Fault Management in IP-Over-WDM Networks: WDM Protection Versus IP Restoration

Laxman Sahasrabuddhe, S. Ramamurthy, and Biswanath Mukherjee

***Abstract*—We consider an IP-over-WDM network in which network nodes employ optical crossconnects and IP routers. Nodes are connected by fibers to form a mesh topology. Any two IP routers in this network can be connected together by an all-optical wavelength-division multiplexing (WDM) channel, called a lightpath, and the collection of lightpaths that are set up form a virtual topology.**

In this paper, we concentrate on single fiber failures, since they are the predominant form of failures in optical networks. Since each lightpath is expected to operate at a rate of few gigabits per second, a fiber failure can cause a significant loss of bandwidth and revenue. Thus, the network designer must provide a fault-management technique that combats fiber failures. We consider two fault-management techniques in an IP-over-WDM network: 1) provide protection at the WDM layer (i.e., set up a backup lightpath for every primary lightpath) or 2) provide restoration at the IP layer (i.e., overprovision the network so that after a fiber failure, the network should still be able to carry all the traffic it was carrying before the fiber failure). We formulate these fault-management problems mathematically, develop heuristics to find efficient solutions in typical networks, and analyze their characteristics (e.g., maximum guaranteed network capacity in the event of a fiber failure and the recovery time) relative to each other.

***Index Terms*—Fault management, integer linear program, Internet protocol (IP), optical network, protection, restoration, wavelength-division multiplexing (WDM), wavelength routing.**

I. Introduction

WAVELENGTH-division multiplexing (WDM) divides the tremendous bandwidth of a fiber (up to 50 Tbits/s) into many nonoverlapping wavelengths, called WDM channels [1], [2]. Each WDM channel may be operated at whatever speed one desires, e.g., peak electronic speed of a few gigabits per second (Gbps). Transmissions on different wavelengths are coupled into a single fiber using wavelength multiplexers. An optical crossconnect (OXC) can switch the optical signal on a WDM channel from an input port to an output port without requiring the signal to undergo any optoelectronic conversion. If an OXC is equipped with wavelength converters, then the OXC can also change the wavelength of an incoming optical signal as it passes through the switch.

A lightpath is a point-to-point all-optical wavelength channel that connects a transmitter at a source node to a receiver at a destination node [3]. Using OXCs at intermediate nodes and via appropriate routing and wavelength assignment, a lightpath can create virtual (or logical) neighbors out of nodes that are geographically far apart in the network; thus, a set of lightpaths embeds a virtual (or logical) topology on the network.[1] In the virtual topology, a lightpath carries not only the direct traffic between the nodes it interconnects but also traffic between nodes that are not directly connected in the virtual topology by employing the "multihop approach," namely, by using electronic packet switching at the intermediate nodes in the virtual topology. This electronic packet-switching functionality can be provided by Internet protocol (IP) routers, leading to an IP-over-WDM. Fig. 1(a) shows the architecture of a node that has a single transceiver per wavelength. Note that the node architecture can be extended to support multiple transceivers per wavelength by adding additional fibers between the OXC and the IP router. Fig.1(b) shows an example of multihop communication between node 0 and node 9.

Upgrading an optical network is a costly affair; hence, it is desirable to design the optical network so that it can accommodate a large increase in network traffic before it needs to be upgraded. In this paper, we model the variation in network traffic by multiplying the traffic matrix by a scalar, called the "load factor," which we denote by α.

We consider the following network design problem. We are given an IP-over-WDM network and a traffic matrix. We are required to find a virtual topology and the corresponding traffic flow assignment that will a) provide protection against a single fiber failure[2] and b) maximize α. Note that for a given traffic matrix, maximizing the value of α is equivalent to maximizing the guaranteed network capacity, which we define as the maximum amount of traffic in the network that can be protected against a single fiber failure event.

Next we elaborate on the two fault-management techniques and compare them via an illustrative example.

A. Fault-Management Techniques

There are essentially two types of fault-management techniques [5]–[7]: protection [8]–[13] and restoration [14]–[16]. In *protection*, spare capacity is reserved during call setup. In *restoration*, the spare capacity available after the fault's occurrence is utilized for rerouting the disrupted traffic. Generally,

Manuscript received February 15, 2001; revised July 30, 2001. This work was supported by the National Science Foundation under Grant ANI-9805285.

L. Sahasrabuddhe and B. Mukherjee are with Summit Networks, Inc., San Jose, CA 95616 USA (e-mail: sahasrab@cs.ucdavis.edu).

S. Ramamurthy is with Tellium, Inc., Oceanport, NJ 07757 USA.

Publisher Item Identifier S 0733-8716(02)00150-6.

[1]In this paper, the term "link" refers to a unidirectional fiber, while the term "fiber" refers to a bidirectional fiber. We make this distinction because lightpaths in our study are unidirectional while physical connectivity between nodes is provided via bidirectional fiber links.

[2]Since single fiber failures are the predominant form of failures in optical networks, we concentrate on this form of failure. The frequency of faults in networks is represented by a quantity called *failure-in-time* (FIT), which is defined as the number of failures of a network component in 10^9 h. Some representative FIT values for network components are [4] 10^4 FITs per 10 km of fiber, 10^5–10^6 FITs for SONET equipment, 10^3–10^4 FITs for couplers and multiplexers, etc.

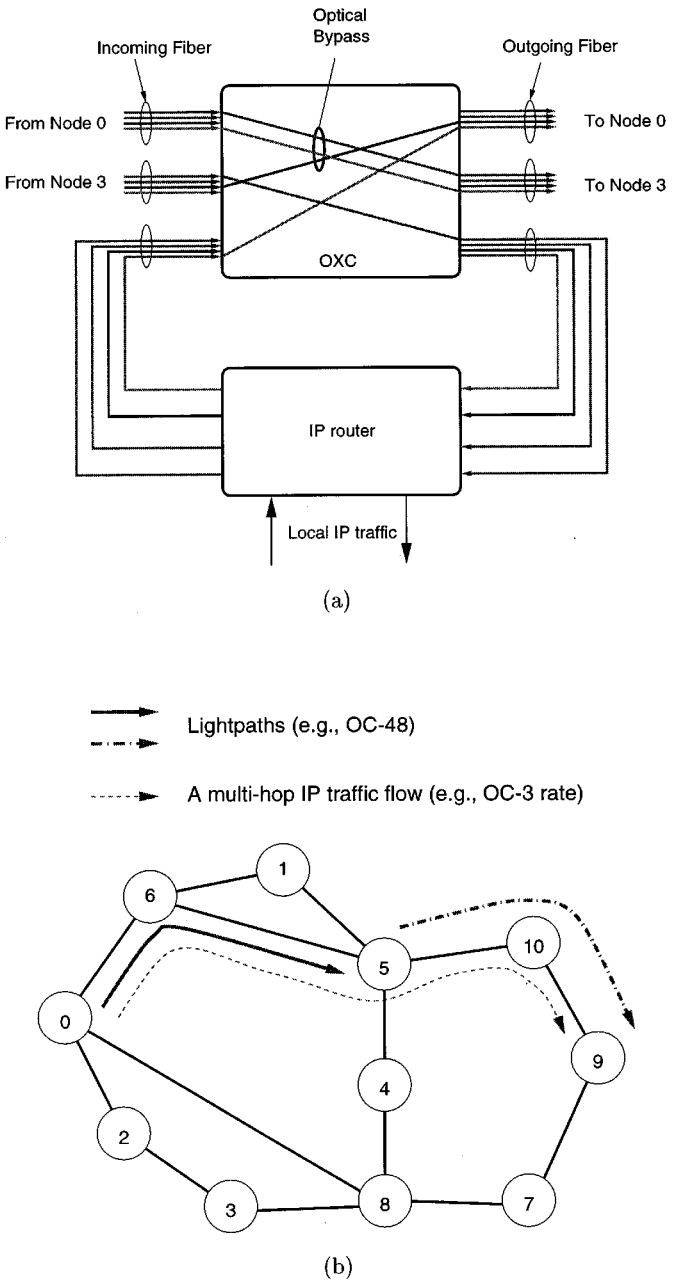

Fig. 1. (a) Architecture of a node in an IP-over-WDM network. (b) An example that illustrates communication via the "multihop approach." IP traffic from node 0 to node 9 is switched electronically from the 0→5 lightpath to the 5→9 lightpath at node 5.

restoration schemes are more efficient in utilizing capacity due to the sharing of the spare capacities, while protection schemes have a faster recovery time and provide guarantees on the recovery.

For an IP-over-WDM network, two possible fault-management techniques are 1) provide protection at the WDM layer or 2) provide restoration at the IP layer. In case 1), we need to set up a backup lightpath for every primary lightpath in the network. In case 2), we need to overprovision the network so that after a fiber failure, the network should still be able to carry all the traffic it was carrying before the fiber failure (after rerouting the disrupted traffic).

1) WDM Protection: In WDM path protection, during the call setup of a lightpath, a backup lightpath is set up as well so that in the event of a fiber failure, all the traffic on the primary lightpath can be diverted to the backup lightpath.[3] . Path protection comes in two flavors. In this paper, we will employ shared-path protection because it is more capacity efficient than dedicated-path protection. (Both of these approaches are briefly described below.)

a) *Dedicated-path protection:* At the time of call setup, for each primary path, a fiber-disjoint[4] backup path and wavelength are reserved and dedicated to that call. The backup wavelength reserved on the links of the backup path are dedicated to that call and are not shared with other backup paths.

b) *Shared-path protection:* At the time of call setup, for a primary path, a fiber-disjoint backup path and wavelength are reserved. However, the backup wavelength reserved on the links of the backup path may be shared with other backup paths. As a result, backup channels are shared among different failure scenarios (which are not expected to occur simultaneously), and therefore shared-path protection is more capacity efficient when compared with dedicated-path protection.

2) IP Restoration: The Internet can be viewed as a collection of autonomous systems (ASs), each of which can range in size from a small corporate network to a large backbone network. An AS consists of a set of routers that belong to the same administrative domain. Routers within an AS exchange routing information by employing an interior gateway protocol (IGP). (An example of an IGP employed by routers in an AS is the "open shortest path first" (OSPF) protocol.) By using an IGP, an AS can combat a link failure—i.e., when a link fails along a primary path between two nodes/routers in the AS, the IGP can dynamically find an alternate path between the two nodes. In this paper, we assume that the IGP can perform load sharing—i.e., if there are multiple routes from a source to a destination, then the IGP can distribute traffic over these multiple routes.

B. Illustrative Example

In this section, we illustrate the two fault-management techniques via an example. In the 11-node network shown in Fig. 2, let us assume that a WDM channel can carry one unit of traffic, and we want to send one unit of traffic from node 4 to node 6 and one unit of traffic from node 5 to node 9. Let us also assume that the network has two wavelengths λ_1 and λ_2, and there are two transceivers (i.e., one transmitter and receiver per wavelength) per node. Now, the goal is to set up primary lightpaths (and backup lightpaths) such that even after a fiber failure, the network should be able to route the same amount of traffic.

If we employ WDM-layer shared-path protection, then a possible solution is shown in Fig. 2. The primary lightpaths are (4, 5,

[3]An alternative to path protection is called link protection [8] However, WDM path protection typically outperforms link protection. Accordingly, WDM link protection will not be considered in this paper.

[4]By fiber disjoint, we mean that the backup path for a connection has no fibers in common with the primary path for that connection. Node failures can be accommodated by making the primary and the backup paths node disjoint as well.

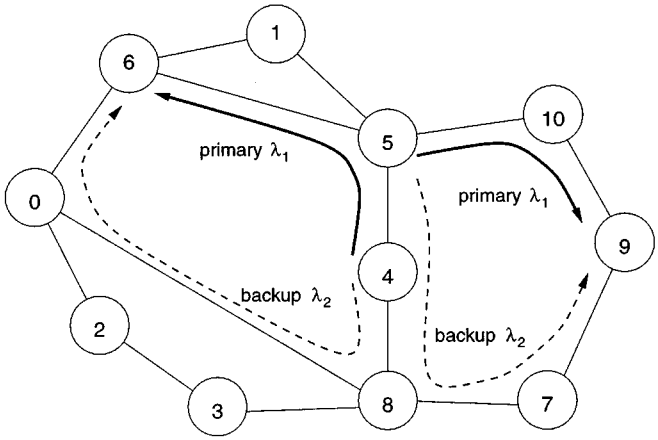

Fig. 2. The WDM shared-path protection solution.

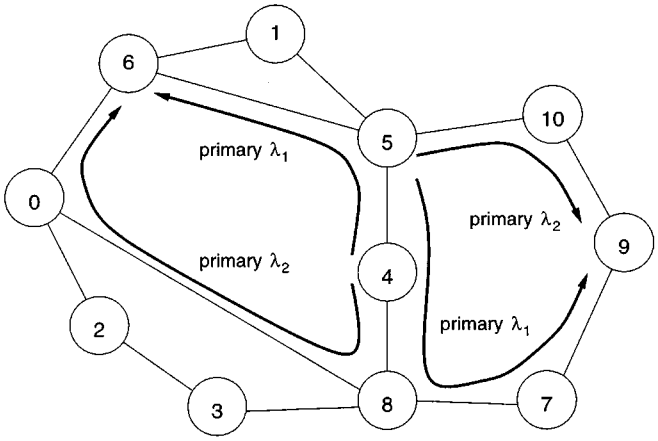

Fig. 3. The IP-restoration solution.

6) and (5, 10, 9), both on wavelength λ_1. The backup lightpaths are (4, 8, 0, 6) and (5, 4, 8, 7, 9), both on wavelength λ_2. Note that since the primary lightpaths are fiber disjoint, the backup lightpaths can share wavelength λ_2 on fiber (4, 8). Now, if the fiber (4, 5) fails, then all the traffic on the primary lightpath (4, 5, 6) on λ_1 is routed over the backup lightpath (4, 8, 0, 6) on λ_2.

Next, let us consider the IP-restoration technique shown in Fig. 3. The solution consists of two lightpaths between node 4 and node 6 along the routes (4, 5, 6) and (4, 8, 0, 6) on wavelengths λ_1 and λ_2, respectively. Similarly, there are two lightpaths from node 5 to node 9 along the routes (5, 10, 9) and (5, 4, 8, 7, 9) on wavelengths λ_2 and λ_1, respectively. Recall that in the IP-restoration scheme, we do not back up lightpaths at the WDM layer. Thus, before fiber (4, 5) fails, 0.5 units of traffic between node 4 and node 6 are routed over lightpaths (4, 5, 6) and (4, 8, 0, 6). After fiber (4, 5) fails, 0.5 units of traffic that were flowing over the lightpath (4, 5, 6) are routed over lightpath (4, 8, 0, 6).

C. Contribution of This Paper

The contribution of this paper has six parts. First, we derive a formula to compute the maximum guaranteed network capacity in an IP-over-WDM network that employs the two fault-management techniques. Second, we develop mathematical formulations of these fault-management techniques,[5] which turn out to be integer linear programs (ILPs). The solution to the ILP formulation[6] provides us with an optimal virtual topology and a traffic flow assignment that maximizes the guaranteed network capacity. Third, since the complete ILP formulations were taking a very long time to solve, we experimented by splitting the ILP formulations into two parts. For WDM shared-path protection, the first part sets up primary lightpaths, while the second part sets up the backups lightpaths. For IP restoration, the first part sets up primary lightpaths, while the second part overprovisions the network by setting up some "extra" lightpaths. This approach speeded up the solution time at the cost of optimality. Fourth, we develop heuristic algorithms for computing a virtual topology and the traffic flow assignment that maximizes the guaranteed network capacity. Fifth, for the IP restoration case, we obtain results for the amount of "premium" and "nonpremium" traffic that may be carried in the network. (Recall that in the IP restoration case, the network is overprovisioned. Thus, the "overprovisioned" capacity may be employed to carry "nonpremium" traffic that is not guaranteed against fiber failures.) Finally, we analytically compare the recovery time for WDM protection with that of IP restoration.

Our results from these ILP formulations and heuristics demonstrate an interesting phenomenon in which the WDM shared-path protection technique outperforms the IP-restoration technique under certain conditions, such as having a single transmitter and receiver per wavelength per node.

D. Organization

The rest of this paper is organized as follows. In Section II, we derive a formula to compute the maximum guaranteed network capacity in an IP-over-WDM network. Section III contains the ILP formulations for the two fault-management approaches. Section IV describes the heuristic algorithms for computing a virtual topology and the traffic-flow assignments for the two fault-management techniques. Section V presents an analysis of the recovery times for WDM protection and IP restoration. Section VI presents some illustrative numerical results, and Section VII concludes the study.

II. An Upper Bound for the Guaranteed Network Capacity

In this section, we derive a formula to compute an upper bound for the guaranteed network capacity, which is equivalent to finding an upper bound for α, the load factor. An upper bound for α can be computed by finding the minimum of the following three upper bounds.

1) Given the topology G of the network and the traffic matrix Λ, we can compute an upper bound on α as follows. Let C be a cutset that partitions the topology G into two components whose node sets are V_1 and V_2. Now, let us define the *congestion with a single link failure* of a cutset

[5]The routing and wavelength assignment (RWA) problem (with no protection) has been shown to be NP-complete [3]. We anticipate that the fault-management problems are NP-complete as well because they include RWA as a subproblem.

[6]We have utilized the *CPLEX 6.5* software package to solve the instances of the ILPs.

as the average traffic on the links in the cutset, under the assumption that one of the links in the cutset has failed. We denote this congestion by τ_C, i.e.,

$$\tau_C = \frac{\sum_{u \in V_1, v \in V_2} \Lambda_{uv}}{|C| - 1} \tag{1}$$

where Λ_{uv} is equal to the traffic from node u to node v. Let τ_C^* be the maximum value of τ_C taken over all possible cutsets. Thus, if the capacity of a lightpath is equal to B, then the load factor α cannot be greater than (B/τ_C^*). Hence, an upper bound[7] on α is

$$U_1 = \frac{B}{\tau_C^*}. \tag{2}$$

2) If node i has t_i transmitters and r_i receivers, then the maximum amount of traffic that can be sourced or sinked at node i is bounded by $t_i \cdot B$ and $r_i \cdot B$, respectively. The amount of traffic sourced from node i is given by $\sum_{j \in V} \Lambda_{ij}$ and the amount of traffic sinked at node i is given by $\sum_{j \in V} \Lambda_{ji}$. Thus

$$U_2 = \min\left(\frac{t_i \cdot B}{\sum_{j \in V} \Lambda_{ij}}, \frac{r_i \cdot B}{\sum_{j \in V} \Lambda_{ji}}\right). \tag{3}$$

3) The following upper bound is used only for the IP restoration technique. Let the degree of node i be denoted by $\deg(i)$. Note that in IP restoration, after a fiber failure, only $\lfloor t_i \cdot (\deg(i) - 1/\deg(i)) \rfloor$ transmitters and only $\lfloor r_i \cdot (\deg(i) - 1/\deg(i)) \rfloor$ receivers are *guaranteed* to be attached to an operational fiber. Thus, in IP restoration, the maximum amount of traffic that can be sourced or sinked at node i after a fiber failure is bounded by $\lfloor t_i \cdot (\deg(i) - 1/\deg(i)) \rfloor \cdot B$ and $\lfloor r_i (\deg(i) - 1/\deg(i)) \rfloor \cdot B$, respectively. Thus

$$U_3 = \min\left(\frac{\left\lfloor t_i \cdot \frac{\deg(i)-1}{\deg(i)} \right\rfloor \cdot B}{\sum_{j \in V} \Lambda_{ij}}, \frac{\left\lfloor r_i \cdot \frac{\deg(i)-1}{\deg(i)} \right\rfloor \cdot B}{\sum_{j \in V} \Lambda_{ji}}\right). \tag{4}$$

Note that $U_3 < U_2$. Thus, based on the above analysis, tighter upper bounds for the load factor for WDM shared-path protection and IP restoration can be computed as follows:

$$U_{\text{WDM}} = \min(U_1, U_2) \tag{5}$$

$$U_{\text{IP}} = \min(U_1, U_3). \tag{6}$$

III. Problem Formulation

A. Notation

We define the notation employed to develop the ILPs and then present the ILPs. We are given the following:

1) the network topology represented as a directed graph G;
2) the traffic matrix, i.e., the amount of traffic flow that is to be routed between node pairs (this matrix will be multiplied by a "load factor" to model the maximum traffic intensity that can be carried by the network under each of the two fault-management techniques);
3) number of transmitters and receivers at the nodes;
4) alternate routing tables at each node.[8]

Given:

N	nodes in the network (numbered 1 through N);
E	unidirectional fiber links in the network (numbered 1 through E);
F	bidirectional fibers in the network (numbered 1 through $F, E = 2 \times F$);
W	maximum number of wavelengths on a link;
Trans_i^w	number of transmitters at node i on wavelength w;
Rec_i^w	number of receivers at node i on wavelength w;
R_{ij}	set of alternate routes for node-pair ij;
$M = \max(\lvert R_{ij} \rvert)$	maximum number of alternate routes between any node-pair ij
R_{ij}^k	set of eligible alternate routes between node pair ij after fiber k fails;
Λ_{sd}	the traffic demand matrix for node pair sd in terms of bits per second;
α	the load factor; the traffic demand matrix can be multiplied by α in order to model the increase in the traffic intensity in the network;

we require the ILPs to solve for the following variables.

w_k	number of wavelengths used by primary lightpaths on link k. These variables are employed only in ILP1 and ILP2. (We remark that there are four ILPs formulated in this—ILP1, ILP2, ILP3, and ILP4—descriptions of which will follow shortly.)
s_k	number of *spare* wavelengths used on link k. These variables are employed only in ILP1 and ILP2.
m_k^w	takes on the value of one if one or more backup lightpaths are using wavelength w on link k; zero otherwise.
V_{ij}	number of primary lightpaths between node-pair ij.
$\gamma_{ij,r}^w$	takes on the value of one if the rth route between node pair ij utilizes wavelength w before any fiber failures; zero otherwise.
$\delta_{ij,p}^{b,w}$	takes on the value of one if a primary on route p between node pair ij is protected by route b between node pair ij by employing wavelength w; zero otherwise. These variables are employed only in ILP1 and ILP2.
λ_{ij}^{sd}	amount of traffic between source s and destination d that flows through the lightpath between node pair ij. These variables are employed only in ILP1 and ILP2.
$\lambda_{ij,r}^{sd}$	amount of traffic between source s and destination d that flows through the lightpath that is routed over the rth route between node pair ij. These variables are employed only in ILP3 and ILP4.

[7]Note that it may be difficult to compute the exact value of this upper bound for large networks. For further details, see [17].

[8]The alternate routing table at node s consists of a collection of k shortest path routes for every (s, d) node pair in the network ($k = 3$ may suffice in most networks [18]). In this paper, we assume that for a given node pair, all the routes in the alternate routing table are edge disjoint.

Γ_k^{sd} amount of traffic between source s and destination d that is disrupted due to the failure of fiber k. These variables are employed only in ILP3 and ILP4.

Ω maximum number of transceivers that are being used for primary lightpaths at any node. These variables are employed only in ILP2 and ILP4.

$X_{ij,r}$ excess capacity on all the lightpaths that are routed over the rth route between node pair ij. These variables are employed only in ILP3 and ILP4.

$\beta_{ij,r}^{sd,k}$ amount of disrupted traffic between source s and destination d that is rerouted through a lightpath that is routed over the rth route between node pair ij. These variables are employed only in ILP3 and ILP4.

S_{ij} number of primary lightpaths between node pair ij in the "seed topology." These variables are employed only in ILP4.

B. WDM Protection: Single ILP Formulation (ILP1)

In this section, we provide a detailed mathematical formulation of the WDM-protection technique. The formulation, which turns out to be an ILP, consists of three parts: the objective function [(7)], constraints for setting up primary and backup lightpaths [(8)–(24)], and constraints for routing packet traffic over the primary lightpaths [(25)–(28)]. Intuitively, the objective function should be "*Maximize* α." But we found that if we use "*Maximize* α" as the objective function, then the ILP solver (*CPLEX* 6.5) takes a very long time to optimally solve the ILP. Hence, we decided to choose an objective function that allowed the ILP solver to quickly find a feasible solution. Now, by solving the ILP for different values of α, we determined the maximum value of α (i.e., the maximum load factor) for which the ILP generated a feasible solution. The ILP formulation is as follows.

Minimize the total capacity used

$$\text{Minimize} \sum_{k=1}^{E} (w_k + s_k). \tag{7}$$

Constraints for Setting Up Lightpaths With Shared-Path Protection: The number of channels on each link is bounded

$$w_k + s_k \leq W \quad 1 \leq k \leq E. \tag{8}$$

The definition of the number of primary lightpaths between a node pair is

$$\sum_{r \in R_{ij}} \sum_{w=1}^{W} \gamma_{ij,r}^{w} = V_{ij} \quad \forall ij. \tag{9}$$

The definition of the number of primary lightpaths traversing a link is

$$w_k = \sum_{ij} \sum_{r \in R_{ij}, k \in r} \sum_{w=1}^{W} \gamma_{ij,r}^{w} \quad 1 \leq k \leq E. \tag{10}$$

The definition of the spare capacity required on link k is

$$s_k = \sum_{w=1}^{W} m_k^w \quad 1 \leq k \leq E. \tag{11}$$

The constraints to indicate whether wavelength w is reserved for some restoration path on link k are

$$m_k^w \leq \sum_{ij} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W \tag{12}$$
$$N(N-1) \times E \times M \times m_k^w \geq \sum_{ij} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W. \tag{13}$$

The constraint to ensure that wavelength w on link j is used either by a primary lightpath or by backup lightpaths is

$$\left(\sum_{ij} \sum_{r \in R_{ij}: k \in r} \gamma_{ij,r}^{w} \right) + m_k^w \leq 1$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W. \tag{14}$$

The constraints to ensure that two backup lightpaths share wavelength w on link k only if the corresponding primary paths are fiber disjoint are

$$\sum_{ij} \sum_{p \in R_{ij}: f \in p} \sum_{b \in R_{ij}: k \in b} \delta_{ij,p}^{b,w} \leq 1$$
$$1 \leq f \leq F, \quad 1 \leq k \leq E, \quad 1 \leq w \leq W. \tag{15}$$

The constraints to indicate whether transmitter t_i^w is being used for a backup lightpath are

$$t_i^w \leq \sum_{j=1}^{N} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W \tag{16}$$
$$N(N-1) \times E \times M \times t_i^w \geq \sum_{j=1}^{N} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W. \tag{17}$$

The constraints to ensure that node i uses at most Trans_i^w transmitters on wavelength w are

$$\left(\sum_{j} \sum_{p \in R_{ij}} \gamma_{ij,p}^{w} \right) + t_i^w \leq \text{Trans}_i^w$$
$$1 \leq i \leq N, \quad 1 \leq w \leq W. \tag{18}$$

The constraints to ensure that two backup lightpaths originating at node i share a transmitter on wavelength w only if the corresponding primary paths are fiber disjoint are

$$\sum_{j=1}^{N} \sum_{p \in R_{ij}: f \in p} \sum_{b \in R_{ij}: b \neq p} \delta_{ij,p}^{b,w} \leq \text{Trans}_i^w$$
$$1 \leq f \leq F, \quad 1 \leq i \leq N, \quad 1 \leq w \leq W. \tag{19}$$

The constraints to indicate whether receiver r_j^w is being used for a backup lightpath are

$$r_j^w \leq \sum_{i=1}^{N} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W \tag{20}$$
$$N(N-1) \times E \times M \times r_j^w \geq \sum_{i=1}^{N} \sum_{p, b \in R_{ij}, k \in b} \delta_{ij,p}^{b,w}$$
$$1 \leq k \leq E, \quad 1 \leq w \leq W. \tag{21}$$

The constraints to ensure that node j uses at most Rec_j^w receivers on wavelength w are

$$\left(\sum_i \sum_{p \in R_{ij}} \gamma_{ij,p}^w\right) + r_j^w \le \text{Rec}_j^w \quad 1 \le j \le N, \quad 1 \le w \le W. \quad (22)$$

The constraints to ensure that two backup lightpaths terminating at node j share a receiver on wavelength w only if the corresponding primary paths are fiber disjoint are

$$\sum_{i=1}^{N} \sum_{p \in R_{ij}: f \in p} \sum_{b \in R_{ij}: b \ne p} \delta_{ij,p}^{b,w} \le \text{Rec}_j^w \quad 1 \le f \le F, \quad 1 \le j \le N, \quad 1 \le w \le W. \quad (23)$$

The constraints to ensure that every primary lightpath is protected by a backup lightpath are

$$\sum_{w=1}^{W} \gamma_{ij,p}^w = \sum_{b \in R_{ij}, b \ne p} \sum_{w=1}^{W} \delta_{ij,p}^{b,w} \quad \forall ij, \forall p \in R_{ij}, \quad 1 \le w \le W. \quad (24)$$

1) Multicommodity Flow Constraints for Routing Traffic on the Virtual Topology[9]*:* The constraints to ensure that the amount of traffic sourced from node s to destination node d is equal to $\alpha \times \Lambda_{sd}$ are

$$\sum_j \lambda_{sj}^{sd} = \alpha \times \Lambda_{sd} \quad \forall sd. \quad (25)$$

The constraints to ensure that the amount of traffic received by node d from node s is equal to $\alpha \times \Lambda_{sd}$ are

$$\sum_i \lambda_{id}^{sd} = \alpha \times \Lambda_{sd} \quad \forall sd. \quad (26)$$

Traffic conservation constraints at the intermediate nodes are

$$\sum_i \lambda_{ik}^{sd} = \sum_j \lambda_{kj}^{sd} \quad \forall sd, \forall k: k \ne s, \quad k \ne d. \quad (27)$$

The constraints to ensure that the total amount of traffic flowing through a lightpath is less than the capacity of the lightpath are

$$\sum_{sd} \lambda_{ij}^{sd} \le V_{ij} \quad \forall ij. \quad (28)$$

C. WDM Protection: Split ILP Formulation (ILP2)

The intuition behind splitting the ILP formulation is to quickly solve two smaller ILPs instead of solving one large ILP (which may take much more time). To do so, we first find a set of "good" primary lightpaths and then set up backup lightpaths for the primary lightpaths.

1) Part I: Find a Set of "Good" Primary Lightpaths: The objective function minimizes the amount of resources (wavelength links in the network and transceivers per node) required to set up the primary lightpaths. The first term in the minimization function is the total number of wavelength links that are utilized for primary lightpaths. The second term corresponds to the number of transceivers used per node for setting up the primary lightpaths. In the absence of the second term, the solution for ILP2 may employ all the transceivers at a node for primary lightpaths and leave no free transmitter for the backup lightpaths. Thus, the second term tries to ensure that each node has some transceivers that can be employed to set up the backup lightpaths

$$\text{Minimize} \sum_{k=1}^{E} w_k + E \times \Omega. \quad (29)$$

The definition of the maximum number of transceivers at any nodes in the network that are being used for primary lightpaths is

$$\sum_j V_{ij} \le \Omega \quad \forall i \quad (30)$$

$$\sum_i V_{ij} \le \Omega \quad \forall j. \quad (31)$$

2) Multicommodity Flow Constraints for Routing Packets on the Virtual Topology: Same as (25)–(28).

3) Part II: Set Up the Backup Lightpaths for the Primary Lightpaths: Same as (7)–(24).

D. IP Restoration: Single ILP Formulation (ILP3)

In this section, we provide a detailed mathematical formulation of the IP restoration technique. The formulation, which turns out to be an ILP, consists of five parts: the objective function [(32)], constraints for setting up primary lightpaths [(33)–(35)]), constraints for routing packet traffic over the primary lightpaths [(36)–(39)]), constraints for computing the disrupted traffic for every fiber failure scenario [(40)], and constraints for rerouting disrupted traffic over the spare capacity [(41)–(44)]. Due to reasons similar to those described in Section III-B, we employ an objective function that allows the ILP solver to quickly find a feasible solution. Thus, by solving the ILP for different values of α, we determined the maximum value of α (i.e., the maximum load factor) for which the ILP generated a feasible solution. The ILP formulation is as follows.

Minimize the average hop distance *before* a fault

$$\sum_{sd} \sum_{ij} \lambda_{ij}^{sd}. \quad (32)$$

The constraints to ensure that node i uses at most Trans_i^w transmitters on wavelength w are

$$\sum_j \sum_{r \in R_{ij}} \gamma_{ij,r}^w \le \text{Trans}_i^w \quad \forall i, \quad 1 \le w \le W. \quad (33)$$

The constraints to ensure that node j uses at most Rec_j^w receivers on wavelength w are

$$\sum_i \sum_{r \in R_{ij}} \gamma_{ij,r}^w \le \text{Rec}_j^w \quad \forall j, \quad 1 \le w \le W. \quad (34)$$

The constraints to ensure that wavelength w on link j is used by at most one lightpath are

$$\sum_{ij} \sum_{r \in R_{ij}, k \in r} \gamma_{ij,r}^w \le 1 \quad 1 \le k \le E, \quad 1 \le w \le W. \quad (35)$$

1) Multicommodity Flow Constraints for Routing Traffic on the Virtual Topology: The constraints to ensure that the amount of traffic sourced from node s to destination node d is equal to $\alpha \times \Lambda_{sd}$ are

$$\sum_j \sum_{r \in R_{sj}} \lambda_{sj,r}^{sd} = \alpha \times \Lambda_{sd} \quad \forall sd. \quad (36)$$

[9]These constraints model the multihop communication shown in Fig. 1(b).

The constraint to ensure that the amount of traffic received by node d from source node s is equal to $\alpha \times \Lambda_{sd}$ is

$$\sum_i \sum_{r \in R_{id}} \lambda_{id,r}^{sd} = \alpha \times \Lambda_{sd} \quad \forall sd. \tag{37}$$

Traffic conservation constraints at intermediate nodes are

$$\sum_i \sum_{r \in R_{il}} \lambda_{il,r}^{sd} = \sum_j \sum_{r \in R_{lj}} \lambda_{lj,r}^{sd} \quad \forall sd, \forall l\colon l \neq s, \quad l \neq d. \tag{38}$$

The definition of spare capacity, with $X_{ij,r}$ equal to the total spare capacity on the lightpaths from node i to node j along route r, is

$$\sum_{sd} \lambda_{ij,r}^{sd} + X_{ij,r} = \sum_{w=1}^{W} \gamma_{ij,r}^{w} \quad \forall ij, \forall r \in R_{ij}. \tag{39}$$

2) After Fault: The definition of disrupted traffic, where Γ_{sd}^{k} is equal to the disrupted traffic from source s to destination d due to the failure of fiber k, is

$$\sum_{ij} \sum_{r \in R_{ij}: k \in r} \lambda_{ij,r}^{sd} = \Gamma_{sd}^{k} \quad \forall sd, \quad 1 \leq k \leq F. \tag{40}$$

3) Multicommodity Flow Constraints for the Disrupted Traffic: The constraints to ensure that the amount of rerouted traffic from node s to node d after the failure of fiber k is equal to the disrupted traffic (Γ_{sd}^{k}) are

$$\sum_j \sum_{r \in R_{sj}: k \notin r} \beta_{sj,r}^{sd,k} = \Gamma_{sd}^{k} \quad \forall sd, \quad 1 \leq k \leq F. \tag{41}$$

The constraints to ensure that the amount of rerouted traffic received at node d from source node s after the failure of fiber k is equal to the disrupted traffic (Γ_{sd}^{k}) are

$$\sum_i \sum_{r \in R_{id}: k \notin r} \beta_{id,r}^{sd,k} = \Gamma_{sd}^{k} \quad \forall sd, \quad 1 \leq k \leq F. \tag{42}$$

Traffic conservation constraints for rerouting the disrupted traffic are

$$\sum_i \sum_{r \in R_{il}: k \notin r} \beta_{il,r}^{sd,k} = \sum_j \sum_{r \in R_{lj}: k \notin r} \beta_{lj,r}^{sd,k} \quad \forall sd, \forall k, \forall l\colon l \neq s, \quad l \neq d. \tag{43}$$

The constraints to ensure that the total amount of disrupted traffic that is rerouted over a lightpath is less than the spare capacity on the lightpath are

$$\sum_{sd} \beta_{ij,r}^{sd,k} \leq X_{ij,r} \quad 1 \leq k \leq F, \quad \forall ij, \forall r \in R_{ij}. \tag{44}$$

E. IP Restoration: Split ILP Formulation (ILP4)

The intuition behind the split ILP formulation is to find a set of lightpaths that form a good "seed" topology, i.e., a set of lightpaths that use few transmitters, receivers, and wavelengths. Next, we add more lightpaths to the "seed" topology, so that, after the fault, there are enough resources available to carry the disrupted traffic.

1) Part I: Find a Good "Seed" Topology: Minimize the amount of resources required to set up the primary lightpaths [same as (29)].

The definition of the number of primary lightpaths between a node pair in the seed topology is

$$\sum_{r \in R_{ij}} \sum_{w=1}^{W} \gamma_{ij,r}^{w} = S_{ij} \quad \forall ij. \tag{45}$$

The definition of the maximum number of transceivers that are being used for primary lightpaths at a node in the network is

$$\sum_j S_{ij} \leq \Omega \quad \forall i \tag{46}$$

$$\sum_i S_{ij} \leq \Omega \quad \forall j. \tag{47}$$

The constraints to ensure that node i uses at most Trans_i^w transmitters on wavelength w are the same as (33).

The constraints to ensure that node j uses at most Rec_j^w receivers on wavelength w are the same as (34).

The constraints to ensure that wavelength w on link j is used by at most one lightpath are the same as (35).

Multicommodity flow constraints for routing traffic on the virtual topology are the same as (36)–(38).

The constraints to ensure that the total amount of traffic flowing through a lightpath is less than the capacity of the lightpath are

$$\sum_{sd} \lambda_{ij,r}^{sd} \leq S_{ij} \quad \forall ij, \forall r \in R_{ij}\colon k \notin r. \tag{48}$$

2) Part II: Solve the Full ILP Formulation by Employing the Seed Topology: We employ the following constraints in addition to all the constraints in the single ILP formulation described in Section III-D.

The constraints to ensure that the seed topology is a subset of the virtual topology are

$$V_{ij} \geq S_{ij} \quad \forall ij. \tag{49}$$

IV. Heuristic Algorithms

A. WDM Protection

The heuristic algorithm is based on the concept of a "branch-exchange." The algorithm starts by constructing an initial virtual topology and iterates between the following two phases. In the first phase, the heuristic attempts to tear down as many lightpaths as possible (i.e., the heuristic attempts to free up as many resources as possible), without increasing the load on the maximally loaded link. The heuristic tears down lightpaths in increasing order of their loads (in other words, the least loaded lightpath is removed first).

In the second phase, the heuristic attempts to decrease the load of the maximally loaded link by setting up as many lightpaths as possible by employing the resources freed up in the first phase. The order in which lightpaths are set up is greedy, i.e., the algorithm chooses the most effective lightpath among all of the possible lightpaths that can be set up.

The heuristic iterates between these two phases until either it finds a stable virtual topology—i.e., the lightpaths that are torn down in the first phase are the same as lightpaths that are set up in the second phase—or a user-specified maximum iteration count is reached. A more detailed version (pseudocode) of the

```
Given: (a) Physical topology, (b) Number of wavelengths, (c) Number of transmitters
          and receivers at the nodes (d) The traffic matrix.
Find: A virtual topology that maximizes the scale-up factor for the traffic matrix.

// Let VT denote the virtual topology. Find some suitable starting topology.
1  Initialize(VT)
   // Route traffic using shortest-path routing with load-sharing (i.e., distribute
   // the traffic on all shortest paths). Find the load of the maximally-loaded-link.
2  MaxLoad = Route_traffic_and_return_MaxLoad(VT)
   // Do ''branch exchanges'' until the topology stabilizes or ''maxcount'' is reached.
3  while (topology_not_stabilized && number_of_iterations < MaxIterations) {
     // Phase I: tear-down lightpaths *without* increasing the value of MaxLoad.
4    LightpathList = Sort_lightpaths_by_MaxLoad(VT)
5    while (LightpathList is not empty) {
       // Tear-down the lightpath with the minimum load.
6      Lightpath = LightpathList.remove_first_item()
7      tear_down_primary_and_backup(Lightpath, VT)
       // Restore the lightpath if the value of MaxLoad has increased.
8      if (Route_Traffic_and_ReturnMaxLoad(VT) > MaxLoad) {
9      restore_primary_and_backup(Lightpath, VT)
       }
       // Otherwise, sort the lightpaths in increasing order of the new load values.
10     else {
11     Sort_lightpaths_by_MaxLoad(VT)
       }
     }
     // Phase II: Try to set up a lightpath between (i,j). Store it in NewLightpathList.
12   for (all node pairs (ij)) {
13     if (set_up_primary_and_backup(ij, VT))
14       MaxLoad = RouteTraffic_and_ReturnMaxLoad(VT)
15       add_to_list(MaxLoad, ij, NewLightpathList)
         // Tear-down the lightpath between node-pair (ij).
16       tear_down_primary_and_backup(ij, VT)
       }
     }
     // Sort lightpaths in increasing order of the MaxLoad values.
17   Sort_list_by_MaxLoad(NewLightpathList)
     // Try to set up as many lightpaths as possible.
18   while (NewLightpathList is not empty) {
19     NewLightpath = NewLightpathList.first_item()
       // Recompute NewLightpathList
20     if (set_up_primary_and_backup(NewLightpath, VT)) {
21       for (all node pairs (ij)) {
22         if (set_up_primary_and_backup(ij, VT)) {
23           MaxLoad = RouteTraffic_and_ReturnMaxLoad(VT)
24           add_to_list(MaxLoad, ij, NewLightpathList)
             // Tear-down the lightpath between node-pair (ij).
25           tear_down_primary_and_backup(ij, VT)
           }
         }
       }
     }
   }
```

Fig. 4. WDM heuristic algorithm.

heuristic algorithm can be found in Fig. 4. An explanation for the pseudocode is given below.

- *Line 1:* Find a suitable virtual topology to start the algorithm. In this study, we started with a virtual topology that is identical to the physical topology.
- *Line 2:* The traffic between a source and destination node is *equally* distributed over multiple shortest paths from the source to the destination. Now, the "bottleneck-lightpaths" in the network are those lightpaths that are carrying the maximum amount of load in the network (we denote the maximum load by *MaxLoad*). Thus, in phase I of the algorithm, the heuristic removes only those lightpaths[10] that do not increase the value of *MaxLoad*.
- *Line 3:* This is the beginning of the main loop of the "branch-exchange" algorithm. The algorithms iterates through lines 4–27 until either it finds a stable virtual topology—i.e., the lightpaths that are torn down in the first phase are the same as lightpaths that are set up in the second phase—or a user-specified maximum iteration count is reached. Lines 4–11 implement phase I and lines 12–27 implement phase II of the "branch-exchange" algorithm.
- *Line 4: LightpathList* contains a sorted list of all the lightpaths in the virtual topology. The lightpaths are sorted in increasing order based on their load. Thus, the lightpath with the minimum load will be the first element in the list.
- *Line 5–11:* After removing the least loaded lightpath, we reroute all the traffic. If the amount of traffic in the "bottleneck-lightpaths" has increased due to rerouting, then we restore the lightpath we just removed. Otherwise, we sort again the lightpaths based on their loads and try to remove another lightpath. This loop terminates when no more lightpaths can be removed from *LightpathList* without increasing the value of *MaxLoad*. This marks the end of phase I (the "lightpath removal" phase) in the two-phase "branch-exchange" algorithm.
- *Line 12–16:* This is the beginning of phase II. In this phase, we set up *one lightpath at a time* in the network by employing the resources that were freed up in phase I of the algorithm. Recall that for every source–destination pair, the algorithm has a list of precomputed edge-disjoint alternate paths. The algorithm chooses the first successful alternate path for routing the primary lightpath. Then, of the remaining alternate lightpaths, the algorithm chooses the first successful path for routing the backup lightpath. Each time we set up a lightpath, we route the traffic and calculate the value of *MaxLoad*. Thus, at the end of this loop, *NewLightpathList* will contain a list of all the lightpaths (and the corresponding values of *MaxLoad*) that can be set up.
- *Line 17:* In this step, we sort all the lightpaths in *NewLightpathList* based on the values of *MaxLoad*. Thus, after sorting, the first element in the list corresponds to a lightpath that, if set up, will result in the lowest value of *MaxLoad*.
- *Line 18–27:* We set up the first lightpath in *NewLightpathList* and reroute the traffic (note that if the lightpath cannot be set up, then we remove the lightpath from *NewLightpathList* and try the next lightpath in the list). Then, we sort the lightpaths in *NewLightpathList* based on the recalculated values of *MaxLoad*. We iterate through these steps (lines 18–27) as long as *NewLightpathList* is nonempty. This marks the end of phase II.

[10]Note that in the remainder of this section, when we say "set up (or tear down) a lightpath," we actually mean "set up (or tear down) a primary lightpath and the corresponding shared backup lightpath."

B. IP Restoration

The IP heuristic is very similar to the WDM heuristic described in the previous section except for the following two main differences: 1) the lightpath-setup routine only needs to set up the primary lightpath and 2) the function

```
Given: (a) Physical topology, (b) Number of wavelengths, (c) Number of transmitters
          and receivers at the nodes, and (d) The traffic matrix.
Find: A virtual topology that maximizes the scale-up factor for the traffic matrix.

// Let VT denote the virtual topology. Find some suitable starting topology.
1  Initialize(VT)
   // Route the traffic using shortest-path routing with load-sharing (i.e., distribute
   // the traffic on all shortest paths). Find the load of the maximally-loaded-link.
2  MaxLoad = RouteTraffic_and_ReturnMaxLoad(VT)
   // Do ''branch exchanges'' until the topology stabilizes or ''maxcount'' is reached.
3  while (topology_not_stabilized && number_of_iterations < MaxIterations) {
     // Phase I: tear-down lighpaths without increasing the value of MaxLoad.
4    LightpathList = Sort_lightpaths_by_MaxLoad(VT)
5    while (LightpathList is not empty) {
       // Tear-down the lightpath with the minimum load.
6      Lightpath = LightpathList.remove_first_item()
7      tear_down_lightpath(Lightpath, VT)
       // Restore the lightpath if the value of MaxLoad has increased.
8      if (RouteTraffic_and_ReturnMaxLoad(VT) > MaxLoad) {
9        restore_lightpath(Lightpath, VT)
       }
       // Otherwise, sort the lightpaths in increasing order of the new load values.
10     else {
11       Sort_lightpaths_by_MaxLoad(VT)
       }
     }
     // Phase II: Set up as many lightpaths as possible. Store them in NewLightpathList.
12   for (all node pairs (ij)) {
13     if (set_up_lightpath(ij, VT) returns success) {
14       MaxLoad = RouteTraffic_and_ReturnMaxLoad(VT)
15       add_to_list(MaxLoad, ij, NewLightpathList)
         // Remove the lightpath between node-pair (ij) that we just set up.
16       tear_down_lightpath(ij, VT)
       }
     }
     // Sort lightpaths in increasing order of the MaxLoad values.
17   Sort_lightpaths_by_MaxLoad(NewLightpathList)
     // Try to set up as many lightpaths as possible.
18   while (NewLightpathList is not empty) {
       // Set up the first lightpath in NewLightpathList. Note that, we do not remove
       // the lightpath from NewLightpathList, because we want the algorithm to be able
       // to add multiple lightpaths between the same source-destination pair.
19     NewLightpath = NewLightpathList.first_item()
20     set_up_lightpath(NewLightpath, VT)
       // Recompute the NewLightpathList.
21     for (all the lightpaths in NewLightpathList) {
22       if (set_up_lightpath(lightpath, VT)) {
23         MaxLoad = RouteTraffic_and_ReturnMaxLoad(VT)
24         change_MaxLoad(MaxLoad, lightpath, NewLightpathList)
           // Tear-down the lightpath between node-pair (ij).
25         tear_down_lightpath(lightpath, VT)
         }
26       else {
           // If the lightpath cannot be set up, then remove it from the list.
27         NewLightpathList.remove_item(lightpath)
         }
       }
     }
   }
```

Fig. 5. IP heuristic algorithm.

RouteTraffic_and_ReturnMaxLoad computes the traffic on the "bottleneck-lightpaths" by finding the maximum value of *MaxLoad* over all fiber-failure scenarios. The pseudocode for the heuristic algorithm is shown in Fig. 5.

V. Recovery-Time Analysis

The time it takes for the network to recover from a fiber failure is indicative of the potential data and revenue loss due to a fiber failure. In this section, we analytically compare the protection-switching time for WDM shared-path protection with the restoration time for IP restoration. In our calculations, we employ "typical" values for the various terms, such as the propagation delay, fault detection time, switch configuration time, etc., which, to the best of our knowledge, are representative of today's networks. But the values for these terms can vary significantly depending on the technology used.

A. WDM Shared-Path Protection

For WDM shared-path protection, we employ the analysis given in [8]. The assumptions are as follows.

1) The fiber failure is detected by the network nodes adjacent to the fiber. We assume that the time to detect a fiber failure is F. In our calculations, we use $F = 100$ μs.
2) The nodes adjacent to the failed fiber send alarm signals over an out-of-band reliable control network.
3) The transmission time for the alarm messages can be neglected in comparison to the propagation delay.
4) Message processing time at a node is denoted by D. For our calculations, we use $D = 100$ μs. The queueing delays of control messages at a node are assumed to be included in the message processing time.
5) Propagation delay on each fiber is denoted by P. For our calculations, we assume that the fiber length is equal to 80 km, which corresponds to a delay of 400 μs.
6) The time to configure and test a cross-connect is C. We use $C = 5$ ms in our calculations.
7) The number of hops from the node adjacent to the failed fiber to the source node of the connection is h_s.
8) The number of hops in the backup route from the source node to the destination node is h_b.

Fig.6(a) illustrates the steps in the recovery process for WDM shared-path protection. Upon detecting a fiber failure, the end-nodes of the failed fiber send alarm messages to the source node and the destination node of the connection. Then, the source node sends a setup message to the destination node along the backup route (which is determined at the time of call setup) and configures the cross-connects at each intermediate node. The destination node, upon receiving the setup message, sends a confirm message back to the source node, thus completing the recovery process. The total time for shared-path protection is given by

$$F + h_s \times P + (h_s + 1) \times D + (h_b + 1) \times C + 2 \times h_b \times P + 2 \times (h_b + 1) \times D. \quad (50)$$

B. IP Restoration

For IP restoration, the assumptions are as follows.

1) The fiber failure is detected by the destination nodes of all the failed lightpaths. Since we assume that the WDM hardware is tightly coupled with the IP layer, hence the time to detect a fiber failure (F) is dominated by the time it takes to service an interrupt, which we assume to be on the order of 10 ms. Thus, we use $F = 10$ ms in our calculations.
2) The destination nodes of all the failed lightpaths broadcast link-state update messages over the network.

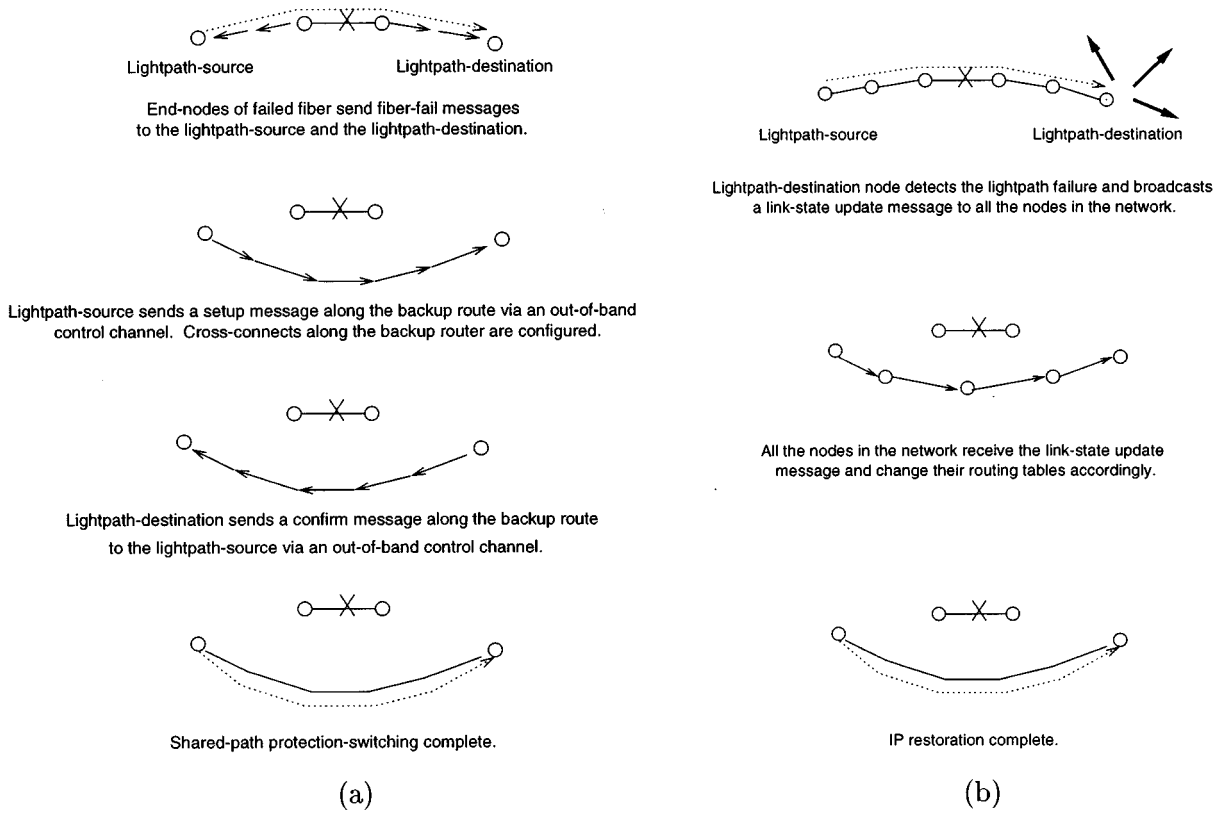

Fig. 6. Steps taken to recover from a fiber failure in (a) WDM shared-path protection and (b) IP restoration.

3) The routing tables in the network stabilize after all the nodes in the network receive all the link-state update messages.
4) The transmission time for the link-state update messages can be neglected in comparison to the propagation delay.
5) The processing time for link-state update messages is dominated by the time it takes to run the broadcast algorithm, i.e., the time it takes to forward the message to the neighboring nodes. We assume that the IP router has dedicated hardware for running the broadcast algorithm. Thus, we use $D = 1$ ms.
6) The propagation delay on a fiber $P = 400\ \mu$s.
7) The time required to recompute the routing table at a node is R. We use $R = 200$ ms in our calculations, which is representative of the time required to recompute the routing tables in an IP router.
8) The number of hops from the failed fiber to the destination node of the failed lightpath is h_d.
9) The number of hops from the destination node of the failed lightpath to the most distant node in the network is n.

Fig. 6(b) illustrates the steps in the recovery process for IP restoration. Upon detecting a lightpath failure, the destination node of the failed lightpath sends a link-state update message to all the nodes in the network. Then, each node updates its routing table after processing the link-state update message. The total time for IP restoration is given by

$$F + h_d \times P + n \times P + (n+1) \times D + R. \qquad (51)$$

VI. Illustrative Numerical Results

We employ the network shown in Fig. 1(b) (which is a small network of interconnected rings typically used in the metro-area telecom environment). The traffic matrix is randomly generated, such that a certain fraction f of the traffic is uniformly distributed over the range [0,1] and the remaining traffic is uniformly distributed over [0,H], where $H(H > 1)$ is the ratio of the average traffic between node pairs with high traffic values and node pairs with low traffic values. All traffic values are normalized to the capacity of a WDM channel, i.e., the capacity of a WDM channel is equal to one. The traffic matrix that was employed for our illustrative examples shown here was generated with parameters $f = 0.8$ and $H = 10$.

Fig. 7 shows the maximum load that was obtained by employing WDM shared-path protection. The number of wavelengths in the network was varied from 4 to 16. Throughout this initial example, we assumed a single transmitter and receiver per wavelength per node (i.e., a single transmitter array and receiver array per node) in the network. The three curves in Fig. 7 correspond to the load values obtained from the theoretical upper bound, the split ILP solution, and the heuristic, respectively.[11] Note that the split ILP solution performs better than the heuristic solution. For the four-wavelength case, the heuristic was unable to find a feasible solution; thus in Fig. 7, the load for four wavelengths is equal to zero.

[11]Although we do not present single ILP formulation results for the network shown in Fig. 1(b) (because the ILP solver takes a very long time to solve), we have solved the single ILP formulation for smaller networks. We found that the load obtained from the split ILP solution was slightly less than that obtained from the single ILP solution.

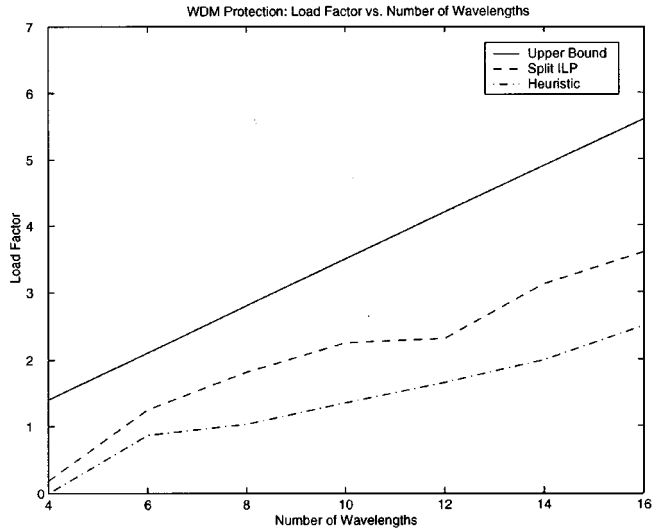

Fig. 7. Maximum guaranteed network capacity (i.e., maximum load factor) versus number of wavelengths for WDM shared-path protection with one transceiver per wavelength per node.

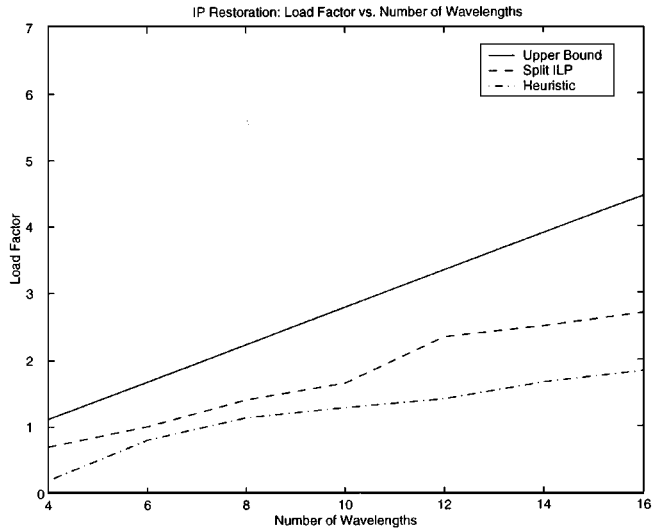

Fig. 8. Maximum guaranteed network capacity versus number of wavelengths for IP restoration with one transceiver per wavelength per node.

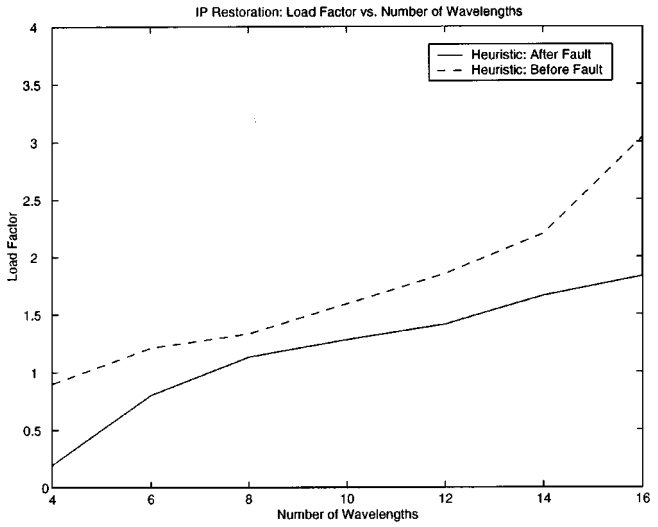

Fig. 9. Load factor versus number of wavelengths for IP restoration before and after a fiber failure. We assume a single transceiver per wavelength per node.

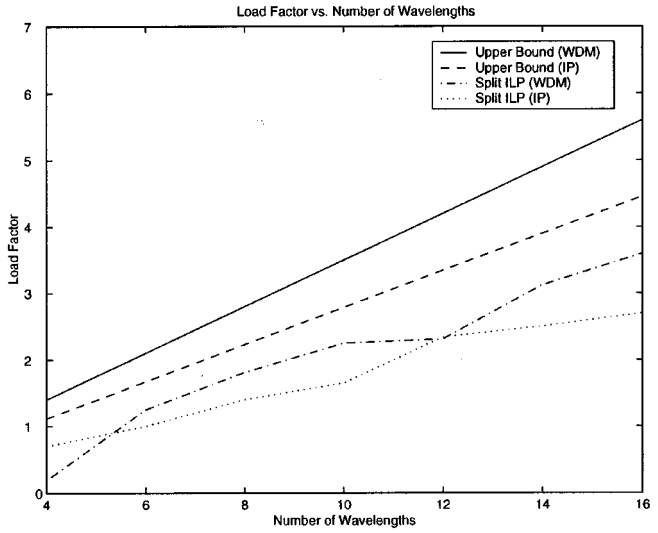

Fig. 10. Maximum guaranteed network capacity versus number of wavelengths for WDM shared-path protection and IP restoration with a single transceiver per wavelength per node.

Fig.8 shows the maximum load that was obtained by employing IP restoration in the network. The number of wavelengths in the network was varied from 4 to 16. We assumed a single transmitter and receiver per wavelength per node in the network. The three curves in Fig. 8 correspond to the load values obtained from the theoretical upper bound, the split ILP solution, and the heuristic, respectively. Again, note that the split ILP solution performs better than the heuristic solution. The two curves in Fig. 9 show the maximum load obtained by the heuristic *before* and *after* a fiber failure. Thus, the difference between the two curves in Fig. 9 is the amount of "extra capacity" in the network that is used for rerouting the disrupted traffic after a fiber failure occurs. Note that this extra capacity may be employed for carrying "nonpremium" traffic that may be dropped in the event of a fiber failure.

Fig. 10 compares the maximum load obtained by employing WDM shared-path protection with that obtained by employing IP restoration. The two straight lines correspond to the load value obtained from the theoretical upper bound for WDM shared-path protection and IP restoration, while the two curves correspond to the load value obtained from the split ILP solution for WDM shared-path protection and split ILP solution for IP restoration. Note that in Fig. 10, WDM shared-path protection outperforms IP restoration for several data points. The intuition behind this phenomenon is that the load for WDM shared-path protection is bounded by the minimum of the two upper bounds U_1 and U_2, while the load for IP restoration is bounded by the minimum of the two upper bounds U_1, U_3. Now, since the upper bound U_3 is always less than U_2, and in this particular example, since the upper bound U_3 is also less than U_1, the upper bound on α for the IP restoration solution is lower than the upper bound for the WDM solution. On the other hand, if we allow multiple transceivers per wavelength per node, then IP restoration performs slightly better than

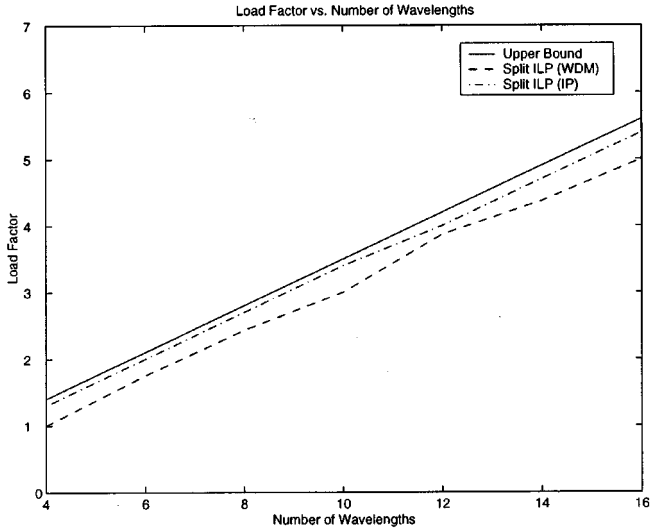

Fig. 11. Maximum guaranteed network capacity versus number of wavelengths for WDM shared-path protection and IP restoration with multiple transceivers per wavelength per node.

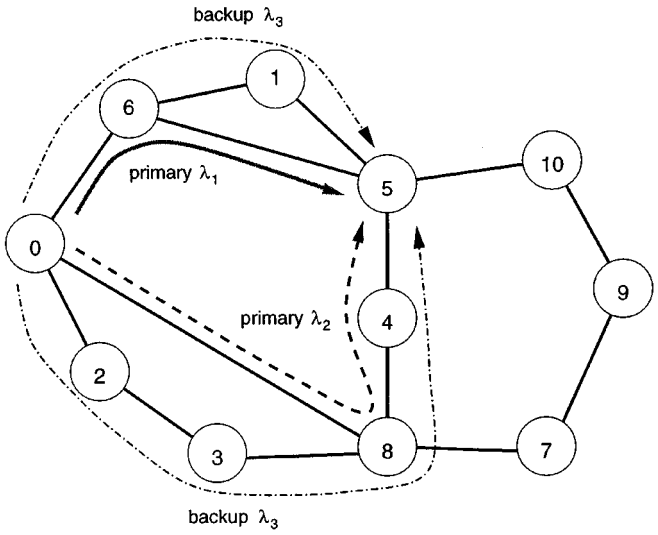

Fig. 12. A scenario in which WDM shared-path protection can generate a feasible solution while IP restoration cannot.

WDM shared-path protection,[12] as shown in Fig. 11. We further explain this phenomenon via the following example.

Consider the network shown in Fig. 12. Let us assume that we have three wavelengths in the network and three transceivers each at nodes 0 and 5. Let us also assume that none of the transceivers at nodes 1, 2, 3, 4, 6, and 8 are free. Also, let us assume that none of the wavelengths on link (8, 7) are free. Now, suppose that we want to route two units of traffic from node 0 to node 5. If we employ WDM shared-path protection, then one possible solution is shown in Fig. 12. The solution consists of two primary lightpaths between node 0 and node 5 along the routes (0, 6, 5) and (0, 8, 4, 5) on wavelengths λ_1 and λ_2, respectively. The two backup lightpaths are routed along (0, 6, 1, 5) and (0, 2, 3, 8, 4, 5) on wavelength λ_3. Note that the backup lightpaths share the transceiver on wavelength λ_3 at node 0 and node 5. Note that no IP solution exists for this scenario. To see why, suppose we set up a third lightpath between nodes 0 and 5 on λ_3. If this lightpath is routed over route (0, 6, 1, 5), then we will not have enough capacity to route two units of traffic when link (0, 6) fails. Similarly, if we route the third lightpath over route (0, 8, 4, 5), then we will not have enough capacity when link (4, 5) fails. Since none of the wavelengths on link (8, 7) are available, we cannot route the third lightpath over route (0, 2, 3, 8, 7, 9, 10, 5). Thus, we note that under certain scenarios, WDM shared-path protection can produce feasible solutions while IP restoration cannot.

[12]Note that in Fig. 11, the gap between the upper bound curve and the split ILP curve is much smaller than the gap between the same two curves in Fig. 10. One plausible reason for the larger gap in Fig. 10 is that it is not possible to find a virtual topology that satisfies the single transceiver constraint, as well as allows a load factor that is close to the upper bound.

TABLE I
THE AVERAGE WDM PROTECTION AND IP RESTORATION TIMES IN MILLISECONDS FOR THE 11-NODE NETWORK SHOWN IN FIG. 1(b) WITH 16 WAVELENGTHS AND MULTIPLE TRANSCEIVERS PER WAVELENGTH PER NODE. TO COMPUTE THE RECOVERY TIMES, WE USED THE COLLECTION OF LIGHTPATHS THAT MAXIMIZES THE LOAD FACTOR α

Failed link	WDM protection	IP restoration
(0, 2)	25.67	220.8
(0, 6)	29.9	218
(0, 8)	25.33	218
(1, 5)	27.27	219.4
(1, 6)	23.6	218
(2, 3)	20.96	216.6
(3, 8)	32.75	220.8
(4, 5)	26.82	216.6
(4, 8)	27.52	220.8
(5, 6)	28.34	218
(5, 10)	33.97	219.4
(7, 8)	34.04	220.8
(7, 9)	30.3	219.4
(9, 10)	29.9	218

Table I shows the average WDM shared-path protection and IP restoration times in milliseconds for the 11-node network shown in Fig. 1(b). We assume that the network has 16 wavelengths and that each node is equipped with multiple transceivers on each wavelength. The recovery times were computed by using the collection of lightpaths that maximize the load factor α. We note that the recovery times for IP restoration are in the 200-ms range and are significantly longer than those for WDM shared-path protection (which are an order of magnitude lower), because for IP restoration, the time to detect a fiber failure and the time to update routing tables are significantly longer than those for WDM shared-path protection. Moreover, in IP restoration, a fiber failure may affect the routing tables of all the nodes in the network, while in WDM shared-path protection, only the nodes along the failed lightpaths and the nodes on the corresponding backup lightpaths are affected.

VII. Conclusion

In this paper, we investigated the maximum guaranteed network capacity and recovery times for two fault-management techniques for IP-over-WDM networks: WDM shared-path protection and IP restoration. We developed mathematical formulations of these fault-management techniques, which turn out to be integer linear programs. We also developed heuristics for both of the techniques. We compared the maximum guaranteed network capacity for the two techniques by plotting the traffic load factor versus the number of wavelengths for a network of interconnected rings typically used in the metro-area telecom environment. From the plots, we observe that for several data points, WDM shared-path protection outperformed IP restoration for our example network, possibly due to the limited number of transceivers per node. We developed analytical formulas for the recovery times for WDM shared-path protection and IP restoration. We found that the recovery times for WDM shared-path protection are much faster than the recovery times for IP restoration. However, in the IP restoration technique, the extra capacity in the network may be employed for carrying "nonpremium" traffic that may be dropped in the event of a fiber failure.

References

[1] B. Mukherjee, *Optical Communication Networks*. New York: McGraw-Hill, 1997.

[2] R. Ramaswami and K. Sivarajan, *Optical Networks: A Practical Perspective*. San Francisco, CA: Morgan Kaufmann, 1998.

[3] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: An approach to high-bandwidth optical WAN's," *IEEE Trans. Commun.*, vol. 40, pp. 1171–1182, July 1992.

[4] "Optical fiber communication conference," presented at the Tutorial Sessions, San Diego, CA, Feb. 1999.

[5] T. Wu, *Fiber Network Service Survivability*. Norwood, MA: Artech House, 1992.

[6] ——, "Emerging technologies for fiber network survivability," *IEEE Commun. Mag.*, pp. 58–74, Feb. 1995.

[7] O. Gerstel, "Opportunities for optical protection and restoration," in *Optical Fiber Communication Conf.*, vol. 2, San Jose, CA, Feb. 1998, pp. 269–270.

[8] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part I—Protection," in *Proc. IEEE INFOCOM'99*, vol. 2, New York, NY, Mar. 1999, pp. 744–751.

[9] A. Fumagalli, I. Cerutti, M. Tacca, and F. Masetti *et al.*, "Survivable networks based on optimal routing and WDM self-healing rings," in *Proc. IEEE INFOCOM'99*, vol. 2, New York, NY, Mar. 1999, pp. 726–733.

[10] G. Sahin and M. Azizoglu, "Optical layer survivability: Single service-class case," in *Proc. OptiComm 2000*, TX, Oct. 2000.

[11] S. Arakawa, M. Murata, and H. Miyahara, "Design methods of multilayer survivability in IP over WDM networks," in *Proc. OptiComm 2000*, TX, Oct. 2000.

[12] O. Gerstel and R. Ramaswami, "Optical layer survivability—An implementation perspective," *IEEE J. Select. Areas Commun.*, vol. 18, pp. 1885–1899, Oct. 2000.

[13] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection cycles in mesh WDM networks," *IEEE J. Select. Areas Commun.*, vol. 18, pp. 1924–1937, Oct. 2000.

[14] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part II—Restoration," in *Proc. IEEE ICC'99*, vol. 3, Vancouver, BC, June 1999, pp. 2023–2030.

[15] W. D. Grover, "The selfhealing network: A fast distributed restoration technique for networks using digital crossconnect machines," in *Proc. IEEE Globecom'87*, 1987, pp. 28.2.1–28.2.6.

[16] J. Anderson, B. T. Doshi, S. Dravida, and P. Harshavardhana, "Fast restoration of ATM networks," *IEEE J. Select. Areas Commun.*, vol. 12, pp. 128–138, Jan. 1994.

[17] K. Zhu, L. Sahasrabuddhe, and B. Mukherjee, "Upgrading and protecting traffic in an optical network by bottleneck-cut identification," in *Optical Fiber Communication Conf.*, vol. 4, Baltimore, MD, Mar. 2000, pp. 87–89.

[18] S. Ramamurthy and B. Mukherjee, "Fixed-alternate routing and wavelength conversion in wavelength routed optical networks," in *Proc., IEEE Globecom'98*, vol. 4, Sydney, NSW, Australia, Nov. 1998, pp. 2295–2302.

Laxman Sahasrabuddhe received the B.Tech. degree from the Indian Institute of Technology, Kanpur, in 1992, the M.Tech. degree from the Indian Institute of Technology, Madras, in 1994, and the Ph.D. degree from the University of California, Davis, in 1999. From 1999 to 2000, he was an Embedded Software Engineer at Amber Networks. Currently, he is a Principal Software Engineer at Summit Networks Inc., San Jose, CA.

Dr. Sahasrabuddhe received the Best Doctoral Dissertation Award, from the College of Engineering, University of California, Davis, for his research on WDM optical networks.

S. Ramamurthy received the B.Tech. degree from the Indian Institute of Technology, Madras, and the M.S. and Ph.D. degrees from the University of California, Davis.

He is a Senior Network Architect at Tellium, Oceanport, NJ, where he works on the design of algorithms and protocols for dynamic provisioning and restoration in optical networks. Prior to joining Tellium, he was a Research Scientist at Telecordia Technologies, where he worked on network control and management of IP/WDM optical networks.

Biswanath Mukherjee received the B.Tech. (Hons.) degree from Indian Institute of Technology, Kharagpur, in 1980 and the Ph.D. degree from University of Washington, Seattle, in 1987.

At Washington, he held a GTE Teaching Fellowship and a General Electric Foundation Fellowship. In 1987, he joined the University of California, Davis, where he has been a Professor of computer science since July 1995 and Chairman of computer science since September 1997. He serves on the editorial boards of *ACM/Baltzer Wireless Information Networks*, *Journal of High-Speed Networks*, *Photonic Network Communications*, and *Optical Network Magazine.* He is the author of *Optical Communication Networks* (New York: McGraw-Hill, 1997), which received the Association of American Publishers, Inc.'s 1997 Honorable Mention in Computer Science. His research interests include lightwave networks, network security, and wireless networks.

Prof. Mukherjee was a Cowinner of paper awards presented at the 1991 and the 1994 National Computer Security Conferences. He serves on the editorial boards of the IEEE/ACM Transactions on Networking and IEEE Network. He also served as Editor-at-Large for optical networking and communications for the IEEE Communications Society. He was the Technical Program Chair of the IEEE INFOCOM'96 Conference.