Survivability in Optical Networks
Dongyun Zhou and Suresh Subramaniam, George Washington University

Abstract
Survivability, the ability of a network to withstand and recover from failures, is one of the most important requirements of networks. Its importance is magnified in fiber optic networks with throughputs on the order of gigabits and terabits per second. This article takes a look at the techniques used to achieve survivability in traditional optical networks, and how those techniques are evolving to make next-generation WDM networks survivable.

With the integration of computer and communication technologies and the rapid maturation of fiber optic communication techniques, today's telecommunication networks can provide fast and high-quality services to end users. The service type has broadened from voice only to a diverse array of multimedia services. With more and more business users involved, the interruption of service for even short periods of time may have disastrous consequences. As such, how to prevent service interruption, and reduce the loss of service to a minimum if interruption is inevitable, becomes a critical issue; that is, survivability must be considered in designing telecommunication networks. The survivability of a network refers to a network's capability to provide continuous service in the presence of failures.

Optical fiber has become the dominant transport medium in telecommunication systems because of its advantages in capacity, reliability, cost, and scalability. An attractive feature of optical fiber is its extremely large capacity, on the order of a few terabits per second. The fiber optic medium is the only one capable of providing high-bandwidth service cost-effectively. Today, optical fiber is widely deployed in backbone networks. However, only a small fraction of the full capacity of the installed optical fiber has been realized thus far. The primary reason for this inefficiency is the large mismatch between peak electronic processing and source rates, and fiber capacity. Therefore, new multiplexing techniques such as wavelength-division multiplexing (WDM) have been proposed in order to utilize fiber capacity more efficiently.

In a WDM system, a single fiber can carry many channels, and the total utilized capacity can be increased dramatically. Scientists from Bell Laboratories have successfully demonstrated the transmission of 100 wavelengths over a fiber, with each wavelength modulated at 10 Gb/s, to provide a throughput of 1 Tb/s. Thus, WDM technology is paving the way for the development of new services, and one can be sure that it is about to play a major role in the expansion of optical networks.

While WDM may provide larger bandwidth to users and more revenue to service providers, it also has some potential problems. The most serious is the survivability of WDM systems. Because of the large amount of traffic a fiber carries, a single failure in a WDM system would cause severe service loss. As WDM systems get ready to move from the experimental stage to large-scale commercial deployment, the time is ripe to take stock of the current efforts in network survivability, and to see how these relate to future-to-be-designed WDM mesh networks. To this end, this article focuses on survivability mechanisms used in today's optical networks and recent research efforts in providing survivability for next-generation WDM networks.

In order to design a survivable optical network, one must lay out the possible failures under which the network must be survivable. The basic types of network failures generally considered are link and node failure. Link failure usually occurs because of cable cuts; node failure is due to equipment failure at network nodes. Besides node and link failures, which are common failure situations in any communication network, channel failure is also possible in WDM optical networks. A channel failure is usually caused by the failure of transmitting and/or receiving equipment operating on that channel (wavelength).

Initial work on survivability in WDM optical networks has focused mostly on the recovery from a single link or node failure. This is primarily due to a combination of two factors:
• It is easier to plan for the failure of at most one piece of equipment at a time.
• Cable cuts that cause link failures are common in optical networks.

Man-made errors and uncontrollable natural phenomena (e.g., floods and earthquakes) cause equipment, and therefore node, failures. Channel failure scenarios have received little attention thus far. It should be borne in mind that even a single channel failure might cause the loss of as much traffic as a single fiber failure in a non-WDM system.

In the following sections, we discuss several survivability techniques used in optical networks. We present a classification of the survivability techniques commonly used. We also discuss survivability mechanisms adapted to the very popular synchronous optical network (SONET) structures, which are non-WDM optical networks. The basic approaches to surviv-
able WDM networks are presented, along with a sampling of the results from recent research in this area.

Survivability Techniques in Non-WDM Networks

The techniques that have been proposed and used for survivability in optical networks can be classified under two general categories: predesigned protection and dynamic restoration. Figure 1 shows a classification of techniques used in today's optical networks, as well as those possible for the WDM networks of the future.

Predesigned Protection

Predesigned protection refers to the fact that recovery from network failures is based on preplanned schemes. Usually, it relies on resources (fibers, wavelengths, switches, etc.) dedicated to protection purposes. In predesigned protection, some resources are reserved for recovery from failures at either connection setup or network design time, and kept idle when there is no failure. From this point of view, the use of capacity is not very efficient, but on the other hand, the level and speed of recovery from a failure can be guaranteed. Automatic protection switching (APS) and self-healing ring (SHR) are the most common predesigned protection schemes currently used in non-WDM optical networks.

Automatic Protection Switching — APS is typically used to handle link failures. It has three main architectures: 1 + 1, 1:1, and 1:N APS. The difference between the three architectures is the assignment of protection resources. In 1 + 1 APS (Fig. 2a), a protection link is provided for every working link. The source node transmits the information signal on both the working and protection links. The receiver at the destination node compares the two signals and chooses the better one (e.g., the less noisy one). If one link fails, the destination node is still able to receive the signal on the operational link. In 1:1 APS, shown in Fig. 2b, every working link has a protection link, but the source and destination nodes switch to the protection link only when a failure on the working link is detected. Under normal conditions, the protection link is either idle or used to carry low-priority traffic. Figure 2c shows how a 1:N APS system works. In this scheme, N working links share a single protection link, thereby providing protection against the failure of any one of the N working links. But, unlike in 1:1 APS, the traffic switched to the protection link must be switched back to the working link after it is repaired so that the protection link is available for any future working link failures. In general, m:n protection refers to an APS scheme in which m protection links are shared among n working links. When more than m of the n working links fail simultaneously, the traffic routed to the protection links can be decided according to preassigned priorities.
Self-Healing Ring — SONET SHR is a very successful technique for survivable optical networks. Here, networks are designed to have ring architectures. SHR is more flexible than APS in that it can handle both link and node failures. The development of high-speed add/drop multiplexing (ADM) technology and the simple control mechanism used in SHR have made it a very attractive way to provide survivability.

Unidirectional SHR (USHR) and bidirectional SHR (BSHR) are two types of SHRs in SONET systems. The difference between these two categories is the direction of the traffic flow under normal operation. In USHR, the normal traffic flow goes around the ring in one direction, as shown in Fig. 3a. Any traffic routed to the protection ring because of a failure is carried in the opposite direction. In BSHR, working traffic flows in both directions.

USHR protection can be done in two different ways: line protection switched USHR (USHR/L) and path protection switched USHR (USHR/P). USHR/L is also known as loopback. In loopback, two nodes adjacent to a failure are responsible for switching the affected traffic to the protection ring, as shown in Fig. 3b. In the figure, the fiber between nodes 3 and 4 is cut, so node 4 loops the traffic from working to protection fiber, and node 3 loops the traffic back from protection to working fiber. It is easy to see that loopback can also be applied to node failures. The two nodes adjacent to the failed node perform the loopback, and all the traffic not starting from or ending at the failed node can be restored. USHR/P is basically a 1+1 protection scheme because the signals for every connection are transmitted on both rings. When a failure occurs and affects one of the signals, the ADM at each node decides which signal is still good and then chooses it. As shown in Fig. 3c, the fiber cut between nodes 3 and 4 will disconnect all the traffic toward node 3 on the working ring. Thus, the ADM at node 3 will choose those signals transmitted toward it on the protection ring as the valid signals. USHR/P is the fastest SHR scheme because no switching of signals is needed.

The typical architectures of BSHR are two- and four-fiber line protection BSHR/2 and BSHR/4. In BSHR/2, shown in Fig. 3d, half of the capacity on each ring is reserved for protection. When a failure occurs, the two nodes adjacent to the failed site will loop the affected traffic using the reserved capacity on both rings. In BSHR/4 (Fig. 3e), two fibers are dedicated as working fibers, so the capacity on them can be completely utilized. Upon failure, the nodes adjacent to the failure site simply loop the affected traffic from the working to the protection fibers.

The evolution of communication network topologies in response to traffic dynamics naturally leads to mesh topologies. Protection for such networks is usually more complicated than for point-to-point links or ring networks. Some solutions have been proposed for protection in mesh networks. For example, in one approach called ring covers [1], a set of rings that covers every link in the mesh at least once is found. By using the SHR technique, the network can be protected against fiber cuts and node failures. The drawback of this solution, however, is the need for a large amount of spare capacity to get 100 percent protection guarantee.

Dynamic Restoration

Dynamic restoration implies the discovery of spare capacity dynamically in the network to restore the affected services; that is, the resources used for recovery are not reserved at the time of connection establishment, but are chosen from available resources such as fibers, wavelengths, switches, and so on when the failure occurs. This is typically more efficient than pre-designed protection from the viewpoint of resource utilization. On the other hand, the restoration time is usually longer, and 100 percent service recovery cannot be guaranteed because sufficient spare capacity may not be available at the time of failure.

In SONET networks, intelligent digital cross-connect systems (DCSs) and controllers are used as the main components to realize dynamic restoration. The controllers may be centralized or distributed to achieve a suitable balance between recovery time and complexity of recovery algorithms. But no matter which ones are used, recovery time and complexity are much more than for preplanned protection schemes. Due to the large traffic carried in fiber optic systems, recovery time is a very important parameter to meet quality of service (QoS) requirements. Dynamic restoration techniques are at a disadvantage from this perspective.

Research has shown that both preplanned protection and dynamic restoration schemes have advantages depending on network topology. For example, in a point-to-point link, APS is the best solution, while SHR offers the most benefits in a ring topology [2]. Most of today’s communication networks use these preplanned protection mechanisms rather than dynamic restoration methods. When a large mesh network is to be made survivable, APS and SHR covering may require an inordinate amount of additional capacity. In this situation, dynamic restoration seems to be a practical way to do the job, but much research remains to be done in designing rapid restoration schemes.

---

1 However, it is possible to form undesired connections in this case if proper coordination steps are not taken.

2 However, when a failure occurs, dynamic algorithms may end up using more resources for restoration than may have been reserved under pre-designed protection.
Having presented practical survivability methods in a non-WDM optical network, we now describe how these techniques are adapted and enhanced to provide survivability in WDM optical networks.

Survivability in WDM Optical Networks

Multilayer Protection in WDM Networks

WDM systems are being widely deployed in the backbone network. The use of optical switches and all-optical components introduces a new network layer, called the optical layer or WDM layer, into the layered architecture. The WDM layer supports different higher-layer services, such as SONET connections, asynchronous transfer mode (ATM) virtual circuits, and IP-switched datagram traffic. According to the layered structure of a network, survivability can be offered at the WDM layer or higher layers. Some of the higher-layer services, such as SONET and ATM, actually have their own protection mechanisms, while some may not have recovery mechanisms incorporated in the protocols. Under this situation, the WDM layer should be able to offer them. However, WDM layer survivability cannot protect against failures at higher layers, and some survivability must be provided at higher client layers as well.

Incorporating survivability mechanisms at multiple layers leads to the issues of assigning functions to each layer and coordinating the layers in effecting recovery from a fault. The set of rules describing the point of origination of the fault recovery process and the interaction between the various layers is called an escalation or interworking strategy. Two escalation strategies have been proposed [3] based on the layer at which the fault recovery process is initiated. In the bottom-up strategy, recovery starts at the layer closest to the failure, and escalates upward upon expiration of a holdoff timer. This timer allows the lower layers time to recover from a fault (if possible) before triggering recovery mechanisms at a higher layer. This strategy ensures very quick activation of the recovery process. In the top-down strategy, recovery always starts at the uppermost layer and escalates downward. Holdoff timers are not necessary in this strategy, but a disadvantage is the potentially large number of traffic streams that must be restored at the higher layers. A third strategy would start the recovery process at some intermediate layer, and escalate either upward or downward based on the received alarms and survivability statistics. A cost-performance comparison of the escalation strategies, reported in [3] for an ATM-over-synchronous digital hierarchy (SDH) network, found that the bottom-up approach was better in terms of both equipment cost and recovery time. However, a main attraction of the top-down strategy is that it can provide differentiated QoS for survivability to different users.

The foregoing discussion suggests that WDM layer survivability is desirable. Providing survivability functionality at the WDM layer has many advantages [4, 5]:

- Speed — Recovery at the WDM layer is much faster because the nodes can act quickly upon the occurrence of failures and do not have to wait for higher-layer indication signals.
- Simplicity — It needs less coordination than recovery at higher layers.
- Effectiveness — Optical restoration makes more efficient use of restoration capacity because of resource sharing among different service layers.
- Transparency — The wavelength routing protection technique is independent of the protocols used in higher layers.

Fault Detection and Localization

An important related issue in WDM-layer survivability is fault detection/localization, which is a prerequisite to the fault recovery process. Fault detection and localization in SONET is done using frame overhead bytes and electronic monitoring facilities to detect loss of data or excessive bit error rates [6]. However, similarly advanced techniques are unavailable at this time in the optical domain. There are some proposals to monitor channel continuity and quality using transmitted/received power levels, crosstalk, and so on, and an optical supervisory channel may be used for this purpose [6]. Before these techniques gain maturity, electronic monitoring schemes at all nodes (using optoelectronic conversions) may be used in the interim. Although electronic monitoring techniques remove full transparency, the electronic processing is at a bit, not packet, level. Hence, protocol transparency can still be provided.

When full transparency within the optical core is desired, fault localization cannot be done effectively. When a lightpath fails, the network edge routers may be able to detect the fault, but the exact location of the fault cannot be determined. Fault recovery in such situations is not clearly understood at this time. In the rest of the article, we assume that fault detection/localization can be done and focus on WDM-layer protection.

WDM-Layer Protection

The ideas used in WDM-layer protection are very similar to those in SONET systems. A main reason for this is that WDM technology has been used to upgrade the existing optical networks, thus keeping the network topologies largely unchanged. It is natural to find protection schemes similar to existing techniques and use them in the upgraded networks. For example, in point-to-point WDM systems, 1 + 1, 1:1, and 1:N optical protection are used in a way similar to APS in SONET systems, except that switching is done in the optical domain. WDM SHR architectures also operate along the same lines as SONET SHRs. For example, the idea of loopback recovery in SONET systems is used in WDM networks in [7]. In WDM systems, due to the availability of multiple wavelengths in a single fiber, protection methods can be more flexible. Either a whole fiber or only some wavelengths in the fiber can be dedicated to protection purposes. Of course, the multiplicity in wavelengths also makes the protection schemes more complicated. For example, if the BSHR/2 architecture is used in WDM systems, the wavelengths used for protection have to be chosen carefully to avoid wavelength conversion in the nodes. The wavelengths used on the two rings can be chosen to overlap (i.e., some wavelengths are used as working channels on both rings) or nonoverlapped (i.e., the wavelengths used as working channels on one ring are not used as working channels on the other ring). Nonoverlapped wavelength assignment has the advantage that when a failure occurs, the nodes doing loopback do not have to deal with wavelength conversion, because the affected channels can always use the same wavelengths reserved for them on the other ring.

As WDM system deployment advances beyond the upgrading of existing non-WDM systems, mesh topologies using optical cross-connects (OXCs) are likely to emerge. In such situations, protection can be provided by the OXCs, much like DCSs in SONET networks. Researchers have recently started studying WDM mesh network survivability. Most of the studies so far have considered only single-link failures. To be sure, however, the failure of even a single link in a WDM system causes the failure of several channels simultaneously, a much more serious situation than in non-WDM systems. Furthermore, fiber cuts are among the most common failure scenarios. In the following, we will survey the different schemes used for single-link failure recovery.

3 SDH is a SONET-like standard used in Europe.
Protection from Single-Link Failures

Considering the single-link failure scenario in mesh networks, a simple way to provide survivability is the dedicated fiber scheme. Here, each link in the network has its dedicated backup link. Upon a link failure, traffic is simply routed over its backup link, as shown in the example of Fig. 4a in which the link between nodes 5 and 6 has failed. Because most link failures are due to fiber cable cuts, the backup fiber is required to be diversely routed. This is a complicated task for network design and realization, and is obviously a waste of capacity.

Other solutions that can use the capacity more efficiently have been proposed and, as mentioned earlier, fall under two categories: predesigned protection and dynamic restoration. Dynamic restoration schemes are carried out using intelligent OXCs and controllers in the network. Again, as mentioned before, dynamic restoration algorithms are usually complicated, and restoration time is much longer than for predesigned protection algorithms. Predesigned protection schemes are by far the most studied for WDM optical networks. Because of the multichannel traffic, the design algorithms used in a WDM network are more complicated than those used in non-WDM systems. In the following discussion, we will mostly discuss the proposed predesigned protection approaches.

There are two main predesigned protection techniques against single-link failures in WDM networks. One is link-based protection, the other, path-based protection.\(^4\) We present these in detail below.

**Link-Based Protection** — The basic idea of link-based protection is that a protection path is reserved for each link, and when the link fails, traffic is rerouted (looped back) around the failed link. As an example, in Fig. 4b, after a link failure between nodes 5 and 6, the affected traffic is rerouted through the backup path 5–2–6. Here, the end nodes of the failed link (i.e., nodes 5 and 6) are responsible for recovery.

In a WDM network, each link carries many channels, and the failure of a single link causes the failure of all the channels on the link. In link-based protection, each working channel has a protection wavelength path (a path with one wavelength’s worth of capacity.) The protection wavelength paths used for different working wavelengths on the same link may use different paths and/or different wavelengths. For example, Fig. 4b shows two different protection paths (5–2–6 and 5–1–2–3–6) for the same link 5–6. Link-based protection schemes can be further classified as dedicated or shared link protection.

*Dedicated link protection* means that a protection wavelength path is dedicated to a working channel on a particular link. Therefore, if the protection paths for (some wavelengths on) two different links overlap, different wavelengths must be assigned to the protection path on the overlapping portion even if the working wavelengths on the two links are the same. As an example, consider Fig. 4c. Let \(\lambda_1\) on path 5–2–6 (labeled protection path 1) be the protection wavelength path for a working channel on link 5–6, and the protection path for a working channel on link 1–2 be 1–5–2 (labeled protection path 2). Then a different wavelength, say \(\lambda_2\), must be assigned to protection path 2, even if the working wavelengths on links 5–6 and 1–2 are the same, say \(\lambda_1\). Note that this requires wavelength conversion if link 1–2 fails.

The above example indicates the difficulty in designing efficient protection schemes in large networks. Efficient design is especially difficult if wavelength conversion facilities are unavailable. On the other hand, dedicated link protection may offer protection against the failure of multiple links. For example, in Fig. 4c both working channels can be recovered if both links 1–2 and 5–6 fail simultaneously. However, note that recovery of working channel 5–6 is not possible if both links 5–2 and 5–6 fail at once.

*Shared link protection* allows different protection paths to share a wavelength on the overlapping portion if the corresponding working channels are on different links. Shared link protection utilizes capacity more efficiently than dedicated link protection, and can provide 100 percent recovery from single-link failures.\(^5\) Figure 4d shows an example of shared link protection. Protection paths 1 and 2 (used to protect a working channel on links 5–6 and 1–2, respectively) can share wavelength \(\lambda_1\) on link 5–2. Note, however, that a different wavelength must be used to protect a different working channel on link 5–6 if protection path 1 is used for that working channel.

\(^4\) These are general techniques applicable to non-WDM mesh topologies as well. Our presentation here is adapted to WDM networks.

\(^5\) Shared link protection may be able to recover from some multilink failures as well, but the protection is typically less than dedicated link protection.
Path-Based Protection — In WDM systems, path-based protection refers to the reservation of a protection path and wavelength (protection wavelength path) for each working wavelength path and each link failure. Upon failure of a link, the source and destination nodes of each affected connection switch to the corresponding protection wavelength paths. As opposed to link-based protection, which involves only the nodes adjacent to the link failure, path-based protection needs a mechanism to notify the affected connection end nodes of the failure. This requires the cooperation of several network nodes, and may not be easily achievable.

The protection wavelength paths for every link failure are usually reserved at connection setup, and should be disjoint with the failed link. Upon link failure, the wavelength paths reserved for this failure scenario are activated. As a special case, when a protection wavelength path is disjoint with every link of the working path, the same wavelength path can be used to restore a connection upon any single-link failure along the working path. Note that in this case, the identification of the failed link is not required to initiate recovery. An example of the special case is shown in Fig. 5a, where the working path is 4–5–6. When the link between nodes 5 and 6 fails, nodes 4 and 6 switch the connection to the protection path 4–1–2–6. The wavelength used on the protection path can be the same as or different from the working wavelength. Also, the protection paths used for different connections using the same working path can be different. Similar to link-based protection, path-based protection can be dedicated or shared.

In dedicated path protection, the backup wavelength on the links of a protection path is reserved for a specific working connection. This implies that two overlapping protection paths must use different wavelengths even if the working paths do not overlap. For example, Fig. 5b shows two working paths, 4–5–6 and 1–2–3, both using $\lambda_1$. The protection wavelength path for connection 1 is $\lambda_2$ on 4–1–2–6 ($\lambda_2$ is a working wavelength on link 1–2 and cannot be used for protection). The protection wavelength path for connection 2 is 1–5–2–6–3. Since these two protection paths have the common link 2–6, and $\lambda_2$ is assigned to protection path 1, protection path 2 has to be assigned a different wavelength (e.g., $\lambda_1$).

Dedicated path protection requires a large amount of extra capacity for protection purposes, and when there is no failure, the protection resources are kept idle. The positive aspect is that it is able to provide recovery from not only single-link failures, but also some multilink failures.

Shared path protection allows the use of the same wavelength on a link for two different protection paths if the corresponding working paths are link-disjoint. Thus, it is possible to utilize the capacity more efficiently, while still achieving 100 percent recovery from single-link failures. An example of shared path protection is given in Fig. 5c. The two backup paths can now share $\lambda_2$ on link 2–6. Therefore, only one wavelength on this link has to be reserved for protection, as opposed to two for dedicated path protection.

Recent Research

The basic techniques for survivability in WDM networks were presented in the previous section. We now take a look at some of the recent research in this area, and present a sampling of the results. Most of the research focuses on resource-efficient approaches to provide a given level of recovery, or the best recovery possible with a given amount of resources (fibers, wavelengths, etc.). We consider predesigned protection approaches first.

Predesigned Protection — The attractiveness of SHR architectures has inspired the decomposition of mesh networks into multiple SHRs [1]. In this approach, a set of rings such that each link in the network is traversed by two rings (one in each direction) is found, and the fibers of one ring are backed up by the fibers on the other. However, when this technique is applied to WDM loopback recovery, wavelength conversion may be required [7]. A generalized loopback recovery scheme for link and node failures that does not require wavelength conversion is presented in [7]. In their scheme, they consider a link- and node-redundant mesh network, that is, one in which the failure of a single link or node does not disconnect the network, and assume that two fibers make up a link. They provide an algorithm to label the fibers (1 or 2) and assign half of the wavelengths as working wavelengths on fiber 1 and the remaining half as protection. Here, each wavelength on fiber 1 is backed up by the same wavelength on fiber 2, and vice versa, throughout the network. The protection scheme here does not distinguish between a link or node failure. As in SONET BSHR, the nodes adjacent to the failed link or node perform the loopback.

A predesigned centralized protection scheme for paths based on redundant trees is presented in [8]. The main idea is to create two directed trees in the network such that the failure of a link or node in the network leaves a source node connected to all other nodes on at least one of the trees.

As discussed earlier, protection can be implemented at either the WDM layer and/or higher layers. There have been some studies on the capacity savings to be achieved in the joint design of the WDM layer and a higher virtual path layer, over the independent design of the two layers. Although independent design is more appropriate when multiple client layers are embedded over the WDM layer, joint design may be useful when both the virtual path network and the optical network are controlled by a single entity. A WDM network on which virtual paths (VPs) serving a higher layer are overlaid is considered in [5]. Since a single link failure can cause the simultaneous loss of service on several VPs, a design algorithm called Disjoint Alternate Path (DAP) is presented. The DAP algorithm aims to maintain connectivity between all network port pairs under a single link failure. The goal is to place VPs on the physical topology such that the number of unconnected node pairs at the higher layer is
minimized. Although it does not consider WDM layer protection, the design does minimize the impact of a WDM link failure on the higher layer. The effectiveness of the joint design is demonstrated by embedding six different test virtual topologies on the ARPA-2 physical network topology. DAP is compared favorably with simple Shortest Path Routing (SPR), which does not perform any survivability optimization. In their experiments, the number of affected node pairs could be made zero by using the DAP algorithm, while it ranges from 3 to 37 for the SPR algorithm.

There are many studies in the literature that focus on metrics such as the cost-effectiveness and the speed of recovery of different protection schemes. These metrics depend on a number of factors such as network topology, the number of wavelengths in a fiber, and wavelength conversion capability. Among such studies is [9] which compares the total number of fibers needed for different protection/restoration schemes. By using an example 15-node polygonal network topology with full wavelength conversion, they show that path-based restoration minimizes the fiber requirement for single-link failures. They also present an OXC architecture to realize the restoration.

The authors of [10] consider two problems: computing restoration-maximizing protection paths, given a set of working lightpaths and network resources, and jointly computing capacity-minimizing working and protection lightpaths for a given set of demands. Distributed algorithms with detailed signaling procedures are presented for both problems, and a centralized approach is also presented for the second problem. Using typical time values for message processing, cross-connection, traffic bridging, and failure detection, they show that their distributed algorithms can restore traffic in under a second for even large networks. For example, in a 301-node network with 372 working lightpaths, the restoration time was 572 ms. They also show that their algorithm can achieve near-optimal restoration. Furthermore, they report that shared path protection requires between 60 and 90 percent more capacity than no protection, and dedicated path protection requires almost 200 percent more capacity than no protection. A significant assumption in their work is the availability of wavelength conversion at all nodes.

The authors of [11, 12] compare different approaches to protect mesh WDM networks against single-link failures. In [11], three schemes (dedicated path protection, shared path protection, and shared link protection) are examined. Assuming a static traffic demand and no wavelength conversion, they compare the wavelength capacity requirements (the sum of the number of wavelengths required on each link) of the three approaches for 100 percent restoration. Their results show that shared path protection provides significant savings in capacity utilization over the other two methods. For example, in a 15-node mesh network, their results (obtained by solving integer-linear programs) show that 59 wavelength links suffice if no protection is needed for a 25-connection demand. The number of wavelength links required in dedicated path, shared path, and shared link protection schemes in the same example are 163, 99, and 189, respectively. In [12], the switching times for the various protection schemes are compared by using their proposed protection switching time model. It is concluded that protection switching times are lowest for shared link protection and highest for shared path protection when cross-connect configuration times are low (10 µs). On the other hand, when cross-connect configuration times are high (500 µs), dedicated path protection has the lowest and shared path protection has the highest protection switching times.

In [13], the authors examine ways of solving the optimal capacity assignment problem for a static connection demand using the method of ring covers [1]. They view the problem as consisting of three subproblems: the ring cover problem, the problem of routing the working lightpaths, and the selection of SHR/WDM spare wavelengths for protection. By using the example of the Pan-European network topology, they show that the joint solution of the three problems can save 15 percent in total wavelength mileage when compared to separate solution of the three subproblems.

The problem of dimensioning the network to handle faults under a static traffic demand is the topic of [14–17]. In [14], the number of wavelengths on each fiber is assumed to be fixed, and the objective is to minimize the total number of fiber ports at the OXCs. Protection design is done after design of the working network. The authors use a separate protection path for each link failure on the working path, but these protection paths may share links. Algorithms for selection of routes and wavelengths for the protection paths with and without wavelength conversion, and with and without transceiver tunability are presented. Transceiver tunability allows the use of different wavelengths for working and protection lightpaths. Using simulations on a 4 × 6 polygrid network, they show that the required number of fiber ports without wavelength conversion is 1.2 to 2.2 times the value with wavelength conversion, with larger ratios resulting when there are more wavelengths per fiber. Transceiver tunability results in only slightly better ratios.

A cost model for fibers and OXCs is proposed in [15], and heuristic algorithms are presented to minimize the cost for each of the following protection approaches: shared link, shared path with a separate protection path for each failed link on the working path, and shared path with a single link-disjoint protection path for each working path. As in [14], the impact of wavelength conversion and transceiver tunability are studied using a heuristic based on an integer-linear programming (ILP) formulation and a simulated annealing (SA) approach. The conclusions, obtained by simulating a sample topology spanning Europe, are qualitatively similar to those of [14] with one exception. Transceiver tunability was found to provide substantial benefits when wavelength converters are absent.

A cost model similar to [15] is proposed in [16], as well as algorithms with the objective of minimizing the network cost for restorable networks. Here also, the working network is assumed to be designed before, and independent of, the protection network. Two designs of the protection network are considered: independent design in which the protection for each failure scenario is designed independently (i.e., dedicated protection), and coordinated design in which the protection network is designed considering all failure scenarios together (i.e., shared protection). Three different restoration schemes are also considered; in full reconfiguration all paths may be reconfigured upon failure, whereas in path-based and link-based reconfiguration, only the affected connections may be reconfigured. Numerical results on an example topology spanning the continental United States for 200 connections with 8 wavelengths/fiber are reported. The total redundant capacity (fiber miles) as a ratio of the total working capacity ranges from 0.92 for full reconfiguration to 1.43 for link-based protection, in the independent design approach, and from 0.70 to 1.23 in the coordinated design approach. An integer programming-based protection scheme is presented in [17]. It attempts to assign working paths and the corresponding link-disjoint protection paths so that the total facility cost including the cost of fibers and OXCs is minimized. It assumes that wavelength conversion is available in each OXC, and no wavelength is released if a working path fails. Restoration is rapidly performed with the help of an operation, administration, and maintenance (OAM) channel between the end nodes of the working path. The simulation
results show that the number of OXCs decreases slightly when \( \gamma \) increases, where \( \gamma \) is the ratio of per unit cross-connection to transmission cost. This suggests that in order to minimize the total facility cost, the number of OXCs must be reduced as \( \gamma \) increases.

The authors of [18] propose a scheme to dynamically establish working and protection lightpaths. They assign a protection lightpath for every working lightpath that demands protection, at setup time, using shared-path protection; that is, the backup lightpaths can be multiplexed onto the same channel as long as their working lightpaths are link-disjoint. The main idea here is called primary-backup multiplexing. Here, a previously assigned protection lightpath may be assigned to a newly requested working lightpath, and therefore may not be available for restoration should a failure occur. The amount of protection provided is represented by a number called the percentage of guarantee which refers to the average number of connections that can be restored when a link fails. An algorithm to estimate this latter number is provided. For a fixed amount of network resources, the connection blocking probability is expected to increase with required percentage of guarantee. The multiplexing advantages are evaluated by measuring the blocking performance for different percentages of guarantee. The mesh-torus and ARPA-2 topologies under different load conditions were used as the test setups in their simulations. The authors observe that under light loads, more than 90 percent blocking performance gain (defined to be \((b_{100} - h_b)/b_{100}\) where \(b_h\) is the blocking probability for percentage of guarantee \(x\)) can be achieved with restoration guarantee \(p > 90\) percent. Even under heavy traffic loads, the blocking performance gain is observed to be more than the restoration guarantee reduction.

Finally, the work in [4] considers all three failure scenarios (link, node, and channel failures) in WDM point-to-point links and ring networks with limited wavelength conversion, and proposes recovery mechanisms for each scenario. The schemes are compared according to the required amount of hardware and management overhead. It also proposes an integrated scheme that can handle all types of failures with limited coordination between nodes.

**Dynamic Restoration** — Survivability using dynamic restoration methods has received much less attention than predesigned protection schemes. In [12], distributed control protocols for path and link restoration are presented. Path and link restoration schemes are compared using two metrics: average restoration time and restoration efficiency, which is defined as the proportion of failed connections that are restored. Using their proposed message processing and switching time model and dynamic Poisson traffic with periodically occurring link failures, they show that path restoration has better restoration efficiency, while link restoration has better restoration time.

**Concluding Remarks**

In this article we examine various survivability techniques for optical networks. These techniques can be classified broadly as predesigned protection and dynamic restoration techniques. Automatic protection switching and self-healing ring are the dominant protection techniques used in the electro-optic SONET network. These techniques may be adapted to WDM networks with some modifications. While the availability of multiple channels in a WDM link provides flexibility in capacity assignment, it also makes the design more complicated, due to possible constraints on wavelength assignment.

Most survivability schemes proposed for WDM optical networks have been predesigned protection against single-link failures. Because of the nature of optical equipment, protection against node and channel failures merits more attention than it has received thus far. It may be possible to think of a channel failure as the failure of the entire link, but that may lead to a potential waste of available system resources. We believe that survivability schemes for channel failures will become an important topic of research in the future.

Dynamic restoration schemes have provided a viable alternative to predesigned protection schemes, but little research has been done on the design of rapid restoration schemes that can provide any level of service guarantee. Finally, survivability under equipment failure due to deliberate attacks on the network has not been considered, and such attacks may warrant entirely different solution approaches.

**References**


**Biographies**

**Dongyin Zhou** received B.E. and M.S. degrees in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 1990 and 1995, respectively. She was a system engineer at Bureau of Telecommunications, Hangzhou, China, from 1990 to 1992, and a software design engineer in SPT Co. Ltd., Shanghai, China. She worked as a project manager in UTStarcom, Shanghai, from 1997 to 1999. She is currently a doctoral student in the Electrical and Computer Engineering Department at George Washington University, Washington, D.C. Her research interests are in optical network design and analysis.

**Suresh Subramaniam** received his Ph.D. degree in electrical engineering from the University of Washington, Seattle, in August 1997. Since September 1997 he has been an assistant professor in the Electrical and Computer Engineering Department at George Washington University, Washington, D.C. His research interests are primarily in optical networks, and his research in that area is supported by the NSA, NSF, and DARPA. He has served on the program committees of several conferences. He is a co-editor of the book Optical WDM Networks: Principles and Practice (Kluwer, 2000), and a co-recipient of the Best Paper Award at the 1997 SPIE Conference on All-Optical Communication Systems: Architecture, Control, and Network Issues. He is also a guest editor of an upcoming special issue of the Journal of High Speed Networks.