Quality of Service Based Protection in MPLS Control WDM Mesh Networks

Wushao Wen1, Biswanath Mukherjee2, and S. J. Ben Yoo1
1Dept. of Elect. & Comp. Engineering, University of California, Davis, CA 95616, U.S.A.
2Dept. 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 terms 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 its impact to the sharing of their 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 fully 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 when deciding backup lightpaths. 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 networks, MPLS networks, WDM networks, IP over WDM architecture, quality of service, distributed network control, mesh networks.

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.

However, the four-layer architecture has several serious limitations. First, it needs too much additional resources for protection, and it is not optimized for data networks. Second, it is difficult to provision. 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 [7]. This kind of race protection has been demonstrated in [8] experimentally. Lastly, the ATM layer is unnecessary with the enhanced functions of IP or multi-protocol-label-switching (MPLS) layer.

Now, the networking industry is moving to the IP (MPLS) over WDM network architecture [9], [14], [31], [33]. 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. Protection in IP-over-WDM network has begin to attract more interest in industry and academia [4], [5], [6], [10], [11], [12], [14], [18], [19], [20], [21]. 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.

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

This work was supported, in part, by the UC-Micro program, Cisco systems, and BellSouth.

*Contact author.
II. 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. 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.

![Fig. 1. A sample optical mesh backbone network.](image1)

![Fig. 2. A sample OXC node architecture.](image2)

This study focuses on the protection-related control information. Each controller must keep track of the information on backup lightpaths that traverses 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 reserved for protection of 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.

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 BLID is 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 \( P_i \).

- **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 and only depends on its corresponding working lightpath \( P_i \).

- **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-specific, and varies in different selected backup lightpath. It is independent of the working lightpath.

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

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 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
TABLE 1
A sample backup lightpath switching table.

<table>
<thead>
<tr>
<th>BLID</th>
<th>In Port</th>
<th>Out Port</th>
<th>Path Parameters</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A,U,1</td>
<td>1,λ_5</td>
<td>P_5,λ_5</td>
<td>(0.001,0.01,0.004,0.006)</td>
<td>ready</td>
</tr>
<tr>
<td>J,K,3</td>
<td>M_1,λ_6</td>
<td>K_1,λ_6</td>
<td>(0.0012,0.01,0.0042,0.006)</td>
<td>ready</td>
</tr>
<tr>
<td>N,S,2</td>
<td>M_1,λ_6</td>
<td>K_1,λ_6</td>
<td>(0.001,0.02,0.004,0.016)</td>
<td>ready</td>
</tr>
<tr>
<td>E,V,4</td>
<td>I_1,λ_6</td>
<td>P_5,λ_6</td>
<td>(0.0013,0.01,0.004,0.0057)</td>
<td>ready</td>
</tr>
<tr>
<td>O,H,1</td>
<td>P_1,λ_5</td>
<td>J_1,λ_5</td>
<td>(0.0012,0.03,0.004,0.0258)</td>
<td>reserved</td>
</tr>
</tbody>
</table>

OXC node \(i\) in its outgoing \(j\)th fiber with \(k\)th wavelength in the fiber. A wavelength-link reserved for protection is called a protection wavelength-link. The following parameters are used to specify a protection wavelength-link \(l_{ijk}\) in an optical mesh network.

**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:

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

**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:

\[
r_{ijk} = \forall m, l_{ijk} \in Q_m \:
\]

**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 OXC.

### III. 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 evaluated in terms of the failure probability of the working lightpath and the unavailability of the backup lightpath. Requirements to satisfy these three parameters are related to one another. 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 blocking probability requirements are satisfied while the network resource requirement can be minimum?

A. Shared Backup Lightpath

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 invisibility of connections? It has not been studied previously. The following several 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 \(Q_1, Q_2, ..., Q_M\), respectively. Assume that the usage probability of \(Q_i\) is \(U_i\). If the usage of \(Q_i\) is independent of the usage of \(Q_j (i \neq j, 1 \leq i, j \leq M)\) and \(L_k\), which implies that the failure of their corresponding working lightpaths are independent of one another, then the probability that both \(Q_k\) and at least one of the other shared protection lightpaths are activated, which we denoted here as \(\alpha_k\), will be

\[
\alpha_k = U_k \sum_{i=1}^{m} U_i;
\]

assuming that all nodes and links along \(Q_k\) function properly.

**Proof**: The probability that at least one backup lightpath among \(Q_1, Q_2, ..., Q_m\) is activated is \(\sum_{i=1}^{m} U_i\) since the activations of backup lightpaths are independent of one another. Therefore, the probability of both \(Q_k\) and at least one backup lightpath among \(Q_1, Q_2, ..., Q_m\) 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 $V_{k1}, V_{k2}, ..., V_{kN}$, and the corresponding $N - 1$ fiber links are $l_{k1}, l_{k2}, ..., l_{k(N-1)}$. 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:

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

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 unavailable probability $b_k$ of the $Q_k$ will be:

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

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

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

**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 unavailable probability of the protection 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 unavailable probability $\phi_k$ for this connection is

$$\phi_k = \beta_k \prod_{i=1}^{N} b_{ki}. \quad (4)$$

**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 unavailable probability of a connection by multiplication with a factor equal to the unavailable probability (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 unavailable probability of a backup lightpath, the lightpath should follow the shortest path, and avoid sharing with too many backup lightpaths. To decrease the unavailable probability, 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. A protection mechanism of a WDM network must take this effect into consideration when choosing backup lightpaths.

The following several paragraphs analyze the protection correlation problem. First, we would like to define the following keywords.

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

**Protection-correlation parameter** $\delta_{ij}$: The impact of shared protection lightpath $Q_i$ 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. How to design an algorithm to avoid such high-order correlation so that the resulting backup paths can guarantee the availability? 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,

$$\delta_{ij} = \frac{(\beta_i - \xi_{ij})(\beta_j - \xi_{ij}) + \xi_{ij}}{\beta_i}. \quad (5)$$
Proof: Backup lightpaths $Q_i$ and $Q_j$ will be both activated with probability $\beta_i - \xi_{ij}(\beta_j - \xi_{ij})$, 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 $\delta_{ij} = \frac{(\beta_i - \xi_{ij})(\beta_j - \xi_{ij})}{\beta_i \beta_j}$.

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 $\beta_{ij}$, 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 $U_{ij}$ 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 $P_j$, $P_k$ for these three backup paths are correlated with each other as shown in Fig. 3, 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 $Q_i$, $\delta_{i(j,k)}$, 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:

$$\delta_{i(j,k)} \leq \delta_{ij} + \delta_{ik}.$$  \hspace{1cm} (6)

**Fig. 3.** 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:

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

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 paths exist, and the backup paths for those working path are shared backup lightpaths, then the impact on the blocking probability of one of those backup lightpaths by the sharing of other backup lightpaths will be less than the sum of the protection-correlation parameter of those backup lightpath.

Fig. 3 show one example for Proposition 5. In Fig. 3, there are three working lightpath $P_1$ (1 - 7 - 8 - 9 - 4, $\lambda_1$), $P_2$ (2 - 7 - 8 - 9 - 10 - 5, $\lambda_2$), and $P_3$ (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 $Q_1$ (1 - 11 - 16 - 17 - 6, $\lambda_4$), $Q_1$ (2 - 15 - 16 - 17 - 14 - 5, $\lambda_4$), and $Q_1$ (3 - 15 - 16 - 17 - 6, $\lambda_4$) are shared backup lightpaths all using $\lambda_1$.

**IV. Problem Definition**

The problem in this study deals with WDM mesh networks. In our studied network, we assume fiber $i$ has $W_i$ wavelengths for data channels in addition to the control channel $\lambda_i$. 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 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 [1], [15], [16] to calculate the optimum working lightpath \( P_new \) for a new connection. 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 \( P_new \), how to choose and set up a disjointed backup lightpath \( Q_new \) for \( P_new \). Such that the backup lightpath \( Q_new \), together with the working path \( P_new \), can satisfy the QoS requirements of a new connection while minimizing the required network resources. The algorithm should be able to differentiate different connections’ (lightpaths) QoS requirements. We regard such problems as lightpath shared protection (LPS) problems. Since the conventional RWA problems with static traffic requirement is an NP-complete problem [1], [15], the LPS problem should be similar in complexity for static traffic because the LPS problem introduces the path sharing, unavailability, and delay constraints in addition to the conventional RWA problem. The globally optimized solution for a LPS problem with static traffic requirement should be difficult to obtain. However, this study stresses on dynamic provisioning and protection in which a mesh WDM network can set up and take down a lightpath and its corresponding backup lightpath in real-time and dynamically.

V. DSLPM:DISTRIBUTED SHARED-LIGHTPATH-MANAGEMENT ALGORITHM

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

- **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.

- **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. 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 so that it can actually reflect the new status after the backup lightpath is added.

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:

- **Protection-path 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 available residual blocking probability \( R_i \) by the protection-correlation parameter \( \delta_{im} \). That is, \( R_i = R_i - \delta_{im} \).
  - **Step 4:** Use Eqn. (2) to decide the available residual unavailable probability \( r_{ijk} \) for every wavelength-link \( l_{ijk} \) in the path-complement graph for the current protection wavelength \( \lambda_k \).
  - **Step 5:** Use constraint-based shortest-path 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 hop distance path. However, it is necessary to apply the following two constraints for the new backup lightpath calculation:

\[
U_m \leq r_{ijk}, \forall l_{ijk} \in Q_m; \tag{7}
\]

\[
b_m \leq B_m. \tag{8}
\]

These constraints are used to guarantee the availability requirement for every protection lightpath.

- **Step 6:** Repeat Step 2 to Step 5 until all optimum backup lightpaths for all protection wavelengths are decided.

- **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.

- **Protection-path 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. Interested user please refer to [2] for the details procedure.

- **Protection-path setup and network state updated:** After 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 updated its parameters accordingly. 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. Please refer to [2] for take-down procedure.

**C. Backup Lightpath Activation**

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.

**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 path, it is also 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.

**VI. Algorithm Analysis**

The DSLPS 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 set up backup lightpaths. The most complicated 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 have 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 to tens of RTT.

- **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.
We 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. We use Fig. 1 as the network for our study. This simulation makes the following assumptions:

- There are 16 wavelengths in each fiber.
- The fiber cut probability is 5x10⁻⁷/mile/time-unit.
- The OXC failure probability is 1x10⁻⁷/time-unit.
- A connection request is blocked if it cannot setup its working path or its backup path successfully. If a working path is blocked, its backup path setup request will not be carried out.
- Connection is generated from two randomly selected nodes in the network. We assume that there are four classes of the connections in terms 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. Please note that the availability requirement will not be taken into consideration for 1:1 backup and unlimited shared backup schemes in calculating the backup lightpath.

We have studies 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 4 shows the connection blocking probability. It shows that when network’s offered load is low, the connection blocking probability 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.

Figures 5 and 6 show the blocking probability of working lightpaths and backup lightpaths, respectively. Figure 5 shows that, for a given network offered load, the shared protection scheme have higher blocking probability for working paths. This is because, actually, 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 resource. The QoS-based sharing scheme has somewhat higher blocking probability 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 5 and 6 also indicate that the blocking probability for backup path in 1:1 scheme is higher than the working path. 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-disjoined. However, with shared protection schemes, the backup path blocking probability is much lower than the working path.

We can also compare the average number of connections in the network for the three schemes. Figure 7 shows that, the total number of connections a 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 8 shows the average wavelength-link utilization of the network. For a given network, all three schemes’ average link utilization is similar when the offered load is low or high. 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 9 shows the average hop distance (AHD) for different types of lightpaths. It shows that the AHD for working lightpath is similar for all three schemes when the network offered load is low. The AHDs for the shared protection schemes are somewhat lower than the 1:1 scheme because their actual network load is lower than the 1:1 scheme as the result of the 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 those 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 higher probability than the shorter paths. 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 somewhat similar trend. They are higher than those of the working paths at the same offered load because the network requires the backup lightpaths to take a link-disjoined paths with the working paths. The AHD of the backup lightpath for the 1:1 scheme has the 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 the new backup path 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 the similar as the unlimited shared protection scheme.

B. Full Wavelength-conversion Networks

We also study the performance for the three backup schemes in a full wavelength-conversion network. We find that the overall trends of each figure for the full wavelength-conversion is exactly the same as the non wavelength-conversion network.
VIII. 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 fully 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. Backup lightpaths set up by the algorithm can always satisfy their explicit blocking probability requirements even though resource sharing is introduced. The proposed algorithm also takes the correlation of working lightpaths into consideration when finding a backup lightpath. It guarantees that the resource sharing by backup lightpaths and the correlation of the working lightpaths would not violate the availability of all previously set up backup lightpaths when a new backup lightpath is introduced. Our numerical studies have shown that the QoS-based scheme performs as well as 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.

References