journal of Network and Systems Management, 2(2), 135–144. https://doi.org/10.1007/BF02139308

Dravida, S., Anderson, J., Doshi, B. T., and Harshavardhana, P. (1994). Fast Restoration of ATM Networks. IEEE Journal on Selected Areas in Communications, 12(1), 128–136. https://doi.org/10.1109/49.265712

Ellinas, G., Hailemarian, R. G., and Stern, T. E. (2000). Protection Cycles in Mesh WDM Networks. IEEE Journal on Selected Areas in Communications, 18(10), 1924–1937. https://doi.org/10.1109/49.887913

Ellinas, G., and Stern, T. E. (1996). Automatic Protection Switching for Link Failures in Optical Networks With Bi-Directional Links. In Proceedings of IEEE GLOBECOM (Vol. 1, pp. 152–156). IEEE. https://doi.org/10.1109/GLOCOM.1996.594351

Fan, G. (1992). Covering Graphs by Cycles. SIAM Journal on Computing, 21(3), 491–496. https://doi.org/10.1137/0405039

Finn, S. G., Médard, M., and Barry, R. A. (1997). A Novel Approach to Automatic Protection Switching Using Trees. In Proceedings of the International Conference on Communications. IEEE.

Fournier, I. (1985). Longest Cycles in 2-Connected Graphs of Independence Number. In Cycles in Graphs, Annals of Discrete Mathematics (Vol. 115, pp. 201–204). North-Holland.

Goddyn, L. (1985). A Girth Requirement for the Double Cycle Cover Conjecture. In Cycles in Graphs, Annals of Discrete Mathematics (Vol. 115, pp. 13–26). North-Holland. https://doi.org/10.1016/S0304-0208(08)72994-3

Grover, W. D. (1992). Case Studies of Survivable Ring, Mesh and Mesh-Arc Hybrid Networks. In Proceedings of IEEE GLOBECOM (pp. 633–638). IEEE. https://doi.org/10.1109/GLOCOM.1992.276439

Grover, W. D., and Stamatelakis, D. (1998). Cycle-Oriented Distributed Preconfiguration: Ring-Like Speed with Mesh-like Capacity for Self-Planning Network reconfiguration. In Proceedings of IEEE International Conference on Communications (Vol. 2, pp. 537–543). IEEE. https://doi.org/10.1109/ICC.1998.682929

Häggkvist, R., and Jackson, B. (1985). A Note on Maximal Cycles in 2-Connected Graphs. In Cycles in Graphs, Annals of Discrete Mathematics (Vol. 115, pp. 205–208). North-Holland. https://doi.org/10.1016/S0304-0208(08)73011-1

Itai, A., Lipton, R. J., Papadimitriou, C. H., and Rodeh, M. (1981). Covering Graphs with Simple Circuits. SIAM Journal on Computing, 10(4), 746–750. https://doi.org/10.1137/0210058

Jackson, B. (1980). Hamilton Cycles in Regular 2-Connected Graphs. Journal of Combinatorial Theory, Series B, 29(1), 27–46. https://doi.org/10.1016/0095-8956(80)90042-8

Jaeger, F. (1985). A Survey of the Double Cycle Cover Conjecture. In Cycles in Graphs, Annals of Discrete Mathematics (Vol. 115, pp. 1–12). North-Holland. https://doi.org/10.1016/S0304-0208(08)72993-1

Jan, R.-H., Hwang, F.-J., and Cheng, S.-T. (1993). Topological Optimization of a Communication Network Subject to a Reliability Constraint. IEEE Transactions on Reliability, 42(1), 63–70. https://doi.org/10.1109/24.210272

Médard, M., Finn, S. G., and Barry, R. A. (1997). Automatic Protection Switching for Multicasting in Optical Mesh Networks. In Proceedings of the Optical Fiber Communication Conference. IEEE. https://doi.org/10.1364/ONA.1998.AP1

Venkatesan, S., Veerasamy, J., and Shah, J. C. (1995). Spare Capacity Assignment in Telecom Networks Using Path Restoration. In Proceedings of IEEE International Conference on Communications (pp. 370–374). IEEE. https://doi.org/10.1109/MASCOT.1995.378644