# Integrated Dynamic Routing of LSPs in IP over WDM Networks: Full Protection and Partial Spatial-Protection

Qin Zheng and Mohan Gurusamy*

Department of Electrical and Computer Engineering
National University of Singapore, Singapore 117576
{engp1752, elegm}@nus.edu.sg

**Abstract.** We investigate the problem of Label Switched Path (LSP) protection using online integrated routing in IP over WDM networks. While certain mission- and time-critical applications require guaranteed 100% protection, other applications may have less stringent protection requirements. We consider these two kinds of protection scenarios and refer them as full protection (FP) and partial protection (PP), respectively. We first consider the full protection scenario and develop two integrated routing algorithms to select primary LSPs and backup LSPs, respectively. Next we consider the partial protection scenario, particularly, the partial spatial-protection (PSP) wherein the working traffic is unprotected against the failure of certain links along the primary LSPs according to the specified connection protection requirements. We develop an algorithm to determine the set of unprotected links with the objective of improving the backup resource sharing efficiency. We evaluate the performance of the proposed algorithms on the NSFNET and Pan-European optical networks.

## 1 Introduction

In IP/multi-protocol label switching (MPLS) over Wavelength Division Multiplexing (WDM) networks, IP/MPLS routers are directly connected to optical cross-connects (OXCs) which are interconnected via fiber links carrying multiple wavelength channels. IP/MPLS routers are also refereed to as Label Switched Routers (LSRs). End-to-end lightpaths are created across the optical core on the wavelength channels which in turn form the virtual topology to be used by the IP layer. A lightpath must use the same wavelength on all the links along its physical route. The virtual topology is then used by the IP layer for IP routing. Consequently, the IP layer paths can traverse multiple hops (lightpaths).

We consider a single link failure model in this paper and a connection is restorable by using a link-disjoint pair of an active LSP and a backup LSP. Both primary and backup LSPs may traverse a number of lightpaths which in turn

* This work was supported in part by the ONFIG-GMPLS project (NUS WBS No: R-263-000-231-593) funded by SERC, ASTAR, Singapore.

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 538–549, 2004.

are routed over a number of OXCs. The traffic are transmitted on the active (primary or working) LSPs during normal network operations and switched to the backup (protection) LSPs when failure occurs. Protection resources can be shared among multiple backup LSPs if their corresponding primary LSPs will not fail simultaneously.

As a variety of novel types of applications appear in Internet besides the traditional voice and data services, the ability of providing multiple levels of service performance becomes necessary. While voice traffic should have guaranteed 100% protection, other applications may require less stringent protection requirements [1]. Consequently, having various protection grades to satisfy the multi-level service requirements has received much attention recently [1,2,3]. Another motivation is the fact that since Internet traffic is often more sensitive to cost, it is desirable to have a range of protection services and cost [1].

### 1.1 Related Work

Integrated routing that incorporates the resource and topology information from both IP and optical layers has been proposed as a promising solution [4,5,6]. A salient feature of the integrated routing is that the path found can traverse IP logical (virtual) links in the IP layer and new wavelength channels at the optical layer which will lead to the creation of new virtual links. The integrated routing problem was first introduced in [5] and the impact of IP subnets on it was studied in [4]. The differentiated integrated routing considering o-e-o conversion constraints was studied in [7]. These approaches considered LSP provisioning without taking into account the survivability requirements. The problem of integrated routing of restorable connections was studied in [6]. The algorithms proposed for routing of working paths are essentially integrated physical-hop-based routing. The QoS requirements of working traffic and the wavelength resource constraints are not taken into account.

Next we describe the related work on partial protection. The problem of partial protection can be classified into three categories: partial traffic-protection, partial temporal-protection, and partial spatial-protection. In partial traffic-protection, the percentage of working traffic to be protected depends on the specified protection grade. Such a partial traffic-protection is considered in [1]. Partial temporal-protection is introduced in [2] where protection bandwidth can be shared with some working path which allows the connection to be unprotected during some periods of time. In partial spatial-protection, a connection is unprotected against some fiber link failures based on the survivability requirements. The differentiated reliability (DiR) problem studied in [3] belongs to this category.

We consider LSP-level partial spatial-protection in this paper wherein backup LSPs may not be available when certain links along working LSPs fail. We consider online integrated sub-$\lambda$ LSP routing of dynamic requests that arrive one by one with no prior information. In [3], offline $\lambda$ (lightpath) routing of static traffic was studied and lightpath-level partial spatial-protection was considered wherein some links along primary lightpaths are not protected by corresponding

backup lightpaths. As an LSP can traverse one or more lightpaths, protection at the LSP level makes it possible to specify the end-to-end protection grade for each connection request at the IP/MPLS layer.

### 1.2 Contributions

First we consider full protection scenario and develop integrated routing algorithms to select the primary LSPs and backup LSPs taking into account the constraints at both the MPLS and optical layers. Next we consider the LSP-level partial spatial-protection following the single link failure assumption. A connection request specifies the required protection grade (pg) where $0 \leq pg \leq 1$. An equivalent term is maximum failure probability (MFP) where $MFP = 1 - pg$. The MFP of a connection defines the maximum allowable probability with which backup path is not available upon occurrence of a single link failure in the network. For a connection request with less stringent protection requirement, the backup LSP need not be available for every possible link fault that may occur along the primary LSP. It is thus possible to select a set of links along the primary LSP for which the connection is unprotected, given the required protection grade is guaranteed. These links are called *unprotected links* with respect to the primary LSP of interest. As a result, the backup bandwidth on lightpaths along a backup LSP can be shared by another backup LSP even if the corresponding primary LSPs of these two requests share a common link, if one of these two primary LSPs choose the shared link to be an unprotected link.

In this paragraph we illustrate how to determine the number of unprotected links for a connection request with protection grade $pg$. Suppose $F$ is the set of unprotected links. The link failure probability (LFP) is defined as the probability that the given link fails upon a single link fault in the network. The LFP can be derived from normalized link downtime ratio and the length of the links in the network [3]. The following condition must be satisfied $\sum_{i \in F} LFP_{(i)} \leq MPF$ to select $F$ for a specified $pg$. For simplicity, we assume that all the links have equal failure probabilities and thus the LFP for each link is $\frac{1}{L}$ for a network with $L$ fiber links. The number of unprotected links allowed is denoted by $F_m$ where $F_m$ is the largest integer that satisfies the condition $\frac{1}{L} \times F_m \leq MFP$. The case where links have different failure probabilities can be dealt with using the first condition. After converting the protection grade to the number of unprotected links allowed, one crucial problem is to determine the set of unprotected links. We propose an algorithm which selects unprotected links with the objective of reducing the backup bandwidth needed.

## 2 An Example of LSP-Level Partial Spatial-Protection

Fig. 1 shows a network which comprises four IP routers connected to four OXCs through wavelength ports. The OXCs are interconnected by fiber links labeled a through e which carry multiple wavelength channels. Assume that at an instance of time, a new request which requires bandwidth b from router4 to router3

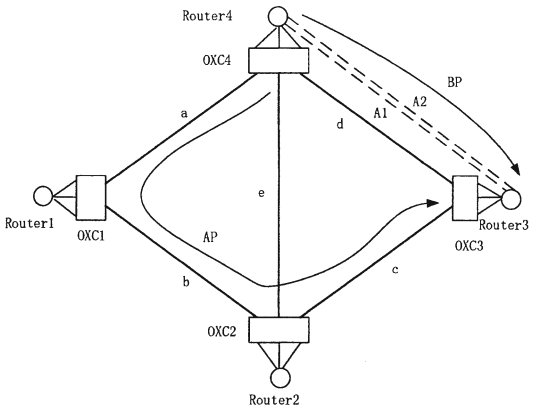


**Fig. 1.** Example of LSP-level partial spatial-protection

arrives. There exists a connection from router4 to router3 with bandwidth b1. The existing connection routes its active path (AP) and backup path (BP) on virtual links (dashed lines) A1 and A2, respectively. A1 traverses fiber links e,c and A2 traverses fiber link d. Suppose that the new request opens a new virtual link on fiber link a-b-c for the primary path and uses existing virtual link A2 in the backup path. Assume that the existing request has 100% protection requirement while the new request specifies the connection to be 80% restorable against any single link failure.

Now we compute the amount of protection bandwidth to be reserved on the backup path for the new request. As the primary paths of the two requests traverse one common fiber link c, the backup resources on arc A2 cannot be shared by the new request. As a result, $b1 + b$ amount of bandwidth needs to be reserved on arc A2 if the new request is to be provided with 100% protection. Next we consider the protection grade of specified 80% survivability for the new request. Since we assume that all the fiber links are equally likely to fail and there are five links in the network, it implies that the new request can be unprotected against the failure of one fiber link. As fiber link c is the common risk of the two requests which makes sharing impossible, we choose it to be unprotected. Consequently, $max(b1, b)$ amount of bandwidth needs to be reserved on arc A2. We note that choosing fiber link a or b to be unprotected will require $b1 + b$ amount of protection bandwidth on arc A2.

## 3 The Proposed Integrated Routing Algorithms

### 3.1 Network Model and Problem Statement

We consider a network of $N$ nodes connected by $L$ bidirectional fiber links each carrying $W$ wavelength channels. We assume that each node comprises an OXC and a LSR. The OXCs have no wavelength conversion capability. We consider

dynamic traffic where LSP requests arrive one-by-one with no prior information about future requests. An LSP-request is specified as $< s, d, b, pg >$ where $s$ is the source node, $d$ is the destination node, $b$ is the amount of bandwidth required, and $pg$ is the specified protection grade. For each connection request, a link-disjoint primary path and backup path must be found. The objective is to reduce the delay for working traffic and minimize the protection bandwidth needed on the backup path while satisfying the protection grade. We consider the case of $pg = 100\%$ in this section.

**Notations**

- $l_j^W$ is the number of available wavelength channels on fiber link $l_j$ at an instance of time. Initially, $l_j^W$=$W$.
- $a_m$ is the unidirectional wavelength-switched path (lightpath) defined as an ordered vector of traversed fiber links $a_m =< l_1, l_2, ...l_{h_m} >$, where $h_m$ denotes the physical length of $a_m$. Further, $a_m$ represents the directed arc between two nodes in the virtual topology, with a fixed bandwidth denoted by $B_m$. We use the terms *link* and *arc* to refer to the edges in the physical topology and virtual topology.
- $r_m^j$ is a binary variable which indicates whether link $l_j$ is used in arc $a_m$.
- $n_p^l$ denotes the number of LSRs traversed by the primary LSP.
- $V_p^m$ is a binary variable which indicates whether the primary LSP traverses arc $a_m$.
- $C_p^j$ is a binary variable which indicates whether the primary LSP traverses a free wavelength channel on link $l_j$. Note the path found by integrated routing can traverse arcs and wavelength channels which lead to the creation of new arcs.
- $A_p^j$ is a binary variable which indicates whether the primary LSP traverses link $l_j$.
- $A_p$ denotes the set of links traversed by the primary LSP.
- $V_b^m$ is a binary variable which indicates whether the backup LSP traverses arc $a_m$.
- $C_b^j$ is a binary variable which indicates whether the backup LSP traverses a free wavelength channel on link $l_j$.
- $T_m$ is an ordered vector associated with arc $a_m$ to record the backup bandwidth required to protect against each fiber link failure in the network. $T_m =< B_m^1, B_m^2, ..., B_m^j, ...B_m^L >$, where $B_m^j$ is the amount of backup bandwidth needed on $a_m$ when link $l_j$ fails.
- $T_m^B$ denotes the backup bandwidth reserved on arc $a_m$ which is the maximum value in the vector $T_m$.
- $T_m^l$ denotes the link corresponding to $T_m^B$. This information is used to determine the set of unprotected links as discussed in Section 4.1.
- $b_m^a$ denotes the additional backup bandwidth needed on arc $a_m$ to route the backup path for the current request.
- $k_1, k_2$ constants, $k_1 \gg k_2$ such that $k_1 x' > k_2 y'$, where $x'$ is the smallest possible non-zero $x$-value and $y'$ is the largest possible non-zero $y$-value in a function of the form $k_1 x + k_2 y$ .

### 3.2 Algorithms

**Primary Path Selection.** The Minimum Delay Least Congestion integrated routing algorithm (MDLC-IRA) is used to select the primary path. MDLC-IRA chooses a path that traverses minimum number of LSRs, which attempts to minimize the global average queuing delay. In case of a tie, the path which creates lightpaths on fiber links with more available channels is preferred. The objective is to avoid saturating wavelength resources on certain links, thus increases the possibility of opening new lightpaths on these links. Consider a path $p$ which traverses $n_p^l$ number of LSRs. If $l_j^W$ is the number of free wavelength channels on link $j$ traversed by $p$, $W - l_j^W$ gives the number of occupied channels on it. Now the cost $C$ of path $p$ is defined as

$$C = k_1 n_p^l + k_2 max_{C_p^j=1}(W - l_j^W) \tag{1}$$

The MDLC-IRA chooses the path that minimizes the cost $C$ as the primary path. MDLC-IRA assigns edge weights as follows: each o-e-o edge is assigned weight $k_1$. For each link $j$, $k_2(W - l_j^W)$ is set as weight. A Dijkstra-like shortest path algorithm is used to compute the minimum cost path and the wavelength resources on links are dealt with to decide the bottleneck similar to the widest-shortest path selection.

**Backup Path Selection.** The Minimum Bandwidth Least Congestion integrated routing algorithm (MBLC-IRA) is used to route the backup path. MBLC-IRA minimizes the total amount of bandwidth that needs to be reserved on the backup path. The additional bandwidth needed on links traversed is $b$ and that on existing arcs is given by $b_m^a$ ($b_m^a \leq b$) which is determined by Equation (3) and (4). The tie is broken using a method as in MDLC-IRA. MBLC-IRA assigns edge weights in the following way: Each o-e-o edge is assigned weight $\epsilon$. For each arc $a_m$, $k_1 h_m b_m^a$ is set as weight. For each link $j$, $k_1 b + k_2(W - l_j^W)$ is set as weight. A Dijkstra-like shortest path algorithm is used to compute the minimum cost path and the wavelength resources on links are dealt with to decide the bottleneck similar to the widest-shortest path selection.

$$C = k_1\Big(\sum_{C_b^j=1} b + \sum_{V_b^m=1} h_m b_m^a\Big) + k_2 max_{C_b^j=1}(W - l_j^W) \tag{2}$$

$$A_p^j = C_p^j \;\; or \;\; V_p^m r_m^j \tag{3}$$

$$b_m^a = max_{j=1}^{L}(B_m^j + A_p^j b) - T_m^B \tag{4}$$

Once the primary path is chosen, whether fiber link $j$ is traversed by it can be determined from Equation (3). This helps to determine the set of fiber links traversed by the chosen primary path. The $b_m^a$ value on arc $a_m$ is calculated using Equation (4). It requires updates of the entries in $T_m$ that correspond to the links traversed by the primary path. For each link $j$ traversed by the primary path, the entry $B_m^j$ in $T_m$ associated with arc $a_m$ is increased by $b$. The

additional backup bandwidth needed $b_m^a$ on arc $a_m$ is the amount by which the maximum value $T_m^B$ is increased. For the example in Fig. 1, the $T_m^B$ value of arc A2 is b1 and b1+b before and after the new request is honored, respectively. The $b_m^a$ value of arc A2 is b and $T_m^l$ is link c.

## 4 LSP-Level Partial Spatial-Protection

In this section, we consider multiple levels of protection grades of connections and the objective is to satisfy these user-specific requirements to minimize the network resources. We first propose an algorithm to determine the unprotected links according to the protection grades. We explain how the algorithm can improve the backup sharing efficiency and in turn reduce the total amount of bandwidth required on the backup path. Finally, we discuss the actual *restorable probability* of each connection request which is defined as the probability that the backup LSP is available upon a single link failure.

### 4.1 Improved Backup Sharing Efficiency with PSP

Consider a connection request $< s, d, b, pg >$ where $pg$ is the specified protection grade denoting the PSP requirement. We translate the protection grade into the permissible number of unprotected links, denoted by $F_m$. We recall that the failure probability of each of the $L$ links is assumed to be the same and $F_m$ is the largest integer number that satisfies $\frac{1}{L} \times F_m \leq MFP$ where $MFP = 1 - pg$. We emphasize that our routing algorithm can be easily modified to account for the case where links have different failure probabilities.

We first choose the primary path and backup path by using MDLC-IRA and MBLC-IRA, respectively. We then choose $F_m$ number of links to be unprotected by using the following algorithm in a way to increase the backup sharing efficiency. The following pseudo code shows the steps taken place to determine the unprotected link set $F$.

The algorithm searches the existing arcs traversed by the current backup path in step1. If $b_m^a > 0$ (which means that the backup bandwidth on arc $a_m$ is increased) and $T_m^l$ is not in $F$, then $T_m^l$ is added to $F$. The number of chosen links ($F_l$) is increased by 1. The idea is to combine the choice of unprotected links with the backup sharing on existing arcs along the backup path. Step1 continues if $F \subset A_p$ (the fiber link set traversed by the current primary path) and $F_l < F_m$. If the above condition still holds when all the existing arcs are searched, the algorithm chooses the unprotected links randomly from the remaining links in $A_p$ but not in $F$ in step2. We note that the unprotected links can also be selected from the remaining links based on the link criticality if such information is available in the network. The proposed algorithm only uses $T_m^l$ information on the arcs traversed by the current backup path which makes the decision of unprotected links quickly.

For the example in Fig. 1, the proposed algorithm will choose link c as the unprotected link. As a result, the corresponding $B_m^c$ value of arc A2 will remain

unchanged. The $T_m^B$ value of arc A2 is b1 and max(b1,b) before and after the new request is honored, respectively. The additional backup bandwidth needed on arc A2 is max(b1,b)-b1 to protect the new request.

### 4.2 Discussion on Connection Restorable Probability

Although connections are protected with specific survivability grades, they have higher probability to be restored against a single link failure. Generally, the unprotected links selected in step 2 can be restored as they are allowed to share the backup resources on $a_m$ freely (without increasing $T_m^B$). Furthermore, we consider dynamic traffic and the values in $T_m$ for each arc $a_m$ keep changing whenever a new request is honored or an existing request terminates. In both cases, the $B_m^j$ value for unprotected link $j$ on arc $a_m$ could be sufficiently lower than $T_m^B$ to satisfy the condition $B_m^j + b \leq T_m^B$ which means that this arc can be used as backup even when unprotected link $j$ fails. We study this effect in Section 5.3.

## 5 Performance Study

### 5.1 Simulation Model

We consider a dynamic network traffic model, and connections are setup and torn down dynamically. The traffic arrival at a node follows Poisson distribution with rate $\lambda$ and the holding time of a connection is exponentially distributed with a mean of $1/\mu$. The destination node for a connection is selected using a uniform distribution among all the nodes except the source node. The traffic load per node is defined as $\lambda/\mu$ and expressed in Erlangs.

Simulation experiments are performed on two networks: NSFNET with 14 nodes and 21 links and the Pan-European optical network with 19 nodes and 38 links. We assume 8 wavelength channels on each fiber link in the two networks. The bandwidth requested by a connection is uniformly distributed in the range of (1, 6). The maximum capacity of a wavelength is assumed to be 10. The system parameter varied is the load per node. For the NSFNET, the load is varied from 2.0 to 8.0 Erlangs. For the Pan-European optical network, the load is varied from 2.0 to 12.0 Erlangs as it is denser than the NSFNET.

In the first set of experiments, we consider full protection (FP) for all requests and compare the performance of the proposed integrated routing algorithms MDLC-IRA and MBLC-IRA to the integrated IP-hop routing and integrated physical-hop routing algorithms. Both the integrated IP-hop routing algorithm and integrated physical-hop routing algorithm route a path on virtual links and wavelength channels. The integrated IP-hop routing finds the primary path and backup path based on the virtual hop counts. The integrated physical-hop routing simply finds both paths based on the physical hop counts. In the second set of experiments, the protection grades are taken into account and we show the improvements obtained using partial spatial-protection (PSP) compared to

the full protection. We consider three classes of traffic which permit 0, 1 and 2 unprotected links in the primary path, respectively. We assume that the failures are uniformly distributed among all the fiber links in the network and each link has the equal probability to fail. Each request is randomly assigned to class 0, 1, or 2 with probability 0.4, 0.3 and 0.3, respectively.

The performance metrics considered are the *blocking probability* and *average restorable probability*. Each simulation experiment is run with a large number of connection requests on the order of 100000 per node. The experiment is repeated several times to achieve accurate results with a small confidence interval for a 95% confidence level.

### 5.2 Blocking Probability

Blocking probability is defined as the percentage of rejected connections among all the connection requests. The objective of online routing algorithms is to minimize this metric. Figure 2 and Fig. 3 show the blocking probability of different integrated routing algorithms in the two networks with full protection. We recall that, the MDLC-IRA and MBLC-IRA are used to route the primary path and backup path, respectively. In both figures we observe that the proposed routing algorithms MDLC-IRA and MBLC-IRA perform best and the integrated physical-hop routing algorithm is better than the integrated IP-hop routing algorithm. The integrated IP-hop routing algorithm performs poorly as it prefers paths traversing less virtual links. When there is no existing IP link with enough bandwidth between the ingress and egress nodes, the algorithm will try to open a new virtual link which leads to inefficient resource usage and higher blocking.

Figure 4 and Fig. 5 show the blocking probability of the proposed routing algorithms MDLC-IRA and MBLC-IRA with and without considering protection grades. In both figures we observe that the performance is much better when protection grades are taken into account. This is because the bandwidth on the backup paths are reduced by appropriately choosing the set of unprotected links.

### 5.3 Average Restorable Probability

The protection grades of class 0, 1, 2 traffic are 100%, $20/21 = 95.24\%$ and $19/21 = 90.48\%$, respectively in the NSFNET; and 100%, $37/38 = 97.37\%$ and $36/38 = 94.74\%$, respectively in the Pan-European network. Average restorable probability is defined as the average probability that a connection can be restored against any link failure in the network. As differentiated protection grades are provided to each class of traffic, this metric is important to measure whether the user-specific requirements can be met. In our experiments, we measure the restorable probability for each connection constantly at a time period 0.01 of the mean connection holding time. Then for each traffic load, these values of all the measuring periods are used to get the mean probability for each class.

Figure 6 and Fig. 7 show the average restorable probability for each class of traffic in the two networks. In the experiments, all the requests can satisfy their corresponding protection requirements. In both figures we observe that the

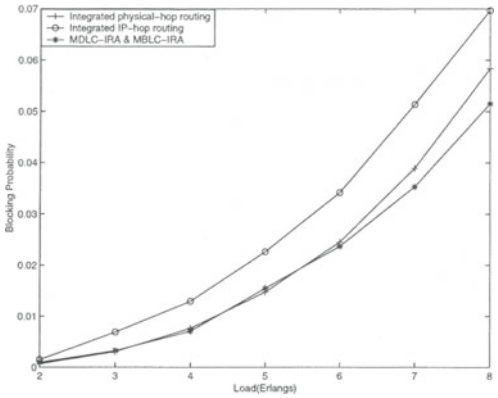


**Fig. 2.** Blocking probability with FP in NSFNET

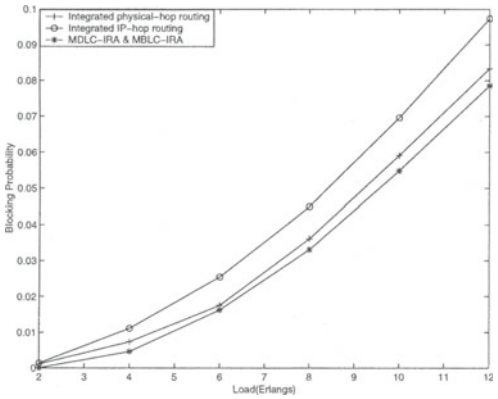


**Fig. 3.** Blocking probability with FP in Pan-European Network

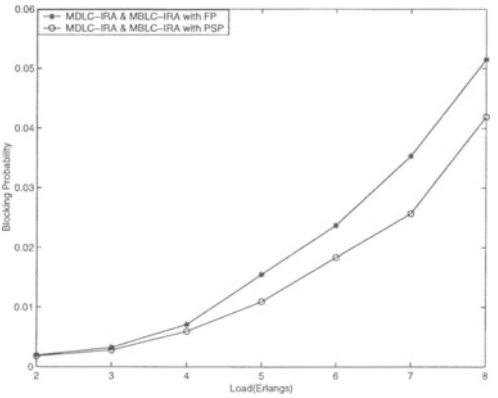


**Fig. 4.** Blocking probability with FP and PSP in NSFNET

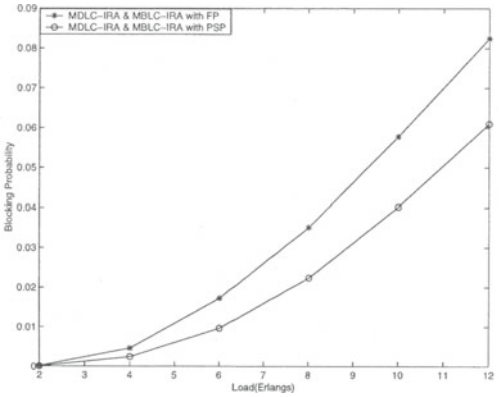


**Fig. 5.** Blocking probability with FP and PSP in Pan-European Network

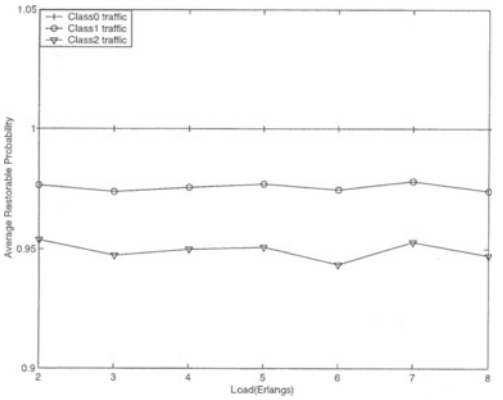


**Fig. 6.** Average restorable probability with PSP in NSFNET

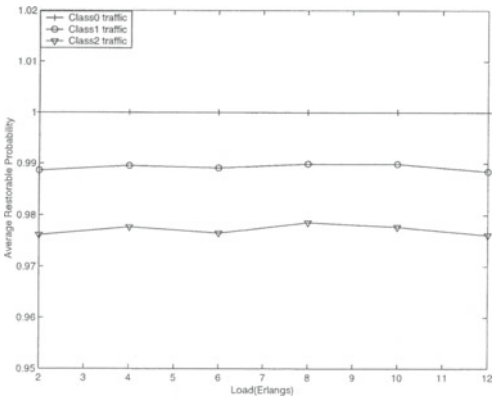


**Fig. 7.** Average restorable probability with PSP in Pan-European Network

average restorable probability is above the protection grades required. As explained in Section 4.2, although each connection has the number of unprotected links corresponding to the protection grade, backup resources could be available even when these links fail due to the backup sharing and dynamic nature of connection requests.

## 6 Conclusions

We considered the problem of LSP protection using integrated routing with the objective of providing different protection grades (full and partial). We developed integrated routing algorithms MDLC-IRA and MBLC-IRA to select the primary LSPs and backup LSPs taking into account the constraints at both the MPLS and optical layers. We proposed an algorithm to determine the set of unprotected links according to the specific spatial-protection requirements to reduce the bandwidth to be reserved on the backup path. We argued that although connections are provided with a specific protection grade, they have higher probability to survive from a single link failure due to backup sharing and the dynamic nature of traffic. We evaluated the performance of the proposed algorithms on the NSFNET and Pan-European optical networks. Through extensive simulations, we demonstrated that LSP full protection using the proposed integrated routing algorithms can reduce the connection blocking probability considerably. The blocking performance improves significantly due to the improved backup sharing efficiency when protection grades are considered. Further, connections in each class have higher probability to be restored than their protection requirements.

## References

1. Gerstel, O., Sasaki, G.: Quality of protection (QoP): a quantitative unifying paradigm to protection service grades. Optical Networks Magazine Vol. 3 (2002)
2. Mohan, G., Somani, A.: Routing dependable connections with specified failure restoration guarantees in WDM networks. IEEE INFOCOM Vol. 3 (2000) 1761–1770
3. Fumagalli, A., Tacca, M., Unghvary, F., Farago, A.: Shared path protection with differentiated reliability. IEEE ICC Vol. 4 (2002) 2157–2161
4. Acharya, S., Gupta, B., Risbood, P., Srivastava, A.: IP-subnet aware routing in WDM mesh networks. IEEE INFOCOM Vol. 1 (2003) 1333–1343
5. Kodialam, M., Lakshman, T. V.: Integrated dynamic IP and wavelength routing in IP over WDM networks. IEEE INFOCOM Vol. 1 (2001) 358–366
6. Zheng, Q., Mohan, G.: An Efficient Dynamic Protection Scheme in Integrated IP/WDM Networks. IEEE ICC Vol. 2 (2003) 1494–1498
7. Cheng Tien E., Mohan, G.: Differentiated QoS routing in GMPLS-based IP/WDM Networks. IEEE Globecom Vol. 3 (2002) 2757–2761