**DIFFERENTIATED QoS FOR SURVIVABLE WDM OPTICAL NETWORKS**

Chava Vijaya Saradhi, Institute for Infocomm Research, Mohan Gurusamy National University of Singapore

Luying Zhou, Institute for Infocomm Research

**ABSTRACT**

Optical networks based on WDM technology have become a promising solution to realize transport networks that can meet the ever-increasing demand for bandwidth. As WDM networks carry a huge volume of traffic, maintaining a high level of survivability is an important and critical issue. The development of GMPLS switching technology led to the direct integration of IP and WDM. In these IP-over-WDM networks different applications/end users need different levels of fault tolerance and differ in how much they are willing to pay for the service they get. The current trend in network development is moving toward a unified solution providing support for voice, data, and various multimedia services. Therefore, it is imperative that WDM networks incorporate fault tolerance into QoS requirements with various QoS parameters such as tolerance to single or multiple component failures, protection bandwidth, recovery time, and recovery granularity besides resource utilization and call acceptance ratio. This article presents a survey of various methods that have been proposed for providing service differentiation in survivable WDM networks and discuss their performance. Such methods are broadly classified under various paradigms such as differentiated reliability, R-connections, qualiy of protection, and quality of recovery.

**INTRODUCTION**

In the emerging next-generation transport networks, called intelligent optical networks, wavelength-division multiplexing (WDM)-based optical components like optical add-drop multiplexers (OADMs) and optical crossconnects (OXC}s will have full knowledge of the wavelengths in the network, such as status, and traffic carrying capacity of each wavelength. IP-over-WDM (IP/WDM) networks make use of the highly reconfigurable nature of lightpaths offered by WDM to create secure tunnels of high bandwidth to carry IP traffic across intelligent WDM optical transport networks. In these networks, the traffic demand can be either static or dynamic. In static lightpath establishment (SLE), traffic demand between node pairs is known a-priori, and the goal is to establish lightpaths to optimize a certain objective function. The dynamic lightpath establishment (DLE) problem concerns establishing lightpaths with an objective of increasing the average call acceptance ratio when connection requests arrive and depart dynamically.

Like any communication network, WDM networks are prone to hardware failures (of components, like OXC{s, switches, cable cuts) and software bugs (protocol). A cable cut causes a link failure, making all its constituent fibers fail. A node failure may be occur due to the failure of an OXC. When a component fails, all the lightpaths currently using that component will fail. Because WDM networks carry huge volumes of traffic, maintaining a high level of service availability at an acceptable level of overhead is an important issue.

The optical layer consists of WDM systems and intelligent optical switches that perform all restoration and end-to-end optical layer provisioning. Restoration could be provided at the optical layer or at the higher client layers, such as IP/generalized multiprotocol label switching (GMPLS), each of which has its own merits. The optical layer has faster recovery and provisioning times, and uses the wavelength channels optimally with less signaling overhead. Therefore, many functions are moving to the optical layer. Foremost are routing, switching, and network protection/restoration [1, 2]. High-speed mesh restoration becomes a necessity, and this is made possible by doing the restoration at the optical layer using optical switches. Such restorations can be performed within a duration of 50–200 ms, compared to minutes to tens of minutes in traditional mesh restoration architectures of today. A comprehensive survey of the protection/restoration schemes available in the literature can be found in [2, references therein].

On one hand, the type of applications being deployed across the public Internet today are increasingly mission-critical, whereby business success can be jeopardized by the poor performance of the network. It does not matter how attractive and potentially lucrative our applications are if the network does not function reliably and consistently. In such scenarios IP/WDM networks would not be a viable solution unless they can guarantee fault tolerance, reliability, and availability to end users. Widely scattered users of these networks usually do not care about the network topology and implementation. What they care about is something fundamental, such as:
• Do I get services with guaranteed timeliness and fault tolerance with an acceptable level of overhead?

• Do I have certain reliability for my data passing through the network?

• Do I have the network available when I want to access my mission-critical applications?

On the other hand, the trend in current network development is moving toward a unified solution that will support voice, data, and various multimedia services. Different applications/end users need different levels of fault tolerance and recovery time, and differ in how much they are willing to pay for the service they get. In these scenarios quality of service (QoS) becomes a vital tool to ensure that all applications can coexist and function at acceptable levels of performance. Considerable research efforts have been dedicated to the study of survivability mechanisms in WDM networks. But the need remains for research focused on service differentiation in survivable WDM networks. In this article we present a survey of various methods of service differentiation in survivable WDM networks with respect to differentiated reliability (DIR), quality of protection (QoP), and quality of recovery (QoR); explain the operation of these schemes; and discuss their performance. The rest of the article is organized as follows. We begin by reviewing some commonly used terms and provide motivation for differentiated QoS in survivable WDM networks. Several static and dynamic methods supporting QoS in survivable networks are presented. We briefly describe the possibility of using a GMPLS framework to provide differentiated QoS in IP/WDM networks. Finally, some concluding remarks are made.

**Survivability in WDM Networks: Basics and Terminology**

Fault tolerance refers to the ability of the network to configure and reestablish communication upon a failure. A related term, restoration, refers to the process of rerouting affected traffic upon a component failure. A network with restoration capability is known as a survivable or restorable network. The lightpath that carries traffic during normal operation is known as the primary or working lightpath. When a primary lightpath fails, the traffic is rerouted over a new lightpath known as the backup or secondary lightpath. The process of assigning network resources to a given traffic demand is known as provisioning a network. Given a set of traffic demands, the provisioning problem is to allocate resources to the primary and backup lightpaths for each demand to minimize the spare resource utilization.

A connection request with a fault tolerance requirement is called a dependable connection (D-connection) [1]. Restoration methods differ in their assumptions about the functionalities of crossconnects (wavelength-selective or -convertible), traffic demand (static or dynamic), performance metric (restoration guarantee, restoration time, spare resource utilization, etc.), and mode of network control (centralized or distributed). The methods designed for establishing connections with fault tolerance requirements can be broadly divided into reactive and proactive. In reactive (also known as dynamic [1, 2]), restoration, when an existing lightpath fails, a search is initiated to find a new lightpath that does not use the failed components. This has an advantage of low overhead in the absence of failures. However, this does not guarantee successful recovery, as an attempt to establish a new lightpath may fail due to resource shortage at the time of failure recovery. In addition, these methods also require fault isolation to find exact failure leading to longer recovery time, which may not be required in some of the proactive methods [3]. In a proactive method (also known as protection [2]), backup lightpaths are identified and resources reserved along the backup lightpaths at the time of establishing the primary lightpath itself.

A proactive or reactive restoration method is either link- or path-based. A link-based method employs local detouring, while a path-based method employs end-to-end detouring. Local detouring reroutes the traffic around the failed component, while in end-to-end detouring a backup lightpath is selected between the end nodes of the failed primary lightpath. Local detouring is inefficient in terms of resource utilization [4]. Furthermore, handling node failures is very difficult in local detouring. A proactive restoration method may use a dedicated backup lightpath for a primary lightpath. In a dedicated backup scheme wavelength channels are not shared between any two backup lightpaths. For better resource utilization, multiplexing (or sharing) techniques can be employed. If two lightpaths do not fail simultaneously, their backup lightpaths can share a wavelength channel. This technique is known as backup multiplexing, backup bandwidth sharing, or shared protection [1]. A proactive restoration method can employ primary backup multiplexing or primary backup bandwidth sharing [1] to further improve resource utilization. This technique allows a wavelength channel to be shared by a primary and one or more backup lightpaths.

The two primary measures of dependability are reliability and availability. Reliability of a resource (or component) is the probability that it functions correctly (potentially despite faults) over an interval of time. Availability of a resource (or component) is the probability that it is operational at any given instance of time. Reliability/availability is the probability that enough resources reserved for this connection are functioning properly to communicate from the source to the destination over a period of time. Availability of a connection is the probability that enough resources reserved for this connection are available to communicate from one node to the other at any given instance of time. Reliability/availability has a range from 0 (never operational) to 1 (perfectly reliable). It is assumed (with reasonable justification) that reliability/availability have a cost. Therefore, a more reliable/available connection comes at a greater cost. However, the relation between cost and reliability/availability may not be linear.

In optical networks the following protection alternatives, also known as reliability of service (RoS) classes, have been considered [5]:

- Guaranteed protection
- Best effort protection
- Unprotected connections
- Preemptable connections

In [6] a framework to support the above RoS classes in connection-oriented networks is presented. Many research efforts have widely studied guaranteed and unprotected connections. However, the grade of service for best effort and preemptable connections was recently quantified. In the following we present a brief survey of these methods that tries to include all the service classes on a continuous spectrum of protection grades.

**Reliability of Service (RoS) Grades**

The notion of QoS was proposed to capture a qualitatively and quantitatively defined performance contract between the service provider and the end user applications. The goal of QoS routing is to satisfy requested QoS requirements for every admitted call, and achieve global efficiency in resource allocation and average call acceptance ratio by suitably selecting network routes and wavelengths. The QoS requirements of a connection can be given as a set of constraints, which can be link or path constraints, and additive metrics or multiplicative metrics. For unicast traffic, the goal of QoS routing is to find a route and wavelength that meet the requirements of a connection between the source-destination pair. In this article we consider only unicast traffic. Service differentiation in survivable WDM networks can be provided in many dimensions with any of the following QoS parameters: reliability, avail-
ability, protection bandwidth, recovery time, and recovery bandwidth. In this article we explain various paradigms, such as DiR, QoP, and QoR, aimed at achieving service differentiation in survivable WDM networks.

Consistent with [5], we define the protection alternatives discussed earlier as the protection classes, while the continuous set of protection levels are called protection grades to make a distinction between the two approaches. The reliability of grades can be classified in many ways. There are different paradigms proposed in the literature, which are broadly classified as probabilistic schemes, which provide probabilistic guarantees on any one of reliability, availability, and so on, and absolute schemes, which provide absolute guarantees on any one QoS parameter such as recovery time, protection bandwidth, recovery bandwidth, or recovery success ratio. Service differentiation can be provided at the time of protection or dynamic restoration. Based on these criteria, these schemes are further classified into quality of protection and quality of recovery methods.

THE IMPORTANCE AND ESTIMATION OF RELIABILITY

Fiber reliability from the point of view of loss variation for various cable environment parameters (e.g., temperature, humidity, and radiation) was studied in [7]. Even though the majority of fiber failures have been reported to be due to external factors such as digups or fire, a few have also been due to strength loss of the fiber itself. However, despite the low probability of fiber failure, the associated economic risk is appreciable because of:

- The high cost of fiber repair or replacement
- Large volumes of data passing through optical networks
- Deployment of micro-electro-mechanical (MEM) optical switches that work based on the rotation of mirrors, whose reliability is particularly important

The reliability of optical fiber used in certain biomedical applications is extremely important because failure of the fiber during use might be fatal for the patient. Because of this type of application, long-term reliability is an important factor for practical use of fiber. At the initial stages of provisioning the network, the network provider can use the reliability information provided by the component vendors and available failure statistics of the optical components used in the network. As time goes on, they can also estimate failure probability based on past experiences. So after some years of experience, we can use the estimated failure probability before establishing a lightpath.

DIFFERENTIATED RELIABLE CONNECTIONS

Recently there has been considerable interest in providing various reliability classes to include all the service classes on a continuous spectrum of protection grades. The problem of providing reliable connections in optical ring networks is considered in [8]. Given the occurrence of a single failure in the network, the failure probability of the link under consideration \((i,j)\) is denoted \(P(i,j)\). It is assumed that the probability of a single failure is given; then the failure probability of each link is normalized to the probability of having a single failure in the network. For uniform distribution of failures across the link, the failure probability of a link \((i,j)\) is then \(P(i,j) = \frac{1}{|E|} \forall (i,j) \in E\), where \(E\) is the set of links in the network.

As the failure of different links is mutually exclusive and disjoint under the single link failure assumption, the failure probability of a path is given by the sum of the failure probabilities of all the links along the path.

In the DiR scheme each connection is assigned a maximum failure probability (MFP) and determined by the application requirements but not by the protection mechanism. A connection with \(MFP(c)\) is characterized as a connection in reliability class \(c\) and indicates that in the event of a component failure, it will sustain with a probability of \(1 - MFP(c)\) under the single failure assumption. Each connection is then routed and assigned wavelengths in such a way that the MFP requirement is met. The lower-class connections are assigned protection wavelengths used by the higher-class connections. However, in case of failure, a higher-class connection is allowed to preempt a lower-class connection if the later is using protection resources dedicated to the former.

As an example, consider Fig. 1 with uniform failure distribution. Assume that the higher-class connection \((h_p)\), between nodes 1 and 4; the shortest path is 1–7–4) must be 100 percent protected, so it is assigned a protection path \((h_p, 1–2–3–4)\). The lower class connection \((h_b, 2–3–4–5–6)\) reuses the protection wavelengths assigned to the higher-class connection on links (2, 3) and (3, 4). The failure probability of the lower-class connection is thus given by \(P_f = P_f(2, 3) + P_f(3, 4) + P_f(4, 5) + P_f(5, 6)\) (failure probability of the unprotected links of the lower-class connections) plus \(P_f(1, 7) + P_f(7, 4)\) (probability of being preempted by a higher-class connection).

DiR APPLIED TO DESIGNING OPTICAL RING NETWORKS

In [8] DiR is applied to the design of optical ring networks, with the objective of finding the routes and wavelengths used by the lightpaths in order to minimize the total ring wavelength mileage, subject to guaranteeing the MFP requested by the connection; that is, the problem is considered a provisioning problem, and called a DiR design problem. The authors in [8] presented a greedy algorithm, Difficult-Reuse-First (DRF), to suboptimally solve the DiR design problem in WDM rings. In DRF, the requests are classified into two sets: the set of demands that require protection (\(PSet\)) and the set of demands that do not require protection (\(NPSet\)). For all the connections in \(PSet\), working lightpaths are routed using shortest paths in terms of number of hops, and protection lightpaths are routed in the opposite direction (in a ring only two disjoint routes exist between any node pair). The demands in the \(NPSet\) are sorted in increasing order according to the difference \(X = (MFP(c) - mfp_{sd}) \geq 0\), where \(mfp_{sd}\) is the minimum failure probability path between nodes \(s\) and \(d\). The value \(X\) indicates the excess of reliability provided to the demand if a new wavelength is added to all the links along the minimum failure probability path. Now the algorithm looks for ways to reduce (not below zero) the excess reliability offered to the connection by reusing the already provisioned protection wavelengths in place of the newly added wavelengths. To do this efficiently, the authors have proposed to construct an auxiliary graph from the original graph. The demands under consideration are routed using a shortest path algorithm on the auxiliary graph. Here, the links weights used by the shortest path algorithm are a linear combination of link length and link failure probability.
As expected, the simulation results show the potential advantage of the proposed scheme in terms of overall network costs when considering reliability requirements. Several performance metrics are used to evaluate the performance: total wavelength mileage, total protection wavelength mileage, total reused mileage, and failure probability distribution. As the reliability requirement becomes $l$:

- The protection wavelength mileage required to fulfill the requested reliability degree is reduced.
- Reuse of protection wavelengths is improved.

The proposed approach also differentiates connections with different reliability requirements, whereas shortest path routing is not able to differentiate connections with different reliability requirements.

**DIR APPLIED TO SHARED PATH PROTECTION IN OPTICAL MESH NETWORKS**

The concept of DIR is extended to shared path protection in arbitrary mesh networks in [9]. With the combination of DIR and shared path protection we can expect reduction in the total network cost, as both aim at reducing the network cost by using resources efficiently. A two-step algorithm based on simulated annealing is proposed to minimize the cost of the network. The algorithm searches for the primary and backup paths to be assigned to each demand under the single failure assumption. In the first step the algorithm assigns routes and wavelengths to all the connection demands, allowing the sharing of backup resources to provide 100 percent reliability to all demands. In the second step it tries to reduce the reliability of the connection demands to the required level of reliability. Simulation results show that the proposed algorithm allows reducing network cost in a way that is inversely proportional to the reliability required by the demands.

### RELIABLE CONNECTIONS

In [10], the authors incorporate the reliability of connections as a parameter of QoS and describe a scheme for establishing connections with such QoS requirements. A connection with reliability requirements is called a reliable connection (R-connection).

In this scheme multiple faults are allowed to occur in the network at any instant of time. Here, the reliability of a resource (or component) is defined as the probability that it functions at any instant of time. Here, the reliability of a resource (or component) is defined as the probability that it functions correctly (potentially despite faults) over an interval of time. Let $r_i$ be the reliability of the link; then the reliability of a path consisting of links with reliabilities $r_1, r_2, \ldots, r_n$ will be $\prod_{i=1}^{n} r_i$.

The algorithm in [10] establishes an R-connection with a primary lightpath and an optional backup lightpath. A backup lightpath is provided when the reliability specified by the application requires that a backup lightpath be provided, and it can be either end-to-end or partial, covering only part of the primary lightpath. The length of the primary lightpath covered by the backup lightpath can be chosen to enhance the reliability of the R-connection to the required level and depends on the reliability required by the application/end user, but not on the actual length of the primary, network topology, and design constraints. If certain portions of the primary lightpath are considered less reliable (more vulnerable), backup lightpaths are provided for only those segments of the primary lightpath.

To provide backup lightpaths, resources need to be reserved along the backup lightpaths as well. This is an added cost, and a partial backup scheme preserves resources by using only the required amount of backup lightpaths. Thus, it reduces the spare resource utilization and thereby increases the ratio of the average call acceptance ratio (ACAR). In this scheme, many R-connections will have only a partial backup lightpath rather than an end-to-end backup lightpath. This means that if there is a fault in the part of the primary lightpath not covered by the backup lightpath, the R-connection cannot be restored immediately: the whole path has to be reestablished. But note that those connections with end-to-end backup lightpaths also have to be reestablished if more than one link fail simultaneously.

### R-CONNECTIONS WITH PARTIAL BACKUP LIGHTPATHS

We now explain how to find the reliability of an R-connection from the source to the destination, as shown in Fig. 2 with a partial backup lightpath. The reliability of a segment consisting of links with reliabilities $r_1, r_2, \ldots, r_n$ will be $\prod_{i=1}^{n} r_i$. Let $r_p$ denote the reliability of the primary lightpath, $r_b$ denote that of the primary segment covered by a backup lightpath, $r_p$ that of the backup lightpath, and $r_c$ that of the composite path comprising the primary and partial backup lightpaths.

$$r_c = \frac{r_p}{r_s} \left( r_p + r_b \cdot (1 - r_s) \right).$$

(1)

A primary segment is a sequence of contiguous links along the primary lightpath. A partial backup lightpath covers only a primary segment (i.e., the backup lightpath can be used when a component along the primary segment encounters a fault. Figure 2 shows the benefit of the partial backup lightpath. An R-connection has to be established from the source to the destination. The primary lightpath consists of seven links, 1–7. Here, links 3, 4, and 5 and their end nodes form a primary segment. The partial backup lightpath, consisting of links 8–10 and their end nodes, covers the above primary segment. The end-to-end backup lightpath (which is disjoint from the primary lightpath) consists of seven links, 11–17, and covers the entire primary lightpath. Here, $r_p = \prod_{i=1}^{7} r_i$, $r_b = r_3 \cdot r_4 \cdot r_5$, and $r_c = r_3 \cdot r_4 \cdot r_5$.

Let $r_c$ denote the reliability requested by an application/end user. We now observe how partial backup lightpaths are useful. Suppose the reliability of each of the links is 0.9800, and the required reliability $r_c$ is 0.9150. Then for the R-connection shown in Fig. 2, using partial backup lightpath, $r_p = 0.8681$, $r_b = 0.9411$. Then using Eq. 1, $r_c = 0.9192$. Thus, having a partial backup for any three links is just enough in this case as the required reliability is 0.9150.

### R-CONNECTIONS WITH FULL BACKUP LIGHTPATHS

Using the same terminology as partial backup lightpaths, let $r_p$ denote the reliability of the primary lightpath. Let $r_b$ denote that of the primary segment that is covered by a backup lightpath which in this case is the same as $r_p$ (i.e., $r_c = r_p$). Let $r_b$ denote that of the backup lightpath and $r_c$ that of the composite path comprising primary and partial backup lightpaths.
Now, consider the R-connection shown in Fig. 3 using an end-to-end backup lightpath. Since the entire primary lightpath is covered by the backup lightpath, the reliability of the primary segment is equal to that of the primary lightpath, \( r_e = r_p = 0.8681 \). The reliability of the full backup lightpath (in this case with the same number of links as the primary lightpath), \( r_b = 0.8681 \). Then using Eq. 2, \( r_c = 0.9826 \), which is much more than the reliability required by the R-connection. Note that the end-to-end scheme is not able to distinguish the R-connections with different reliability requirements.

**R-Connections with No Backup Lightpaths**

Now, consider the same R-connection shown in Fig. 3, using no backup lightpath. As there is no backup lightpath, \( r_b = 0 \). So, the composite reliability \( r_c = r_p = 0.8681 \), which is less than the reliability required by the R-connection. The ACAR of no backup schemes is very low as most of the connections are rejected. This is mainly because a no backup scheme will not be able to satisfy the reliability requirements of different connections.

**Performance Study**

From the above examples it is clear that a partial backup scheme preserves resources by using only the required amount of backup lightpaths. By doing so it reduces spare resource utilization and thereby increases the ACAR. The effectiveness of the scheme has been evaluated through extensive simulations. In [10] the authors assume that none of the nodes have wavelength conversion capabilities. The performance metrics taken are ACAR, spare wavelength utilization (the percentage of wavelengths used for backup lightpaths), and reliability distribution. Simulation results shows that the partial backup scheme is capable of achieving better resource utilization and ACAR, and also achieves service differentiation in terms of reliability by providing only the required amount of backup lightpaths. The size of the network also plays an important role, and the proposed scheme performs significantly better than the end-to-end backup scheme and the no backup scheme for large networks at low and moderate loads.

**Quality of Protection**

In [5] the authors presented a unified paradigm to include all the service classes on a continuous spectrum of protection grades. QoP is defined as the probability that the connection will survive through a failure. There are many motivations for having a continuous range of protection grades. First, 50 percent of bandwidth is wasted in synchronous optical network (SONET) rings in order to provide 100 percent protection to traffic. Due to the huge costs of WDM equipment, future WDM networks are expected to be sparser. For sparse networks, even mesh protection requires huge amounts of protection bandwidth. Second, Internet traffic is often more sensitive to reliability, and furthermore most of the failures observed are at the IP layer and cannot be recovered at the optical layer.

**Primary-Backup Bandwidth Sharing**

In this method a wavelength channel is allowed to be shared by a primary lightpath and one or more backup lightpaths [1]. Because of this, connections are allowed to become unprotected due to a failure. A lightpath pair is admissible only if its establishment does not take the network to a state where the average number of non-restorable lightpaths per link exceeds a predefined threshold value. By appropriately choosing a threshold value, a desired trade-off can be achieved between restoration guarantee and blocking probability. Efficient routing and connection admission algorithms are presented. The performance of the algorithm was verified through extensive simulation experiments on mesh-torus and ARPA-2 networks. Relative performance gain and reduction in restoration guarantee are used as performance metrics. The results show that the performance gain is attractive enough to allow some reduction in restoration guarantee. They showed that under light load conditions, more than 90 percent performance gain is achieved at the expense of less than 10 percent reduction in restoration guarantee. They also showed that as network connectivity increases, performance improves.

**Design of Logical Topologies with QoP**

In the QoP scheme, each connection \( C \) is associated with a QoP grade, \(-1 \leq Q(C) \leq 1 \). \( Q(C) = 0 \) means that the connection is survivable, while \( Q(C) < 0 \) means that the connection is preemptable. In general, different protection classes are mapped to different QoP grades as:

- \( Q(C) = 1 \): guaranteed
- \( 0 < Q(C) < 1 \): best effort
- \( Q(C) = 0 \): unprotected
- \(-1 < Q(C) < 0 \): preemptable
- \( Q(C) = -1 \): unused channel

In this model, upon a failure each survivable connection is guaranteed to have a deterministic reduced protection bandwidth \( RSB(C) = SP(C) \cdot B(C) \), where \( B(C) \) is the bandwidth required for the connection and \( SP(C) \) is reduced bandwidth available for the connection. In the same way, upon a failure each preemptable connection is guaranteed to have at most a reduced working bandwidth \( RWCC(C) = PP(C) \cdot B(C) \), where \( PP(C) \) represents reduction of working bandwidth in case of failure. Many problems remain open to further research in defining efficient algorithms for choosing which survivable connections to protect and which preemptable connections to drop. The authors have applied the concept of QoP to ring networks and mesh networks.

**Designing Logical Topologies with QoR**

Several heuristic algorithms for the design of logical topologies with QoR for every node pair in terms of recovery time are presented in [11]. In this scheme highest priority class guarantees the minimum failure recovery time and is represented by \( QoR_1 \), whereas \( QoR_n \) provides no lightpath protection and the recovery is left to the higher layers. In general, \( QoR_n \) guarantees the maximum recovery time associated with the class \( n \). The recovery time, \( RT \), of class \( n \) is given by \( RT(QoR_n) = \alpha + \beta \cdot f(n) \), where \( \alpha = QoR_1 \) is the minimum recovery time, \( \beta = SW \) (the step width of RT), and \( f(n) = n - 1 \) are used. But in general, all these parameters can be anything based on the network topology and connectivity, and are decided by the network administrator.
For a given network topology, there may be no disjoint route that can be used for backup lightpaths and guarantee the maximum recovery time specified by the QoR class. As an example, in Fig. 3 there are two routes from the source node to the destination node. Assume that the propagation delay of the primary route is 30 ms and that of the full backup route 35 ms; if the source-destination pair requires a QoR class with a maximum recovery time of 25 ms, no route can provide the required RT. To provide QoS as described earlier, a primary lightpath P is divided into several segments and protected by several backup lightpaths, Bx, (1 ≤ x ≤ H), where H is the number of hops individually, such that the maximum RT of each backup segment does not exceed a threshold value. In this method the maximum recovery time for primary lightpath P is RT max(P) = max{RTx, 1 ≤ x ≤ H}.

Three heuristic algorithms, first-fit, max-shared, and layered graph, are presented [11]. The objective of logical topology design here is to minimize the number of wavelengths required when the traffic matrix and QoS requirements for each node pair are given. In all three, node pairs are sorted based on QoR requirements; then routes and wavelengths are assigned in descending order of QoR requirements. The backup routes for different segments are computed using a shortest path algorithm, and the wavelengths assigned to the backup paths are the same as those assigned to the primary path. The performance of the different heuristic algorithms is evaluated running simulation experiments on the NSF network. When QoS requirements are high, more backup lightpaths must be configured in the network to offer the required QoS. The layered graph heuristic algorithm finds primary and backup lightpaths such that wavelength resources are used more efficiently than in the other heuristics algorithms.

**Dynamic Routing with Partial Traffic Protection**

In [12] a scheme is proposed to support QoS by providing differentiated reliability services where only a fraction α of data is protected. When a connection request arrives, the edge router (ER) begins a path selection process for the working path. First, the edge router tries to allocate the flow to the existing lightpaths if a lightpath with enough available capacity exists. If there is no lightpath available with enough bandwidth, the routing and wavelength assignment process is invoked. After assigning the lightpath to the primary path, the same procedure is repeated with the link disjoint path with the amount of bandwidth required taken as the fraction α of the primary path. The performance of the proposed scheme is evaluated on a 14-node NSF network. The fraction α is set to 0.7; thus, the bandwidth of the protection path is only 70 percent that of the primary path. As the amount of bandwidth required for the backup path is only a fraction of the primary path’s, the scheme outperforms 1:1 protection with respect to blocking probability and resources reserved for backups.

We now explain with an example how to apply the QoP scheme to different connections. Consider Fig. 1 with three connection requests, C1, C2, C3, and source-destination pairs, (1, 3), (2, 4), (1, 7) respectively. Assume that the capacity of each wavelength is 10 Gb/s and all the connections require only a 3 Gb/s for primary paths. Primary paths chosen for the connections are 1 – 2 – 3 – 2 – 3 – 4, and 1 – 7, respectively. Backup paths for the connections are 1 – 7 – 4 – 3 – 2 – 1 – 7 – 4, and 1 – 2 – 3 – 4 – 7, respectively. Assuming that each connection requires only 50 percent of data to be protected, that is, α = 0.5; the primary bandwidth required on the links (1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (1, 7), and (7, 4) is 3, 6, 3, 0, 0, 3, and 0 Gb/s., respectively; similarly, the protection bandwidth required is 3, 1.5, 3, 0, 0, 3, and 4.5, respectively.

**Dynamic Quality of Recovery**

If service differentiation is provided in dynamic restoration methods, it is called quality of recovery. The QoS parameters in recovery can be recovery time, the time between occurrence of a failure and recovery [11, 13]; recovery success probability, probability that the failed connection is recovered [13]; and bandwidth degradation, the amount of traffic recovered [12]. In the following we explain the methods of providing service differentiation at the time of recovery.

**DIR Applied to Dynamic Restoration Schemes**

The concept of DIR can be extended to dynamic restoration schemes in which, upon failure occurrence, a search is initiated to find a backup lightpath that does not use failed components. Several connections may fail because of a component failure or fiber cut. Consequently, all the disrupted connections may look for spare resources concurrently, resulting in contention during recovery. Preemption policies can be used to resolve contention and provide service differentiation in terms of recovery time and recovery success probability. In [13] service differentiation in both recovery success probability and recovery time is accomplished by using three preemption policies: restoration preemption (RP), working preemption (WP), and restoration and working preemption (RWP).

In RP, restoration attempts made by higher-priority connections can preempt channels already reserved by backup routes chosen by lower-priority connections, forcing lower-priority connections to choose an alternative backup. In WP, restoration attempts made by higher-priority connections can preempt channels already reserved by primary routes chosen by lower-priority connections, forcing lower-priority connections to activate the restoration procedure to find a backup route. In WP, connections that are not directly disrupted by the fault may be indirectly disrupted by preemption. RWP is a combination of RP and WP. The choice of which preemption policy to use by a higher-class connection depends on a networkwide probabilistic parameter, δ. When resource contention occurs, the restoration attempt of a higher-priority connection first applies RP; if it fails, a second attempt with probability δ is made using WP.

A restoration protocol with preemption policies has been presented to recover disrupted connections. Three performance metrics — restoration blocking probability, recovery time, and failure propagation ratio (failure propagation of class 1 is the ratio between preempted primary connections to the connections disrupted by a link failure) — are used to evaluate the performance of the proposed scheme. Simulation experiments are conducted on the NSF network. Simulation results show that RP and WP are able to differentiate both restoration blocking probability and restoration time. However, RP is not able to differentiate between class1 and class0 connections in terms of both restoration blocking probability and recovery time; whereas WP is not able distinguish between class1 and class2 connections in terms of both restoration blocking probability and recovery time. In contrast to both RP and WP, RWP permits the achievement of the differentiation of different classes in terms of both restoration blocking probability and recovery time, and also makes it possible to minimize the FPR by choosing an appropriate value for the networkwide probabilistic parameter, p.

**Applying QoP Concepts in QoR**

In general, all the methods discussed in QoP can be used with the recovery methods where there is no a priori reservation of backup resources. In this method, after a failure all the disrupted connections are restored with different QoS parameters. One kind of service differentiation can be achieved in the amount of data protected. In case of failure,
instead of recovering 100 percent of data, we can differentiate the connections based on recovery bandwidth. The concept of QoP [5] can be extended to provide different reduced working bandwidth and reduced protection bandwidth to survivable and preemptable connections. The concept of QoP with different recovery times [11] can be combined with restoration methods to provide different recovery times after a failure.

**DIFFERENTIATED QoS IN IP-OVER-WDM NETWORKS**

IP/WDM networks may adopt either a peer or an overlay model. In the peer model, a label switch router (LSR) and an OXC are treated as a single network element. In this model, OXCs and LSRs freely exchange all information, and run the same routing and signaling protocol; that is, the topology perceived by the layers is a single integrated IP/WDM topology, with the lightpaths viewed as tunnels. In the overlay model, the IP and optical layers are managed and controlled independently. There are two distinct control planes, each corresponding to a different layer. The ingress edge LSR requests the optical core to set up a lightpath to the egress LSR through the user–network interface (UNI).

In IP/WDM networks, both the peer and overlay approaches can be used for traffic engineering. Traditional IP networks employ routing algorithms such as Open Shortest Path First (OSPF) that are insensitive to dynamically changing traffic flows. The IP/WDM networks can use the traffic engineering capabilities of GMPLS to provide service differentiation; for example, the GMPLS constraint-based routing can find paths that satisfy certain specifications subject to certain constraints [14]. The GMPLS control plane supports not only the packet switching, but also time slot switching, lambda switching, and switching in the space domain. In GMPLS-capable networks, label switched paths (LSPs) at sub-\(\lambda\) bandwidth granularity could be created between edge LSRs. A number of such LSPs can be aggregated onto a lightpath. Differentiated QoS can be provided at the LSP or lightpath level. The various methods presented in this article for providing differentiated QoS can be suitably modified to provide differentiated QoS at the LSP level. As GMPLS supports both integrated services and differentiated services, we can define many service classes. The complete implementation of different service classes is beyond the scope of this article.

Several research efforts have been dedicated to the study of differentiated survivability mechanisms at the optical layer. Many standardization bodies, such as the Internet Engineering Task Force (IETF), are working on shared protection mechanisms and fast recovery mechanisms. However, there is still a need for focused research on the interworking, coordination, and functionality partitioning of these service differentiation mechanisms in multilayer networks.

**SUMMARY AND CONCLUSIONS**

For the potential use of the huge bandwidth provided by next-generation IP-over-WDM networks, service providers should support different applications. Different applications/end users need different levels of fault tolerance and differ in how much they are willing to pay for the service they get. Keeping this growing demand for service differentiation in mind, in this article we present a survey of various service differentiation schemes in survivable WDM optical networks. We explain the algorithms used by these schemes, and discuss their performance and how they achieve service differentiation. We explain the concepts of differentiated reliable connections, quality of protection, and quality of recovery.

Although the goals of all these methods are to satisfy the requested QoS parameters for every admitted call and achieve global efficiency, the metrics used, the scenarios applied, and the assumptions about traffic demands are different. For example, DiR schemes are applied to static traffic and aimed for the design of optical ring networks. The R-connection paradigm is applied to dynamic traffic, and is aimed at reducing spare wavelength utilization while achieving service differentiation in terms of reliability. QoP and QoR mainly try to provide service differentiation by protecting data at different granularities and recovery times, respectively.

**REFERENCES**


**BIographies**

MOHAN GURUSAMY [M] (elegm@nus.edu.sg) received a Ph.D. degree in electronics and communications engineering from the College of Engineering, Jawaharlal Nehru Technological University, Hyderabad, India, and his M.S. (by research) degree in computer science from the Indian Institute of Technology (IIT), Madras, India. He worked as a Project Associate at IIT, Madras, from January 2000 to June 2002. Currently he is a senior research engineer at the Institute for Infocomm Research (I2R), formerly known as Kent Ridge Digital Labs, Singapore. He is also pursuing his Ph.D degree at the National University of Singapore (NUS). He is extensively involved in the development of signaling protocols for a GMPLS-based optical network testbed in the Optical Network Focus Interest Group (ONFIG) project. His current research involves lightweight protocols for sensor networks, sensor data management, and data quality. His research interests include optical networks, wireless networks, real-time systems, sensor networks, sensor data management, and data quality.

MOHAN GURUSAMY [M] (elegm@nus.edu.sg) received a Ph.D. degree in computer science and engineering from IIT, Madras, in 2000. From 1991 to 2000 he served as a lecturer in the Department of Computer Science and Engineering, Regional Engineering College, Tiruchirappalli, India. From January to June 2000 he worked as a senior project officer in the Department of Computer Science and Engineering, IIT, Madras. He joined the National University of Singapore in June 2000, where he is currently an assistant professor in the Department of Electrical and Computer Engineering. He held a visiting position at Iowa State University, January–June 1999. His current research involves high-speed multilamewidth optical circuit and burst switching networks.

LUYING ZHOU (lzhou@i2r.a-star.edu.sg) received B.S. and M.S. degrees in automatic control in 1982 and 1985, respectively, from South China University of Technology, Guangzhou, and a Ph.D. degree in automatic control in 1990 from Xi’an Jiaotong University, Xi’an, China. He is currently a professor at I2R, Singapore. His research interests are in computer communication networks, including wireless, WDM, and optical access networks, specifically in network protocols, performance analysis, and applications.