Quality of Service Based Protection in MPLS Control WDM Mesh Networks

Wushao Wen\textsuperscript{1+}, Biswanath Mukherjee\textsuperscript{2}, and S. J. Ben Yoo\textsuperscript{1}

\textsuperscript{1}Dept. of Elect. & Comp. Engineering, University of California, Davis, CA 95616, U.S.A.
\textsuperscript{2}Dept. of Computer Science, University of California, Davis, CA 95616, U.S.A.
email: wswen@ece.ucdavis.edu

Abstract

Intelligent methods for automatic protection and restoration are critical in optical transport mesh networks. This paper discusses the problem of quality of service (QoS)-based protection in term of the protection-switching time and availability for end-to-end lightpaths in a WDM mesh network. We analyze the backup lightpath-sharing problem in such networks and study the correlation of the working lightpaths and the impact of the correlation on the sharing of the backup lightpaths. We present a multi-protocol-label-switching (MPLS) control-based fully-distributed algorithm to solve the protection problem. The proposed algorithm includes intelligent and automatic procedures to set up, take down, activate, restore, and manage backup lightpaths. It greatly reduces the required resources for protection by allowing the sharing of network resources by multiple backup lightpaths. At the same time, it guarantees, if possible, to satisfy the availability requirement even with resource sharing by taking the correlation of working lightpaths into consideration. A simple analysis of the proposed algorithm in terms of computation time and message complexity indicates that the implementation of the algorithm is practical. The illustrative studies that compare the performance of 1:1, unlimited sharing, and QoS-based sharing backup algorithms indicates that QoS-based sharing achieves comparable performance as unlimited sharing, which is much better than the 1:1 backup scheme in terms of connection blocking probability, average number of connections in the network for a given offered load, and network-resource utilization.

Keywords

IP network, MPLS network, WDM network, IP over WDM architecture, quality of service, distributed network control, mesh network.

I. INTRODUCTION

The conventional data networks use Internet Protocol (IP) over Asynchronous Transfer Mode (ATM) over Synchronous Optical Networks (SONET) or Synchronous Data Hierarchy (SDH) over Wavelength-Division-Multiplexing (WDM) architecture (IP/ATM/SONET/WDM). This four-layer architecture evolved from the architecture of voice-centered communication networks and is now widely implemented. There are some benefits with this four-layer network architecture in term of protection and restoration functions. It facilitates protection and restoration operation for the data network. In this architecture, layer-0 protection provided by optical automatic protection can be very fast. Layer-1 protection provided by SONET (SDH) is very effective and fast, with less than 50 ms automatic protection-switching-time standard. Layer-2 protection and restoration functions provided by ATM layer offer more flexible schemes in selecting an alternative virtual path or circuit identifier (VPI/VCI) in case a VPI or a VCI fails. Layer-3, IP layer, is relatively robust against network failures, while it is relatively slow in response [1].

However, the four-layer architecture has several serious limitations. First, it needs too much additional resources, much more than the typical 100% extra resources required for standard SONET protection, and it is not optimized for data networks. This is because it must reserve a certain degree of protection resources at each layer. Furthermore, the original SONET or SDH network is designed for voice communication and is optimized for constant-bit-rate applications such as conventional voice communication. Although SONET or SDH provides rich traffic-grooming functions to groom low data-rate connections into high data-rate connections, it incurs some framing overhead (greater than 3.33%). This grooming method may no longer be appropriate for data-centric traffic, which is bursty with high bandwidth for a short time, followed by a relatively long

\textsuperscript{+}Contact author. This works has been supported in parts by Alcatel, BellSouth, Cisco, and UC MICRO program.
silent period. The communication network today carries more data than voice traffic as the result of increasing penetration of data communication application. Furthermore, data traffic is increasing much faster than voice traffic today. This trend will continue. Therefore, the next generation data networks should be optimized for data-centric traffic. Second problem is the difficulty in circuit provisioning. Currently, it takes 3-6 months to provide a typical SONET-based optical circuit, and all protection or restoration circuits must be pre-configured and set up permanently, which is not an cost-effective method. The third problem is the protectional race condition. Protectional race condition is the situation where multiple protection mechanisms of more than one layer are simultaneously triggered due to a lower layer network element failure. For example, if a lightpath fails, without proper coordination, all four layers’ protection functions might be activated at the same time. Protection race condition is difficult to avoid in the four-layer architecture since there is no proper coordination between different layers, and their protection functions might overlap. The race condition is critical between WDM layer and SONET or SDH layer. WDM layers can provide restoration and protection switching in 2 \( \mu s \)-60 ms. However, the SONET layer detects failure in the 2.3 \( \mu s \)-100 ms range, and then it may trigger the protection switching immediately right after the failure detection. Therefore, even though WDM layer can switch traffic in less than 1 ms, SONET layer protection might still be triggered [9]. This kind of race protection has been demonstrated in [10] experimentally. Lastly, the ATM layer provides excellent but complicated service to data networks. However, it incurs too much overhead, limits scalability, and is not optimized for IP-centric traffic. With the enhanced functions of IP or multi-protocol-label-switching (MPLS) layer, such as constraint-based routing, traffic engineering, quality of service (QoS) support, virtual private network (VPN) applications, the ATM layer is no longer an essential layer for data networks and should be omitted to increase the efficiency of the network operation.

Now, the networking industry is moving to the IP (MPLS) over WDM network architecture [11], [16], [32], [34]. However, with the removal of SONET or SDH, and ATM layers, a number of functions that are originally provided by these two layers must be implemented either by IP (MPLS) layer or by WDM layer. One such function is the protection and restoration function provided by SONET or SDH layers. SONET or SDH network can use line APS to protect the entire facility at line layer and monitor point-to-point status of a STS-N line by using 1:1 line protection. However, the ring protection schemes are more widely used in SONET or SDH network. There are two major ring-based protection schemes in SONET or SDH protection, Unidirectional-Path-Switching-Ring (UPSR) and Bi-directional-Line-Switching-Ring (BLSR) [2], [4], [5]. Both UPSR and BLSR provide excellent protection results, enabling the protection switching time to be less than 50 ms. However, as indicated previously, ring-based protection schemes are difficult to manage and provision, and they require reserving additional 100% resources. Therefore, ring-based protection schemes are not very good choices in optical data networks, which are mesh-based, and require fast provisioning, convenient management, efficient resource utilization, and differentiated protection. Protection in IP-over-WDM network has begun to attract more interest in industry and academics [6], [7], [8], [12], [13], [14], [16], [20], [21], [22], [23]. However, no practical and uniform solution is available to date. This paper proposes a new framework and algorithm to solve this problem in a MPLS control-based WDM mesh network by using a distributed network control mechanism.

Before exploring further, we want to clarify two keywords—protection and restoration. This study regards protection and restoration as two different mechanisms. Protection is a proactive procedure to increase the connection availability and to minimize the data lost. A protection backup path is set up while setting up the working path, whereas restoration is a reactive procedure, which is only triggered by the failure of the previously established connection [20], [21] or a network state transition so that some of the previously available network resources no longer exists. In our study, we assume that there are two possible cases to trigger the restoration of a backup lightpath: the failure of a network component and the preemption of some protection resource. It is possible that a mesh WDM network might be protected by redundant resources in the pure physical layer. For example, the network might use 1:1 protection for some critical fiber link and use automatic switching to switch a path from the working fiber to the backup fiber. We assume that such kind of failure management is done by the physical layer and will not trigger the backup path activation of our proposed scheme.
II. RELATED WORK

For distributed network control on optical network, R. Ramaswami and A. Segall proposed an architecture for controlling a wavelength-routed optical networks in [15]. This work focused on the mechanisms for controlling optical connections by using distributed control protocols. G. M. Berstein, et al. in [32] examined the issues and challenges involved in developing a standardized optical network control plane. Properties and challenges of optical transport networks were explained in the context of functions in provisioning models, circuit provisioning processes, signaling mechanisms, neighbor and service discovery processes, and resource and topology discovery processes. N. Ghanbi, et al. also explained issues on IP-over-WDM integration in [16].

For WDM network protection, S. Ramamurthy, et al. investigated different approaches to protect mesh-based WDM optical networks for a single-link failure [20], [21]. Various path-protection/restoration and link-protection/restoration schemes were investigated and compared. An integer linear program (ILP) to determine the capacity requirements for the various path-protection scheme for a static traffic demand was proposed [20]. The analysis of the protection-switching time for different protection schemes, distributed restoration protocols and their characteristics, including restoration time and restoration efficiency of the protocols were studied in [21]. O. Gerstel, et al. provided a perspective on optical-layer protection and restoration based on services offered by carriers using optical layer in [8]. They also examined several aspects of optical-protection techniques from an implementation perspective in [9]. O. Crochat, et al. have done some outstanding work on the protection for WDM optical networks. In [6], they addressed the problem of multiple simultaneous failures caused by a single component (OXC, fiber, etc.) failure in a WDM optical network because of the correlation of working lightpaths (lightpaths that share some common network components). A disjoint alternative path (DAP) algorithm was proposed to solve the problem. They presented their extended work in [7] and analyzed three types of failure propagation, called “bottleneck”, “connectivity”, and “multiple group” which were caused by the component failure of correlated lightpaths, and presented a solution based on the definition of appropriate requirements at network design and a WDM channel placement algorithm (PIW).

Y. Ye in [23] also presented an overview of existing optical protection and restoration schemes. A mesh-based, hybrid, optical-protection scheme that can utilize multi-fiber physical links with hierarchical OXC structure was also presented. IP standard-based approach for closer IP-WDM integration and a joint protection and restoration scheme coordinated by IP and WDM layers was also discussed. There are also some good survey papers on IP (MPLS) over WDM networks published recently; interested readers can refer to [12], [13], [14].

The work presented here provides an integrated model and algorithm for QoS-aware protection in WDM optical mesh networks by using an MPLS control-based signaling mechanism. By our novel definition of wavelength-link parameters and detailed analysis of the correlation of working lightpaths to the sharing of their backup lightpaths, our scheme provides a unified and integrated solution to the protection and restoration problem in mesh-based WDM networks.

The rest of this paper is organized as follow. Section III describes the protection state information required in WDM mesh networks. Section IV analyzes the QoS-based protection problem and studies the impact of the backup lightpath sharing to the QoS of a connection. Section V presents an outline of the target problem, distributed-control, differentiated-protection problem. Section VI proposes a novel algorithm to solve this problem. We analyze the complexity of the algorithm in Section VII. Section VIII provides illustrative examples to compare the network performance by using QoS-based protection, 1:1 protection, and unlimited shared protection schemes. Section IX provides conclusive comments and future work.

III. MAINTAINING STATE INFORMATION FOR PROTECTION

The network under study is an IP (MPLS) control-based WDM mesh network. Figure 1 shows a sample national backbone-WDM-mesh network. In this network, nodes are connected by fiber links. Although not shown in the figure, it is possible that multiple fiber links exist between two nodes. Every node in this network is implemented by an optical cross-connect (OXC). Figure 2 shows a sample OXC node architecture. An OXC consists of three main parts: a switching fabric, a controller, and a local add-drop interface. The switching fabric is used to switch an incoming wavelength from a specific fiber or a locally added wavelength (incoming port) to a specific wavelength in an outgoing fiber or a local drop interface (outgoing port). An OXC may
also include a local grooming component to switch low-bandwidth connections. The controller is responsible for controlling the switching fabric and the local add-drop interface, retrieving and maintaining the state information of the switching fabric and the local add-drop components, and communicating with controllers in other OXCs and other network elements, etc. Although Fig. 2 shows that the controller uses a specific control wavelength $\lambda_c$ in every fiber, it is not a requirement. Networks can use time-division multiplexing to use only part of the $\lambda_c$ (OC-1 or OC-3, etc.) to carry control traffic, and other part to carry data traffic. In the normal situation, a separate wavelength has more than necessary bandwidth for control. Alternatively, the control network can be an out-of-band one, which is a separate and independent network to the data transport network.

![Diagram](image)

**Fig. 1.** A sample optical mesh backbone network.

![Diagram](image)

**Fig. 2.** A sample OXC node architecture.

This study focuses on the protection-related control information. Each controller must keep track of the information on backup lightpaths that traverse its node. A lightpath is a light trail from an ingress node
(source) to an egress node (destination) in a routing domain of a WDM mesh network. A lightpath can use a single wavelength or multiple wavelengths (if wavelength converters are available) along the path. A lightpath reserved to protect a working lightpath is called a backup lightpath.

There are two major schemes for lightpath protection in a WDM mesh network, i.e., dedicated lightpath protection and shared lightpath protection.

**Dedicated lightpath protection:** In dedicated lightpath protection, every working lightpath is protected by at least one dedicated backup lightpath. Resources in backup lightpaths are pre-allocated and reserved while the primary working lightpath is established. Dedicated lightpath protection needs 100% or more additional resources since a backup-lightpath might take a longer route than the working lightpath does. Therefore, dedicated lightpath protection is not a cost-effective solution in a WDM mesh network. This scheme is typically used for some connections that require high reliability and availability.

**Shared lightpath protection:** In shared lightpath protection, the network allows a certain degree of network-resource sharing by several backup lightpaths as long as the sharing does not violate any explicit QoS requirement of all connections involved. To allow shared protection, the actual circuit for a backup lightpath is not set up in OXCs’ switching fabric. Instead, only the information of the backup lightpath is maintained in OXCs’ control components. When a working lightpath fails, its backup lightpath is activated, and the actual circuits for the backup lightpath are established in the switching fabrics of OXCs along the backup path. The cut-through method\(^1\) can be used to decrease the protection-switching time. Shared lightpath protection is a cost-effective method to provide the necessary QoS, namely availability requirement for a connection. It can greatly reduce the protection resource requirement. Additional network resources for protection can be much less than 100% of the working resources. It is also possible to differentiate between protection requirements of different connections. However, the control algorithms for shared-protection scheme are more complicated than the dedicated-protection scheme. Strictly speaking, shared lightpath-protection scheme in a WDM mesh network should not be classified as 1:N or M:N path-protection schemes since the shared backup lightpaths do not have the same end nodes.

The controller in an OXC must be able to maintain the information of protection resources. This is done by backup lightpath switching tables. The controller must also be able to distribute the protection-related wavelength-link information, and this is done by a distributed link-state routing protocol.

### A. Backup Lightpath-Switching Table (BLST)

Backup lightpath can be identified by its id (BLID) that is a triplet [source, destination, sequence number]. The sequence number is uniquely assigned by the source node. Let us denote a backup lightpath with path id \(i\) (\(i\) is a triplet structure) as \(Q_i\) and its corresponding working lightpath as \(P_i\). Following parameters are used to specify \(Q_i\):

- **Usage probability** \(U_i\): \(U_i\) is the probability that \(Q_i\) might be used. It is equivalent to the failure probability of the corresponding working lightpath \(P_i\), which we denote here as \(\beta_i\), if \(Q_i\) is the only backup lightpath for \(P_i\). This parameter is independent of the specified backup lightpath and only depends on its corresponding working lightpath \(P_i\).

- **Tolerable unavailability** \(B_i\): \(B_i\) is the maximum tolerable probability that a backup lightpath \(Q_i\) is not available for protection. This parameter is independent of the specified backup lightpath. It depends on the corresponding working lightpath \(P_i\) and the availability requirement of its corresponding connection, i.e., minimum connection-availability requirement.

- **Unavailability** \(b_i\): The parameter \(b_i\) is the sum of failure probability of all network elements along the selected backup lightpath \(Q_i\) plus the sum of the usage probability of all other backup lightpaths that share at least part of the \(Q_i\). This parameter is path-specified, and varies in different selected backup lightpath. It is independent of the working lightpath.

- **Availability balance** \(R_i\): \(R_i\) is the maximum additional usage probability that can be introduced by other new protection lightpaths to share at least part of the backup lightpath \(Q_i\). Based on previous definitions, \(R_i\) can be calculated as \(R_i = B_i - U_i - b_i\).

\(^{1}\)A cut-through method allows the actual data to be sent via the backup path shortly after the path-setup message is sent out to signal the activation of a backup lightpath.
\begin{table} 
\begin{tabular}{|l|l|l|l|l|}
\hline
BLID & In Port & Out Port & Path Parameters & Status \\
\hline
A,U,1 & I, \lambda_5 & P, \lambda_5 & (0.001, 0.01, 0.004, 0.006) & ready \\
J,K,3 & M, \lambda_6 & K, \lambda_6 & (0.0012, 0.01, 0.0042, 0.006) & ready \\
N,S,2 & M, \lambda_6 & K, \lambda_6 & (0.001, 0.02, 0.004, 0.016) & ready \\
E,V,4 & I, \lambda_6 & P, \lambda_6 & (0.0013, 0.01, 0.004, 0.0057) & ready \\
O,H,1 & P, \lambda_5 & J, \lambda_5 & (0.0012, 0.03, 0.004, 0.0258) & reserved \\
\hline
\end{tabular} 
\caption{A sample backup lightpath switching table.} 
\end{table}

Table I shows a sample BLST for OXC L in Fig. 1. There are two protection wavelengths (\lambda_5, \lambda_6), and five backup lightpaths (A-F-I-L-P-U, J-M-L-K, N-M-L-K-S, E-D-G-I-L-P-V, O-P-L-I-J-H) which pass through OXC L. Please be advised that there are multiple entries for a specified in-port or out-port. This is acceptable in shared protection scheme since the actual connections are not established in the switching fabric for backup lightpaths, only the state information is stored in the controller. The four numbers in the column “Path Parameter” are the above defined four parameters, in the same order.

B. State Information of Protection Wavelength-Links

The controller in an OXC must also maintain the state information for a wavelength-link. A wavelength-link is defined as a specified wavelength in a specified fiber in a WDM mesh network. It can be identified by three parameters: head OXC node number, the outgoing fiber number seen by the OXC, and the wavelength number (fiber is regarded as unidirectional). We can use the symbol \( l_{ijk} \) to represent a wavelength-link at OXC node \( i \) in its \( j \)th outgoing fiber with \( k \)th wavelength in the fiber. A wavelength-link reserved for protection is called a protection wavelength-link. An OXC controller can use object-oriented programming language to define a class that specifies all properties for a protection wavelength-link. Protection wavelength-link is the basic protection management element in this study. The following parameters are used to specify a protection wavelength-link \( l_{ijk} \) in an optical mesh network.

\textbf{Usage probability} \( u_{ijk} \): The parameter \( u_{ijk} \) is defined as the sum of usage probability of all backup lightpaths that use wavelength-link \( l_{ijk} \). It is calculated as:

\[ u_{ijk} = \sum_{\forall m, l_{ijk} \in Q_m} U_m. \]  

(1)

\textbf{Availability balance} \( r_{ijk} \): The parameter \( r_{ijk} \) is defined as the minimum availability balance among all backup lightpaths that use wavelength-link \( l_{ijk} \). It can be specified as:

\[ r_{ijk} = \min_{\forall m, l_{ijk} \in Q_m} R_m. \]  

(2)

\textbf{Occupied backup lightpaths}: They are all backup lightpaths that use wavelength-link \( l_{ijk} \). These backup lightpaths can be deduced from the BLST. When using a link-state routing protocol to distribute the wavelength-link information, the parameters for those backup lightpaths should also be encoded and distributed to other OXCs.

IV. QoS-based Protection in WDM Mesh Networks

Protection QoS can be evaluated by three parameters: path-protection-switching (PPS) time, connection availability, and required protection resources. Connection availability can be measured in terms of the failure probability of the working lightpath and the unavailability of the backup lightpath. PPS time is the elapsed time between the working lightpath failure and the connection reestablishment by switching the traffic to the backup lightpath. Requirements to satisfy these three parameters are related to one another. There are some trade-offs among them. If we need faster PPS time and higher availability for a connection, we need more network resources. The question is, based on the QoS requirements, can we establish a backup lightpath in a
WDM mesh network so that both protection switching time and availability requirements are satisfied while the network resource requirement can be minimum.

A. Reducing Path- Protection - Switching (PPS) Time by Using Regional Protection

This subsection studies the protection switching time. SONET/SDH networks have established the protection switching time to be less than 50 ms. In an IP-over-WDM network, we expect the protection scheme in the WDM layer should be able to realize a comparable result. Although an end-to-end lightpath protection scheme is a possible solution for a small WDM network, it may not be realizable in a national backbone network since the propagation time in such a network might be too large to realize the 50 ms time constraint. In order to decrease the protection switching time, we can break a large optical core network into several regions, and use sub-path protection inside each region to decrease the response time. Figure 3 shows this idea.

![Region protection for WDM mesh network.](image)

Figure 3 partitions the sample national WDM mesh network into three protection regions. If a fiber failure (fiber cut, multiplexer or demultiplexer failure, or fiber amplifier failure, etc.) happens inside a region, then the region can use a sub-path protection algorithm to select an alternative path from the ingress node to the egress node of the region. For example, if the fiber G-F used by lightpath P₁ (C-G-F-K-T) in Fig. 3 fails, the protection region 1 can select an alternative protection sub-path C-B-F for the sub-path C-G-F, and all other part of the original working lightpath will remain the same. By using the regional protection scheme, the network can greatly decrease the propagation time to trigger protection switching compared with the end-to-end path protection scheme. In order to protect the fiber links between two regions, the network can specify a regional management node (server node) to serve as the inter-region sub-path protection agent. For example, if a fiber from region i to region j for path P_k fails, region i must calculate the shortest paths from the ingress-node of the working path P_k to all of the border nodes of region i to region j, then the information is sent to the regional management agent M_i. Also, the egress node of path P_k in region j calculates the shortest paths from all border nodes to region i inside region j and sends the information to its regional management agent M_j. Then the management agents M_i and M_j in region i and region j, respectively, communicate with each other and decide the optimum backup lightpath from the path’s ingress node in region i to the egress node in region j.

By using regional protection, it is possible to realize the protection time to be less than 50 ms. Interested reader can refer to [33] for a similar scheme and illustrative results.
B. Reducing Protection Resources by Shared Backup Lightpaths

Connection unavailability is defined as the probability that no backup lightpath is available while the working lightpath fails. Shared protection can decrease the network resource requirement, but it will increase the connection unavailability. However, how much is the impact of backup-lightpath sharing on the connection unavailability? It has not been studied previously. The following propositions study this problem.

**Proposition 1**: Suppose a shared backup lightpath $L_k$ shares part of or the whole lightpath with $M$ ($M \geq 1$) other backup lightpaths. Let these $M$ backup lightpaths be denoted as $Q_1, Q_2, \ldots, Q_M$, respectively. Assume that the usage probability of $Q_i$ is $U_i$. If the usage of $Q_i$ is independent of the usage of $Q_j$ (for $i \neq j$, $1 \leq i, j \leq M$) and $L_k$, which implies that the failure of their corresponding working lightpaths are independent of one another, then the probability that both $L_k$ and at least one of the other shared protection lightpaths $Q_i$ are activated, which we denote here as $\alpha_k$, will be

$$\alpha_k = U_k \sum_{i=1}^{m} U_i;$$  \hspace{1cm} (3)

assuming that all nodes and links along $Q_i$ and $L_k$ function properly.

**Proof**: The probability that at least one backup lightpath among $Q_1, Q_2, \ldots, Q_M$ is activated is $\sum_{i=1}^{m} U_i$, since the activations of backup lightpaths are independent of one another. Therefore, the probability that both $L_k$ and at least one backup lightpath among $Q_1, Q_2, \ldots, Q_M$ are activated is $U_k \sum_{i=1}^{m} U_i$.

Proposition 1 shows that the introduction of a new shared protection lightpath increases the unavailable probability of the affected protection lightpaths by addition, with the value equal to the usage probability of the new backup lightpath, assuming the failure of the new working lightpath is independent of the failure of all affected backup lightpaths’ corresponding working lightpaths. This proposition also indicates that if two protection lightpaths share part of their protection resources, it doesn’t matter how much the sharing is. The impact of resource sharing of a lightpath on another lightpath’s unavailable probability is the same no matter how many resources are shared.

The following proposition specifies how to decide the failure probability $\beta_k$ for a lightpath $P_k$. $P_k$ can be a working lightpath or a backup lightpath.

**Proposition 2**: Suppose a lightpath $P_k$ consists of $N$ nodes, denoted as $V_{k1}, V_{k2}, \ldots, V_{kN}$, and the corresponding $N-1$ fiber links are $l_{k1}, l_{k2}, \ldots, l_{k(N-1)}$. Let us assume that the failure probabilities of node $V_{ki}$ and link $l_{ki}$ are $\nu_{ki}$ and $\mu_{ki}$, respectively. If the failure of any node or any link is independent of the failures of any other nodes or links, then the failing probability $\beta_k$ for the lightpath is:

$$\beta_k = P[\text{lightpath } P \text{ fails}] = 1 - \prod_{i=1}^{N} (1 - \nu_{ki}) \prod_{i=1}^{N-1} (1 - \mu_{ki}), \hspace{1cm} 0 \leq \nu_{ki}, \mu_{ki} \leq 1.$$

The above equation applies to both working lightpath and backup lightpath.

**Proof**: The proof is straightforward from probability theory.

**Proposition 3**: If link or node failures of a shared backup lightpath $Q_k$ are taken into consideration, with the same assumption as in Propositions 1 and 2, the unavailability $b_k$ of the $Q_k$ will be:

$$b_k = P[Q_k \text{ is not available for protection}] = 1 - \prod_{i=1}^{N} (1 - \nu_{ki}) \prod_{i=1}^{N-1} (1 - \mu_{ki}) + \sum_{i=1}^{M} U_i; \hspace{1cm} k \notin [1..M].$$

**Proof**: Proposition 3 is the direct result of Propositions 1 and 2.

$$b_k = P[Q_k \text{ is not available for protection}] = P[Q_k \text{ fails}] + P[Q_k \text{ is blocked}] = 1 - \prod_{i=1}^{N} (1 - \nu_{ki}) \prod_{i=1}^{N-1} (1 - \mu_{ki}) + \sum_{i=1}^{M} U_i; \hspace{1cm} k \notin [1..M].$$
Proposition 4: Suppose there are $N$ ($N \geq 1$) independent backup lightpaths (denoted as $Q_{ki}$, $i = 1, 2, ..., N$) for a working lightpath $P_k$. Let us denote the unavailability of the backup lightpath $Q_{ki}$ as $b_{ki}$ and the failure probability of the working lightpath $P_k$ as $\beta_k$. If the blocking or the failure of these paths are independent of one another, then the unavailability $\phi_k$ for this connection is

$$\phi_k = \beta_k \prod_{i=1}^{N} b_{ki}.$$  

Proof: This proposition is the direct result of probability theory.

Proposition 4 indicates that the introduction of an additional independent backup lightpath will decrease the unavailability of a connection by multiplication with a factor equal to the unavailability (should be much less than 1) of the new backup lightpath.

Propositions 1–4 provide guidelines in selecting a backup lightpath. In order to decrease the unavailability of a backup lightpath, the lightpath should follow the shortest path, and avoid sharing with too many backup lightpaths. To decrease the unavailability, multiple backup lightpaths may be used.

The above propositions assume that the failures of working lightpaths are independent of one another. However, in practice, this is not the case. It is possible that correlation of failures between different working lightpaths exist. For example, with the usage of WDM, different working lightpaths might use the same fiber with different wavelengths. If a fiber cut happens to the sharing fiber, all those working lightpaths that use the fiber fail at the same time, and their backup lightpath must be activated simultaneously. Therefore, a protection mechanism of a WDM network must take this effect into consideration when choosing backup lightpaths. The major sources of failure correlation between working lightpaths include fiber-link failure (fiber cut, fiber amplifier failure, optical multiplexer/demultiplexer failure, etc.) and OXC failure.

The following paragraphs analyze the protection correlation problem. First, we define the following keywords.

Shared-risk parameter $\xi_{ij}$ is the failure probability of the common elements of two working lightpaths $P_i$ and $P_j$. It is also called second-order shared-risk parameter.

Protection-correlation parameter $\delta_{ij}$: The impact of shared protection lightpath $Q_j$ to the unavailability of the backup lightpath $Q_i$ is defined as protection-correlation parameter $\delta_{ij}$.

We can also define higher-order, shared-risk parameters. For example, the failure probability of the common elements of $N$ working lightpaths $P_i$, $i = 1, 2, ..., N$, is the N-order shared-risk parameter $\xi_{123...N}$. Figure 5 shows an example of correlation of shared backup lightpaths. $P_1$ (1-5-6-3, $\lambda_1$) and $P_2$ (2-5-6-4, $\lambda_2$) share the fiber from node 5 to node 6 by using WDM technology. Their corresponding backup paths $Q_1$ (1-7-8-3, $\lambda_3$) and $Q_2$ (2-7-8-4, $\lambda_3$) are shared backup lightpaths, both of which use wavelength $\lambda_3$ on fiber link 7-8. If a fiber failure happens on the fiber link 5-6, both of the backup paths $Q_1$ and $Q_2$ must be activated. Then, at least one of the backup lightpaths $Q_1$ or $Q_2$ fails to provide the protection function and is blocked. How to design an algorithm to avoid such high-order correlation so that the resulting backup paths can guarantee the availability is one of the contributions of this paper.

The following propositions illustrate the impact of the shared-risk parameter on the unavailability of a backup lightpath.

Proposition 5: Suppose two backup lightpaths $Q_i$ and $Q_j$ ($i \neq j$) are shared backup lightpaths, and their corresponding working paths $P_i$ and $P_j$ have shared-risk parameter $\xi_{ij}$. Suppose no correlation between $P_i$ and $P_j$ and other working lightpaths whose backup lightpaths shared with $Q_i$ or $Q_j$ exists. Then,

$$\delta_{ij} = \frac{(\beta_i - \xi_{ij})(\beta_j - \xi_{ij}) + \xi_{ij}}{\beta_i}.$$  

Proof: Backup lightpaths $Q_i$ and $Q_j$ will be both activated with probability $(\beta_i - \xi_{ij})(\beta_j - \xi_{ij}) + \xi_{ij}$, where $\beta_i$ and $\beta_j$ are the failure probability of working paths $P_i$ and $P_j$, respectively. Therefore, protection-correlation parameter $\delta_{ij}$ can be evaluated as $\delta_{ij} = \frac{(\beta_i - \xi_{ij})(\beta_j - \xi_{ij}) + \xi_{ij}}{\beta_i}$.

If the two working lightpaths have no common part, which implies that $\xi_{ij} = 0$, the protection-correlation parameter from path $P_i$ to path $P_j$ is $\beta_j$, which is equivalent to the value used in Proposition 3 in a single
backup lightpath case. Please note that, for a single backup lightpath case, the usage probability $U_i$ of the backup lightpath $Q_i$ is equivalent to the failure probability $\beta_i$ of its corresponding working lightpath $P_i$. Based on Eqn. (5), $\delta_{ij} \neq \delta_{ji}$.

**Proposition 6:** If two backup lightpaths $Q_j$ and $Q_k$ share part of the backup lightpath $Q_i$, and their corresponding working lightpaths $P_i, P_j, P_k$ for these three backup paths are correlated with one another as shown in Fig. 5, and all of them share some common fibers ($\xi_{ijk} \neq 0$), then the combined protection-correlation parameter (3-order protection-correlation parameter) from $Q_j$ and $Q_k$ to $Q_i$, $\delta_{(j,k)}$, which is defined as the total effects to the unavailable probability by the sharing of both $Q_j$ and $Q_k$ to $Q_i$, is less than or equal to the sum of protection-correlation parameters of $Q_j$ to $Q_i$ ($\delta_{ij}$) and $Q_k$ to $Q_i$ ($\delta_{ik}$). We can express the relation by the following equation:

$$\delta_{(j,k)} \leq \delta_{ij} + \delta_{ik}.$$  

\[ \delta_{ij} + \delta_{ik} \]

Fig. 4. The correlation of two lightpaths to their corresponding shared backup lightpaths.

Fig. 5. The correlation of 3 lightpaths to their corresponding shared backup lightpaths.

**Proof:** The probability of either $Q_j$ or $Q_k$ fails while $Q_i$ fails, denoted as $\chi_{i(j,k)}$, can be evaluated as:

$$\chi_{i(j,k)} = \xi_{ij} + \xi_{ik} - \xi_{ijk} + (\beta_i - \xi_{ij} - \xi_{ik} + \xi_{ijk})(\beta_j - \xi_{ij}) + (\beta_i - \xi_{ij} - \xi_{ik} + \xi_{ijk})(\beta_k - \xi_{ik})$$

$$= \xi_{ij} + (\beta_i - \xi_{ij})(\beta_j - \xi_{ij}) + \xi_{ik} + (\beta_i - \xi_{ik})(\beta_j - \xi_{ik}) - \xi_{ijk} - (\xi_{ik} + \xi_{ijk})(\beta_j - \xi_{ij})$$
\[-(\xi_{ij} - \xi_{ijk})(\beta_k - \xi_{ik})\]
\[
\leq \xi_{ij} + (\beta_i - \xi_{ij})(\beta_j - \xi_{ij})
+ \xi_{ik} + (\beta_i - \xi_{ik})(\beta_j - \xi_{ik})
= \delta_{ij}\beta_i + \delta_{ik}\beta_i
= (\delta_{ij} + \delta_{ik})\beta_i.\]

By definition, the 3-order protection-correlation parameter \( \delta_{i(j,k)} = \chi_{i(j,k)}/\beta_i \). Therefore, \( \delta_{i(j,k)} \leq \delta_{ij} + \delta_{ik} \).

We can also easily prove that, if the correlations of more than three working lightpaths exist, and the backup lightpaths for these working lightpaths are shared backup lightpaths, the impact on the blocking probability of one of these backup lightpaths by the sharing of other backup lightpaths will be less than the sum of the 2-order protection-correlation parameter of those backup lightpath.

Figure 5 show one example for Proposition 6. In Fig. 5, there are three working lightpaths \( P1 \ (1 - 7 - 8 - 9 - 4, \lambda_1) \), \( P2 \ (2 - 7 - 8 - 9 - 10 - 5, \lambda_2) \), and \( P3 \ (3 - 8 - 9 - 10 - 6, \lambda_3) \), which share fiber link 8–9 at the same time by using WDM technology. The corresponding backup lightpaths \( Q1 \ (1 - 11 - 16 - 17 - 6, \lambda_4) \), \( Q1 \ (2 - 15 - 16 - 17 - 14 - 5, \lambda_4) \), and \( Q1 \ (3 - 15 - 16 - 17 - 6, \lambda_4) \) are shared backup lightpaths all using \( \lambda_4 \).

The conclusion of Proposition 6 will be used to simplify our design of the shared backup lightpath decision algorithm.

V. Problem Definition

The problem in this study deals with WDM mesh networks, in which every node is an optical cross-connect and is capable of wavelength switching. Also, every optical cross-connect is equipped with a control component that implements all necessary MPLS router’s control functions, such as constrained-based routing protocols, conventional intra-domain routing protocols (such as open-shortest-path-first (OSPF), intermediate system to intermediate system intra-domain routing exchange protocol (IS-IS), etc.), inter-domain routing protocol such as border-gateway protocol (BGP) if the optical cross-connect is a border network node in a routing domain, and constraint-based label-distribution protocol (CR-LDP) or resource ReSerVation Protocol (RSVP-TE). Before we explore further, let us define several additional keywords.

**Definition 1:** *Strict path-complement graph:* A strict path-complement graph is the residue of a graph after deleting all intermediate nodes of the path and all links connecting to those nodes. Figure 6 shows a strict path-complement graph of path C-G-I-L-P-U from the graph in Fig. 1. A strict path-complement graph is not necessarily a connected graph. It is also called a *path-node-complement graph.*

![Fig. 6. Strict path-complement graph for path C-G-I-L-P-U in Fig. 1.](image)

**Definition 2:** *Loose path-complement graph:* A loose path-complement graph is the residue of a graph
after deleting all links along the path. Figure 7 shows a loose path-complement graph of path C-G-I-L-P-U from the graph in Fig. 1. A loose path-complement graph is also called a **path-link-complement graph**. Unless a link along the path is the only link that connects two parts of the graph, a loose path-complement graph is a connected graph.

![Diagram of a network](image)

**Fig. 7.** Loose path-complement graph for path C-G-I-L-P-U in Fig. 1.

**Definition 3:** _Strictly disjointed paths:_ Two paths are strictly disjointed if they have the same source and destination nodes but share no other common nodes or links. They are also called _node-disjointed paths._

**Definition 4:** _Loosely disjointed paths:_ Two paths are loosely disjointed if they have the same source and destination nodes but share no other common links. They are also called _link-disjointed paths._

In our example network, we assume fiber $i$ has $W_i$ wavelengths for data channels in addition to the control channel $\lambda_c$. In such a network, the network manager can assign some wavelengths for working lightpaths and other wavelengths for protection, or the manager can let the routing and wavelength assignment (RWA) algorithm select the wavelength for working or backup path automatically. Let us assume here that, among the $W_i$ different wavelengths for data traffic in the fiber link $i$, $K_i$ wavelengths are for working traffic and the remaining $W_i - K_i$ ($K_i \geq W_i - K_i$) wavelengths are for protection.

We assume that the studied network has a good RWA algorithm [2], [17], [18] to calculate the optimum working lightpath $P_{\text{new}}$ for a new connection. This algorithm should use some constraint-based routing algorithm and be good at dynamic provisioning. The problem we want to solve here is that, for a given network topology and current state of the network as well as the new working lightpath $P_{\text{new}}$, how to choose and set up a backup lightpath $Q_{\text{new}}$ for $P_{\text{new}}$ such that the backup lightpath $Q_{\text{new}}$, together with the working path $P_{\text{new}}$, can satisfy the QoS requirements of a new connection while minimizing the required network resources. The QoS requirements include, but are not restricted to, the unavailable probability of the backup lightpath or the connection, the delay constraints, etc.

The algorithm should be able to differentiate different connections’ (lightpaths’) QoS requirements. We regard such problems as lightpath shared protection (LPSP) problems. Since the conventional RWA problems with static traffic requirement is an NP-hard problem [2], [17], the LPSP problem should be similar in complexity for static traffic because the LPSP problem introduces the path sharing, unavailability, and delay

---

2Unlike voice communication, where all connections require the same quality of service (QoS), data communication has different types of QoS requirements depending on applications. For example, the real-time voice data such as voice over IP (VoIP) application has a very strict delay constraint, requiring the end-to-end delay to be less than about 100 ms; however, it can tolerate a certain amount of data loss. While some data applications such as file transfer protocol (ftp) are not very sensitive to delay, they are strict to the data packet loss. Some other applications such as real-time video require strict delay constraint, small delay jitter as well as very small packet loss. The backup lightpath calculation algorithm should be able to take these requirements into consideration and select an appropriate backup lightpath for a connection.
constraints in addition to the conventional RWA problem. The globally optimized solution for a LPSP problem with static traffic requirement is expected to be difficult to obtain. However, our study stresses on dynamic provisioning and protection in which a WDM mesh network can set up and take down a lightpath and its corresponding backup lightpath in real-time. The solution must be simple, efficient, and easy to implement.

VI. DSLPM: DISTRIBUTED SHARED-LIGHTPATH-MANAGEMENT ALGORITHM

This section describes the procedures to set up, take down, maintain, and activate a QoS-based backup lightpath.

A. Setting Up a Backup Lightpath

In order to setup a backup lightpath, a network must perform three basic procedures: wavelength and backup lightpath selection, backup lightpath confirmation, and connection setup and network state update. This is very similar to the working lightpath setup in a distributed control optical network [15], [32]. For a network without wavelength conversion, a single wavelength is used along a lightpath. If wavelength conversion is possible, then multiple wavelengths can be used.

- **Wavelength and backup lightpath selection:** This should be done by the source OXC’s control component that initiates the backup lightpath setup. A source OXC node must have a mechanism to select the wavelength and route for the backup lightpath. In this study, we assume that the network has some algorithms or mechanisms to choose and set up the new working lightpath, and the source has detailed knowledge on the new working lightpath for the connection, including but not limited to the wavelength used, the route and the corresponding QoS parameters, as well as other correlated lightpaths.

- **Backup-lightpath confirmation:** It is necessary for a backup lightpath decided by the source node to be confirmed by all components (including nodes or links) along the path that the protection resources are available because of distributed control. In case the confirmation fails, the resource reserved for the new backup lightpath must be released and network state should not be modified by the previous backup-lightpath-setup effort.

- **Connection setup and network state update:** After the backup lightpath is confirmed, it is necessary to set up the backup lightpath and then update the information for the network to reflect the new status.

Based on our previous analysis, we propose the following distributed algorithm to solve the protection lightpath setup problem. We denote the new backup lightpath for a new working lightpath $P_m$ as $Q_m$ in the following description. To setup a backup lightpath, the algorithm performs the following steps:

- **Backup-lightpath calculation:** Assume that, when the new working lightpath $P_m$ is set up, all related information on $P_m$ such as its correlation to other working lightpaths is collected and sent to affected OXCs. After the source receives the information, it uses the following steps to decide the backup lightpath $Q_m$.
  - **Step 1:** Construct the lightpath $P_m$’s path-complement graph. It can be strict or loose path-complement graph depending on the specific application requirement. We assume here that strict path-complement graph is used. Select the first protection wavelength as the current protection wavelength.
  - **Step 2:** Select the current protection wavelength $\lambda_k$.
  - **Step 3:** Identify those wavelength-links used by those backup lightpaths whose corresponding working lightpaths are related to the new working lightpath $P_m$. For every affected backup lightpath $Q_i$ using the current wavelength, subtract their availability balance $R_i$ by the protection-correlation parameter $\delta_{im}$. That is, $R_i = R_i - \delta_{im}$.
  - **Step 4:** Use Eqn. (2) to decide the availability balance $r_{ijk}$ for every wavelength-link $l_{ijk}$ in the path-complement graph of the current protection wavelength $\lambda_k$.
  - **Step 5:** Use constraint-based shortest-path (CSP) algorithm to decide the optimum protection lightpath for the current protection wavelength $\lambda_k$. The actual criteria or constraint to select the optimum path is beyond the scope of this study. It can be minimum cost path, minimum distance path, or minimum

$^a$Because of the usage of WDM technology, every fiber link has multiple wavelengths that may be used by different connections and different fibers can pass the same trench.
hop-distance path. However, it is necessary to apply the following two constraints for the new backup lightpath calculation:

\[ U_m \leq r_{ijk}, \forall l_{ijk} \in Q_m; \]   
\[ b_m \leq B_m. \]  

These constraints are used to guarantee the availability requirement for every protection lightpath. The condition in Eqn. (7) is necessary to guarantee that the introduction of the new backup lightpath should not violate other existing backup lightpaths' availability requirement. The condition in Eqn. (8) satisfies the new backup lightpath's availability requirement. Note that it is possible that no backup lightpath that can satisfy all constraints exists. If this is the case, a NULL path will be stored. There are a lot of constrained-based shortest-path routing algorithms [26], [35]; the actual choice of the algorithm is beyond the scope of this study.

- \textbf{Step 6:} Repeat Step 2 to Step 5 until all optimum backup lightpaths for all protection wavelengths are decided.

- \textbf{Step 7:} Select the optimum backup lightpath from all backup lightpaths obtained by previous steps. This is the selected backup lightpath \( Q_m \) for the working path \( P_m \).

This algorithm assumes that no wavelength conversion is available in the network. If wavelength conversions are available between protection wavelengths, we can easily modify the above algorithm to accommodate the wavelength conversion function. The key idea is to allow multiple wavelength-links between nodes, and connections between convertible wavelengths inside an OXC are maintained and considered when selecting a CSP.

- \textbf{Backup-lightpath confirmation and resource reservation:} After a new backup lightpath is decided, a source must notify the network on the new backup lightpath so that the network can confirm that the network resource is actually available, and the introduction of the new backup lightpath does not violate the QoS requirements for all current existing backup lightpaths. To realize these tasks, the source node first uses a broadcast mechanism to broadcast the new backup lightpath information by using \textit{NEW - P - PATH - REQUEST} message. This can be done by an extension to the current link-state routing protocol. The \textit{NEW - P - PATH - REQUEST} message should include all information for the new backup lightpath, especially the backup sharing information. After sending out the \textit{NEW - P - PATH - REQUEST} message, the source node will wait for a response from the other nodes on the new backup lightpath for a period of time. If no negative message \textit{NEW - P - PATH - FAIL} is received before the timeout of the waiting period, then the source will start to setup the new backup lightpath. The timeout timer can be set to 2-3 times the maximum round-trip time (RTT). Upon receiving a \textit{NEW - P - PATH - REQUEST} message, a controller first decides whether its OXC is on the backup lightpath and acts accordingly.

- If the OXC is not on the new backup lightpath, then the controller must identify the backup lightpaths in the protection-switching table that shares part of the new backup lightpath (this information is carried by the \textit{NEW - P - PATH - REQUEST} message), and decides whether the introduction of the backup lightpath violates the availability requirement of those affected lightpaths. Suppose \( Q_i \) is one of the affected backup lightpaths and \( Q_m \) is the new protection lightpath; then to admit the \( Q_m \) the following relation must be satisfied:

\[ R_i - \psi_i \geq \delta_m \]  

where the variable \( \psi_i \) is the sum of the unavailability of other new backup lightpaths that must share part of the backup lightpath \( Q_i \), and these backup lightpaths have sent the \textit{NEW - P - PATH - REQUEST} message to this OXC, but the setup efforts have not yet finished. If no other setup effort is going on, \( \psi_i = 0 \). If Eqn. (9) holds for every affected backup lightpath, then the algorithm updates \( \psi_i \) as \( \psi_i = \psi_i + \delta_m \) for every affected backup lightpath \( Q_i \). If any of the affected lightpath’s parameter cannot satisfy Eqn. (9), a \textit{NEW - P - PATH - FAIL} notification message is sent back to the source, and no update is carried out.

- If the OXC is on the new backup lightpath, then the controller must first identified the wavelength-link used by the new backup lightpath \( Q_m \), decide whether the requirement for the \( Q_m \) can be satisfied, and if not, a \textit{NEW - P - PATH - FAIL} message will return to the source OXC. Otherwise, add a
temporary entry for $Q_m$ in the protection-switching table, and mark the entry as reserved. Then, the controller carries out the same procedure as the controller of the OXC that is not on the new path. If the source receives at least one $NEW - P - PATH - FAIL$ message, the new backup lightpath violates some QoS requirement or the actual resources are not available. A $NEW - P - PATH - REVOKE$ message must be sent out to reverse any information previously modified by $Q_m$. Then the source uses a random exponential back-off algorithm [19] to wait for some random time so that the source can receive up-to-date information on the network. After the waiting period, the source resumes to setup the backup lightpath starting from the beginning.

If no $NEW - P - PATH - FAIL$ message is received by the source OXC after a timeout period, the source starts to set up the actual protection state for the backup lightpath $Q_m$. This can be done by using the extension of the signaling protocol CR-LDP [28], [29] or RSVP [30] to confirm the selected protection path. The CR-LDP or RSVP’s $PATH$ message is used to re-confirm the new backup lightpath, and the $RESV$ message from the destination to source will trigger the actual setup of the backup lightpath (to put the entries in the protection-switching table for the new backup lightpath into ready state). The destination is also responsible to broadcast a $NEW - PATH - CONFIRMED$ message to the network. During this step, if any confirmation fails or the source receives $NEW - P - PATH - FAIL$ message, the setup effort will stop and it will resume after some random delay.

When an OXC receives the $NEW - PATH - CONFIRMED$ message, it will update the affected entries of its backup lightpath-switching table.

When the source receives the $RESV$ message, the backup lightpath is set up successfully.

- **Backup-lightpath setup and network state update:** After the signaling message reaches the destination successfully, reservation for all wavelength-links are done, and resources for the backup lightpath are confirmed; hence, the new backup lightpath is confirmed. The destination then broadcasts a $NEW - PATH - CONFIRMED$ message to all nodes inside the network. Upon receiving $NEW - PATH - CONFIRMED$ message, an OXC not on the new lightpath will first check whether any of its protection-switching entry is a affected entry by the new lightpath $Q_m$. If any entry, say entry $Q_i$, is affected by $Q_m$, then the path parameters $R_i$ and $\psi_i$ for entry $Q_i$ must be updated by $R_i = R_i - \delta_{im}$ and $\psi_i = \psi_i - \delta_{im}$, respectively. After updating the parameters of all affected entries, the new wavelength-link parameters are calculated and the new values are broadcast to other OXCs inside the network via a link-state routing protocol.

An OXC that is on the new backup lightpath must do some additional work. Upon receiving the $NEW - PATH - CONFIRMED$ message, an OXC along the new backup lightpath first changes the entry for the new protection lightpath inside the protection-switching table from reserved to ready state. Then all backup lightpaths ($Q_i, i = 1, 2, \ldots$) that use the same wavelength-link, suppose it is $l_{ijk}$, in the OXC update their backup lightpath parameters as:

\begin{align}
b_i = b_i + \delta_{im}, \quad &\forall m, \ l_{ijk} \in Q_m; \\
R_i = R_i - \delta_{im} \quad &\forall m, \ l_{ijk} \in Q_m.
\end{align}

Then, the new wavelength-link parameter for $l_{ijk}$ is calculated according to Eqn. (1) and (2). And the updated values for the wavelength-link are broadcast to the other nodes inside the network via the link-state routing protocol.

When the $RESV$ message reaches the source that originates the backup lightpath, the backup lightpath is successfully set up and the path information is added to the source node.

After the update for a new backup lightpath is done, the source OXC will broadcast its new state information via the extended link-state routing protocol.

**B. Taking Down a Backup Lightpath**

There are two situations when a backup lightpath must be taken down: a connection is closed or part of the backup lightpath’s resource is no longer available. The first situation is generally initiated by the source node and is the topic of this subsection. The second situation is part of the restoration process and will be discussed in the next subsection.
To take down a previously-set-up backup lightpath, the network needs to release any previously-reserved resources and delete all entries reserved in OXCs along the to-be-taken-down backup lightpath. To take down a previously-set-up backup lightpath $Q_d$, the source node sends out a PATH–RELEASE message to all OXCs along the backup lightpath $Q_d$. PATH–RELEASE message should include the critical information for $Q_d$ including but not limited to the path-id, path performance parameters, etc. PATH–RELEASE message can be carried by CR-LDP or RSVP protocol's PATH message. Upon receiving PATH–RELEASE message, an OXC $i$ on $Q_d$ first identifies those backup lightpaths that share the same wavelength-link (suppose it is $l_{ijk}$) and save their path-ids into the PATH–RELEASE message, which will be sent to the down-stream OXC. Then, the entry for $Q_d$ inside OXC $i$’s protection table is deleted. All information on the entries in the backup-lightpath-switching table that are affected by the deleted backup lightpath is updated.

When the PATH–RELEASE message reaches the destination node, the destination OXC’s control component broadcasts the PATH–RELEASE–DONE message. The PATH–RELEASE–DONE message includes information on the deleted protection lightpath and also the affected path-ids collected and carried by the PATH–RELEASE message. Upon receiving the PATH–RELEASE–DONE message, the OXCs must compare the path-ids with the path-ids in the entries of their protection-switching table. The matching entries’ backup-lightpath parameters (availability, etc.) must subtract the protection distance from the deleted path to itself and the same amount is added to availability balance $R_i$. After updating all entries, the OXCs re-calculate all wavelength-link parameters and then broadcast the new values via a link-state routing protocol. If no match between the path-ids of the entries in the protection-switching table and the path-ids in the PATH–RELEASE–DONE message exists, then an OXC does not need to do anything. When the PATH–RELEASE–DONE message reaches the deleted backup lightpath’s source node, the source knows that the backup lightpath is deleted successfully.

C. Backup-Lightpath Activation

As we know, the actual hardware connection for a backup lightpath is not actually setup. That is why multiple backup lightpaths can share the same wavelength-link. However, when a protection lightpath is actually put into use, which is triggered by the failure of the corresponding working path, the actual hardware connection must be set up in OXCs along the backup lightpath. After the backup lightpath is put into use, all other backup lightpaths that share resources with it are no longer useful and new backup lightpaths must be set up to replace the original ones. The basic procedure to put a backup lightpath into use consists of two steps: backup lightpath activation and restoration of sharing lightpaths. In the backup-lightpath activation step, the source OXC sends out a PATH–ACTIVATION message along the to-be-used backup lightpath. An OXC on the backup lightpath then sets up the actual hardware connection upon receiving the message. A PATH–PREEMPT message to preempt all backup lightpaths that share the to-be-used backup lightpath on that node is then broadcast to all OXCs inside the network to trigger the restoration of those preempted backup lightpaths. When the PATH–ACTIVATION message reaches the egress OXC, the backup lightpath is activated successfully. In order to speed up the response time, the network can use the cut-through\(^4\) method to put the backup lightpath in use earlier.

D. Backup Lightpath Restoration

Network component failure: In case of control component failure, the network should allow previous set up working paths to continue functioning. However, because of the introduction of shared protection, it might be necessary to trigger the backup lightpath restoration procedure because the actual usage of the backup lightpath may need further coordination of the control component. In our proposed scheme, no matter which component fails, the failure will trigger the restoration of the backup lightpaths that the failure component is in.

Protection resource preemption: The actual usage of a backup lightpath will invalidate all other backup lightpaths that share part of it. Therefore, in addition to the restoration of the working lightpath, it is also

\(^4\)A cut-through method allows the backup lightpath to be used shortly after the source sends out PATH–ACTIVATION message without waiting for the confirmation of path activation.
necessary for the network restoration procedure to restore those protections lightpath that are invalidated by the actual usage of the backup path.

The procedures to restore a backup lightpath for both situations are almost the same. After the source node for a backup lightpath notices the failure of the original backup lightpath, it will first release all previously reserved resource for the original backup lightpath by using the takedown procedure, and then use the new protection-lightpath-setup procedure to set up a new backup lightpath.

Finally, we want to point out that the network generally should have a re-routing mechanism to select another working lightpath for a failed working lightpath after the backup lightpath is activated. After the alternate working lightpath is set up, the traffic should be switched to the new working lightpath. And the activated backup lightpath should be reversed to protection ready state.

VII. Algorithm Analysis

The DSLPM algorithm is a fully-distributed backup-lightpath management algorithm. This algorithm guarantees to satisfy the protection QoS requirement while setting up a new backup lightpath QoS requirement. Furthermore, it also guarantees that the new backup lightpath would not violate all previously-setup backup lightpaths. The most complex procedure of our proposed algorithm is the one to set up a new backup lightpath. We analyze this procedure in terms of the computational complexity, time complexity, and message complexity.

- **Computational complexity** can be measured by the algorithm’s complexity of selecting the optimum backup lightpath decided by the source OXC. The complexity of a constrained-based routing algorithm is \( O(n^2) \) by using Dijkstra algorithm, where \( n \) is number of OXCs in a routing domain. Suppose there are \( W \) protection wavelengths, then the algorithm complexity to select a new backup lightpath will be \( O(Wn^2) \). Although other OXCs need to perform some computational tasks while setting up a backup lightpath, the complexity of those computations are on an order of \( O(1) \) and will not increase the order of the computational complexity of the algorithm. We omit the detailed analysis here.

- **Time complexity** is the time it takes to set up a protection lightpath successfully. If a backup lightpath is set up successfully without any retry, then the time it takes will be the sum of the processing time of the source node, the timeout period (2 times maximum round-trip-time RTT), the time to set up the new path by using the signaling protocol, and the last setup network state update (will be 2 RTT plus the processing time along the new backup lightpath). We expect the processing time should be small. Therefore, the time complexity to setup a protection lightpath should be in the order of several RTTs to tens of RTT. For a network with diameter 2000 km, the RTT is about 20 ms. So we can expect a successful setup will be completed on an order of 100s of ms to several seconds, depending on the processing speed of OXCs.

- **Message complexity** can be measured by the total number of broadcast message needed to set up a backup lightpath. Based on the description of our algorithm, the total number of broadcasts will be \( O(n) \) since every affected node may send out an updated information after the new backup lightpath is set up. The maximum number of affected OXCs is all OXCs in the link-state routing domain.

VIII. Illustrative Examples

We will study the performance of the QoS-based shared-protection scheme by comparing its performance with two other schemes: 1:1 protection and unlimited shared protection. In 1:1 protection scheme, an end-to-end connection contains a working lightpath and a dedicated backup lightpath. The resources for a backup lightpath are reserved exclusively for the connection.\(^5\) For unlimited shared protection scheme, a backup lightpath can share resources with another backup lightpath as long as their working lightpaths do not share any fiber. There is not limitation on how many other backup lightpaths to share with a backup lightpath as long as the above-mentioned condition holds. For QoS-based shared protection, a backup lightpath can share with other backup lightpaths only if the sharing will not violate all of the explicit availability requirements, in addition to the same conditions for the unlimited shared protection. We use Fig. 1 as the network for our study. This simulation makes the following assumptions:

\(^5\) Actually, the backup path can carry some preemtible traffic.
• There are 16 wavelengths on each fiber.
• The fiber cut probability is $5 \times 10^7$ /mile/time-unit.
• The OXC failure probability is $1 \times 10^7$ /time-unit.
• A connection request is blocked if it cannot setup its working lightpath or its backup path successfully. If a working lightpath request is blocked, its backup-lightpath-setup request will not be carried out.
• Connections are generated between any two randomly selected nodes in the network. We assume that there are four classes of connections in term of the availability requirement, which are 99%, 99.9%, 99.99%, and 99.999%. A connection takes one of these four classes randomly as its service class.

We have studied two type of networks: non wavelength-conversion network and full wavelength-conversion network.

A. Non Wavelength-Conversion Networks

We first study the three schemes in the network that has no wavelength conversion. Figure 8 shows the connection blocking probability. It shows that, when the network’s offered load\(^6\) is low, the connection blocking probabilities of all the three schemes are 0. When the network’s offered load increases, the blocking probability of the 1:1 scheme increases much faster than the shared protection schemes. The blocking probability for the QoS-based sharing scheme is only a litter higher than the unlimited sharing scheme. However, the difference is negligible.

Figure 8 only takes the network’s offered load into consideration. As we know, the connection blocking probability actually also depends on the network state. The network state can be represented by the average wavelength-link utilization $\mathcal{U}$ defined by Eqn. (12):

$$
\mathcal{U} = \frac{1}{T} \sum_{i=1}^{K} \sum_{j=1}^{W_i} \frac{\tau_{ij}}{T}
$$

where $\tau_{ij}$ is the total busy time during the simulation period that lasts $T$. $K$ is the total number of fiber links in the network, and $W_i$ is the total number of wavelengths in fiber link $i$. Figure 9 shows the network offered load vs. connection blocking probability/average wavelength-link utilization. It shows that the performance of the 1:1 protection scheme is in fact worse than that shown in Fig. 8 when we take the actual network load into consideration.

Figures 10 and 11 show the blocking probability of working lightpaths and backup lightpaths, respectively. Figure 10 shows that, for a given network offered load, the shared protection scheme have higher blocking probability for working paths. This is because, for any given network offered load, the shared protection schemes have more connections in the network than the 1:1 scheme does. The QoS-based sharing scheme has somewhat lower blocking probability than the unlimited sharing scheme for the same reason. However, for backup lightpath, the blocking probability of 1:1 scheme is much higher than the sharing schemes even though it has fewer connections in the network for the same offered load, because the backup lightpath of the 1:1 scheme needs dedicated resources. The QoS-based sharing scheme’s blocking probability is a little higher because the QoS scheme must take the connection availability requirement into consideration. Hence, it needs a little more resources and rejects a few more connections. Figures 10 and 11 also indicate that the blocking probability for backup lightpath in 1:1 scheme is higher than the working lightpath. This is because, the backup path calculation must eliminate those fibers used by its working path so that the backup and its working path can be link-disjoint. However, with shared protection schemes, the backup lightpath blocking probability is much lower than the working lightpath.

We can also compare the average number of connections in the network for the three schemes. Figure 12 shows that, based on the knee points, the total number of connections the network can accommodate in the shared protection schemes can be 50%-80% higher than the 1:1 scheme because the shared protection schemes can decrease the protection resources greatly. QoS-based protection scheme realizes similar performance as the unlimited sharing scheme. Figure 13 shows the average wavelength-link utilization of the network. For a given network, all three schemes’ average link utilizations are similar when the offered load is low or high.

\(^6\)The network offered load is defined as the average holding time of each connection multiply by the average request rate.
However, for intermediate offered load, the shared protection scheme has lower average link utilization while with more number of connections on average in the network. This is because the shared protection scheme greatly reduces the resource requirement for protection. QoS-based sharing scheme performs similar to the unlimited scheme.

Figure 14 shows the average hop distance (AHD) for different types of lightpaths. It shows that the AHD for working lightpaths is similar for all three schemes when the network offered load is low. The AHDs for the shared protection schemes are a little lower than the 1:1 scheme because their actual network load is lower as the result of backup sharing. When the network offered load increases, the AHDs for all three schemes increase initially. This is because, when the network offered load increases, the actual network load increases too. A new lightpath-setup request must take a longer path because the resources along the shortest path may already be occupied by previous setup connections. However, when the network offered load increases further, the AHDs of the working paths for all three schemes decrease because there are more and more lightpaths that will be blocked. A path with higher AHD will be blocked with a higher probability than a shorter path. With more and more paths with smaller AHD accepted and more and more paths with greater AHD rejected, the average AHD for the working path decreases. The AHDs of the working lightpaths for the shared protection schemes decrease faster than the 1:1 scheme because, for the shared protection schemes, their actual network load is much higher than the 1:1 scheme.

AHDs for the backup lightpaths have similar trend. However, they are higher than those of the working paths at the same offered load because the network requires a backup lightpath to take a link-disjoint path with its working path. The AHD of backup lightpaths for the 1:1 scheme has similar trends as its working lightpaths for the same reason mentioned above. However, the AHDs for the backup lightpaths first is flat and then decrease gradually. This is because, for the shared protection scheme, when the network load is not very high, most of the backup paths can be set up successfully since a new backup lightpath can share resources with others. Furthermore, a new backup lightpath can take the shortest path in most cases. However, when the network load increases, the AHDs decrease for the reasons explained previously. The QoS-based shared protection scheme's performance is similar to that of the unlimited shared protection scheme.
Fig. 9. Connection blocking probability/average wavelength-link utilization.

B. Full Wavelength-Conversion Networks

We also study the performance for the three backup schemes in the full wavelength-conversion network. Figures 15, 16, 17, 18, 19, and 20 show the results. From these figures, we find that the overall trends of each figure for the full wavelength-conversion is exactly the same as the non wavelength-conversion network.

C. Comparison of Full and Non wavelength-Conversion Networks

As we already know, full wavelength-conversion network outperforms non wavelength-conversion network. This section compares the QoS-based shared protection scheme in full and non wavelength-conversion network. Figure 21 shows the overall blocking probability of these two networks. It shows that, when the network operates at light or heavy load, both schemes have similar blocking probability. However, when the network is at the intermediate load, full wavelength-conversion network has much smaller blocking probability than the non wavelength-conversion network does.

Please note that Fig. 21 does not take the actual network load into consideration. Figure 22 takes this actual network load into consideration. The Y-axis is the ratio of the blocking probability to the average wavelength-link load. It shows that the actual blocking probability for a given network at the same average wavelength-link load in a non wavelength-conversion network is actually much higher than the full wavelength conversion network.

In conclusion, based on our observed results, shared protection schemes perform better than the 1:1 scheme in terms of connection blocking probability, actual network load, and total number of connections a network can accommodate. Although QoS-based shared protection scheme takes an additional constraint, namely, connection availability into consideration when setting up the backup lightpath, its performance is similar to the unlimited shared protection scheme in both non wavelength-conversion and full wavelength-conversion networks. We have also shown that, when the network operates at intermediate load, full wavelength-conversion network's connection-blocking probability is much smaller than the non wavelength-conversion network.

IX. CONCLUSION

We have presented an MPLS-control-based, fully-distributed algorithm to solve the protection problem in optical mesh networks. Our proposed algorithm includes intelligent and automatic procedures to set up, take
down, activate, restore, and manage backup lightpaths. The algorithm can greatly decrease the required protection resources by allowing resource sharing by multiple lightpaths. The proposed algorithm also takes the correlation of working lightpaths into consideration when choosing a backup lightpath and guarantees that the resource sharing by backup lightpaths and the correlation of the working lightpaths would not violate the availability of all previously-setup backup lightpaths when a new backup lightpath is introduced. Backup lightpaths set up by the algorithm can always satisfy their explicit availability requirements even though resource sharing is introduced. The complexities of the proposed algorithm are analyzed in terms of computation complexity, time complexity, and message complexity. They indicate that the implementation of the algorithm is practical. Our numerical studies show that the QoS-based scheme performs as well as the unlimited shared protection scheme in both non wavelength-conversion and full-wavelength conversion network, which is much better than the dedicated backup scheme. For future work, we would like to explore networks with partial wavelength conversion and study the performance of QoS-based shared backup scheme in such networks.

**Fig. 10.** Working path blocking probability.

**REFERENCES**


Fig. 11. Backup path blocking probability.

Fig. 12. Average number of connections.


Fig. 13. Average wavelength-link utilization for non-wavelength-conversion network.

Fig. 14. Average hop-distance for non-wavelength-conversion network.
Fig. 15. Connection blocking probability for full-wavelength-conversion network.

Fig. 16. Connection blocking probability/average wavelength-link utilization in full-wavelength-conversion network.
Fig. 17. Working path blocking probability for full-wavelength-conversion network.

Fig. 18. Backup path blocking probability for full-wavelength-conversion network.
Fig. 19. Average number of connections for full-wavelength-conversion network.

Fig. 20. Average wavelength-link utilization for full-wavelength-conversion network.
Fig. 21. Comparison of full and non wavelength-conversion networks—Connection blocking probability.

Fig. 22. Comparison of full and non wavelength-conversion networks—Connection blocking probability/average wavelength-link utilization.