

Benefits of Link Protection at Connection Granularity

Karthikeyan Sathyamurthy and Srinivasan Ramasubramanian
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ 85721

Phone: (520) 621-4521 **Fax:** (520) 621-8076 **Email:** srini@ece.arizona.edu

Abstract

This paper develops a connection establishment framework for protecting connections against single-link failures using link protection at the granularity of a connection, referred to as Connection Switched Link Protection (CSLP). As a connection is routed only around a failed link, the channel assignment for the connection on the backup path of the failed link must be consistent with that of the primary path. Such a consistency is guaranteed at the time of call admission. The advantages of employing link protection at the connection level is established by comparing its performance through extensive simulations against link protection at the granularity of a fiber, referred to as Fiber Switched Link Protection (FSLP). Link protection at the connection level is shown to significantly outperform that at the granularity of a fiber, specifically when some traffic requires protection while others do not.

Keywords: Optical networks, Traffic grooming, Dynamic routing, Link Protection

1 Introduction

Optical grooming networks employing wavelength division multiplexing (WDM) and wavelength sharing among multiple low-rate traffic streams provides a scalable backbone network architecture. Present day networks have transmission speeds of up to 40 Gb/s (OC-768) with each wavelength shared connections with much lower capacity like 155 Mb/s (OC-3) or 622 Mb/s (OC-12). As the optical processing and buffer technologies are not mature enough to achieve routing individual packets in runtime, optical networks of today and those in the near future are expected to employ connection-oriented services. In such networks, the major network operation is to establish connections between source-destination pairs on-demand and release them when connections are no longer needed.

Connection establishment in a connection-oriented network consists of two steps: *path selection* and *channel assignment*. Path selection refers to selecting a path from source to destination based on certain criteria. Channel assignment refers to assigning one or more channels depending on the requirement of the call on every link of the chosen path. Dynamic connection establishment has been extensively studied in the context of wavelength-routed WDM networks [1 – 8]. However, this issue has received very little attention in the context of WDM grooming networks until recently [9 – 11]. Similarly, survivable routing has also received significant interest in the context of wavelength-routing networks [12], however it is in its early stages of research in the context of grooming networks. In [11], a framework for connection establishment in optical networks employing traffic grooming and heterogeneous switching architectures has been developed. The framework, referred to as Methodology for Information Collection and Routing in Optical Networks (MICRON), outlines a representation mechanism for link information as matrices, approaches to combining link information to obtain path information, and dynamic routing in the presence of a combination of wavelength and time slot switching.

In order to protect connections from link failures in the network, often two paths are assigned: a *primary* path on which a connection is established and *backup* path on which a connection will be setup in case a primary path fails. A combination of links may share resources in a network, a duct or conduit through which they are laid out, which would result in a failure of more than one link at an instant. Such failures are modeled as Shared Risk Link Group (SRLG). Typically, the objective of the network operation is to protect connections against any SRLG failure.

1.1 Taxonomy of protection schemes

Protection schemes proposed thus far in the literature can be classified as Path Protection and Link Protection. Path protection schemes may be classified into two categories based on their knowledge of the link failure. Assignment of a backup path that does not require precise knowledge of the link failure is referred to as *failure-independent path protection* (FIPP). Alternatively, if a connection may be assigned more than one backup path depending on the failure scenario, then it is referred to as *failure-dependent path protection* (FDPP). The protection approaches developed in [13] and [14] are examples of failure dependent path protection strategies.

Link Protection schemes route a connection around a failed link. In case of a failure, the node connected to the failed link routes the connection around the failed link to the neighboring node on the original path. Such a protection may be achieved in the network in a way that is transparent to the source node, except in a scenario where the link that is connected to the source fails.

In order to achieve efficient utilization of network resources, multiplexing of resources across multiple backup paths and/or a primary path may be employed. More than one backup path may share a resource as long as any failure in the network will cause at most one of the corresponding working connections to fail. If a resource is shared only among backup paths, then it is referred to as *backup-backup* multiplexing. If a resource is occupied by a working connection and one or more backup paths, then it is referred to as *primary-backup* multiplexing. Any failure scenario that would require the shared resource for establishing a backup connection must lead to the

failure of the already existing primary connection occupying that resource.

Fiber Switched Link Protection (FSLP). Fiber Switched Link Protection (FSLP) is a type of link protection in which each link has a primary fiber and spare fiber. On any link failure, all the connections flowing through the link on the primary fiber are switched through the spare fiber present in the links along its fixed backup path.

Figure 1 shows an example network. Assume that link 4 is protected by the backup path 3–5–6. On failure of link 4, the switch at node *B* will be reconfigured such that the connections that were outgoing/incoming on link 4 will be switched to/from the spare fiber of link 3. An intermediate node on the backup path, say node *C*, merely switches the entire spare fiber across the two links 3 and 5. As a link may be present on the backup path of more than one link, the switches may be only configured after the failure. For example, link 1 may have its backup path as 2–3. When link 1 fails, the spare fiber of link 3 will be switched to link 2. If the switch at node *C* was pre-configured to switch spare fiber of link 3 to link 5, then it has to be reconfigured after link 1 fails.

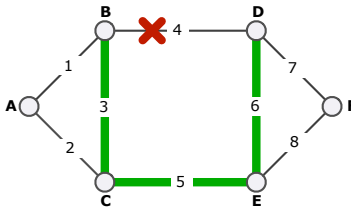


Figure 1. Example network in which link 4 is protected by path 3–5–6.

Figure 2(a) shows the switch architecture and settings at node B when the network is under normal operation without any failures. The input from the primary fiber on every link is fed into the channel switch. The channel switch is responsible for performing wavelength routing, time slot switching, or traffic grooming. When link 4 fails, the connections routed on the primary fiber on link 4 must be re-routed to the secondary fiber on link 3 at node B. The switch settings at node B after link 4 fails is shown in Figure 2(b). The secondary fiber input from node 3 is chosen for drop (at the drop/by-pass selection switch), routed to the input corresponding to link 4 (by the secondary fiber routing switch¹), and selected as the link 4 input (by the primary/secondary fiber selection switch). Similarly, the output from the channel switch (the transit traffic and local traffic) bound for link 4 is switched to the backup fiber on link 3 using switches similar to that at the input stage. It is worth noting that, irrespective of which setting the switch is in, the channel switch gets only one fiber worth of traffic.

FSLP offers fast recovery requiring lesser signaling compared to path protection approaches. However, the drawback of the approach is that the backup paths are established completely along the spare fiber. This leads to the network viewing the connections that may require different levels of Quality-of-Protection (QoP), such as no protection and full protection, in the same manner resulting in a poor performance. Unprotected traffic that is routed along a primary fiber is automatically protected as well. A spare fiber may not be used for routing unprotected traffic as the connections from it are not transferred to the channel switch during normal operation. Irrespective of whether a connection requires protection or not, the connection establishment procedure simply needs to find a path along the primary fiber based on the available resources. The network revenue may be increased by taking advantage of the fact that some unprotected traffic may be dropped on link failure.

Connection Switched Link Protection (CSLP). A logical approach to upgrade the network then is to increase the switching capability at the nodes such that the connections from the primary and spare fibers may be switched

¹The secondary fiber routing switch provides flexibility to change the backup path for a link without manual reconfiguration. Note that, in this example, link 4 is protected by the path 3–5–6. However, it may be changed to 1–2–5–6 if there is a special need.

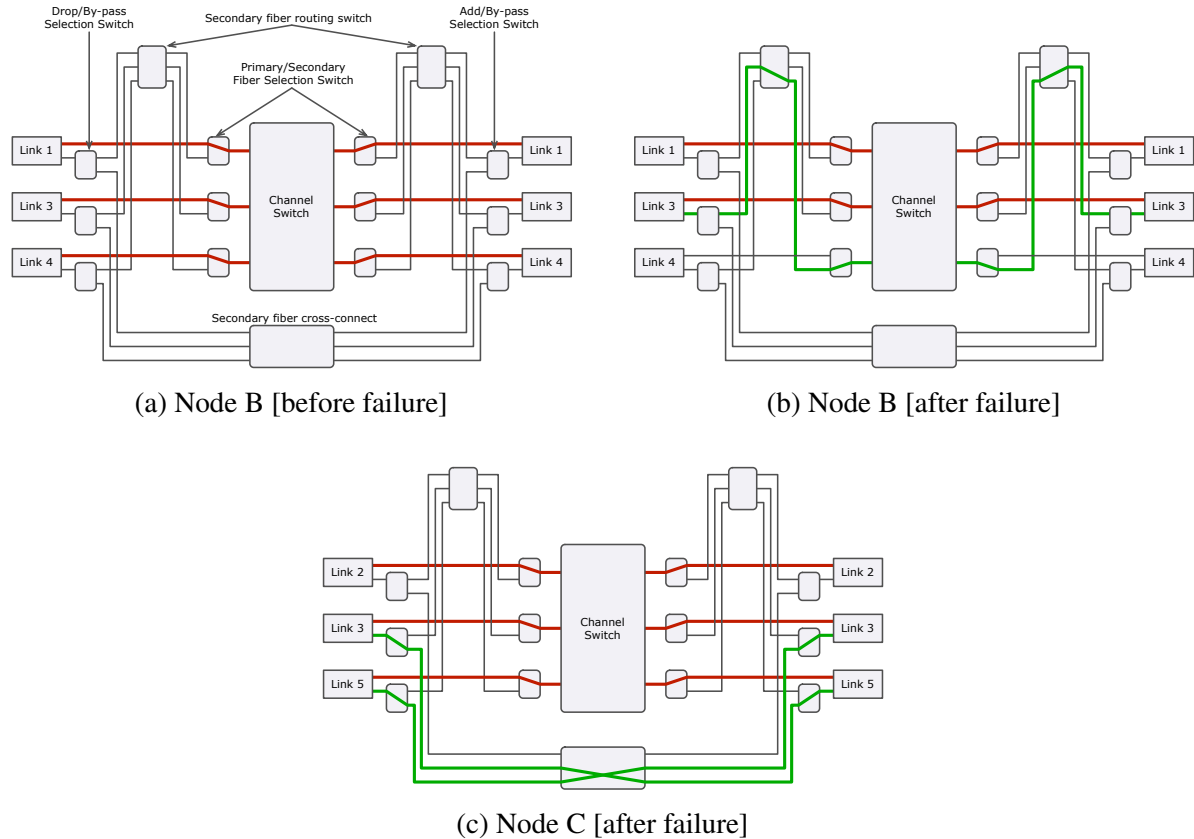


Figure 2. Switch settings at nodes B and C under FSLP approach before and after link 4 failure.

across each other. As both the primary and spare fibers of the networks are now used for normal operation, the onus is now on the connection establishment procedure to ensure that if a connection is routed along a fixed backup path around a failed link, then the channel assignment at the end nodes of a link must be consistent with assignment on the backup path. For example, in the example network considered earlier, assume that a connection from A to F is established along the path 1–4–7. Assume that the connection has been assigned wavelengths W_1 , W_4 , W_7 on links 1, 4, and 7, respectively. When link 4 fails, the connection will be switched along the path 1–3–5–6–7. However, the availability on the backup path must be such that the channel assignments on the non-failed link in the original path must remain the same. If the wavelengths assigned on links 3 and 6 are W_3 and W_6 , respectively, then node B must be able to switch wavelength W_1 on link 1 to W_3 on link 3 and node D must be able to switch wavelength W_6 on link 6 to W_7 on link 7 after link 4 failure. Such a requirement must be satisfied for all link failures in the primary path. Such a link protection strategy is referred to as *Connection Switched Link Protection* (CSLP).

The contribution of this paper is to develop a connection establishment mechanism that considers the channel availability information on the primary and backup paths simultaneously for path selection so that the connections may be protected using link protection. A fixed pre-computed backup is assumed to be known for every link. The connection establishment mechanism employs multiplexing among primary and backup paths to efficiently utilize the network resources. The trade-offs involved in link protection at fiber versus connection levels are studied under mixed traffic scenario involving 50% protected and 50% unprotected traffic and also in a worst-case scenario where all the traffic needs to be protected. The developed link protection strategy at the connection level is based on the MICRON framework for connection establishment [11].

The remainder of the paper is organized as follows: Section 2 explains the assumption on the network model, node architecture, and notations employed. Section 3 describes the MICRON framework and develops the connection establishment methodology with link protection using the framework. The performance of the link protection methodology is evaluated on NSFNET and ARPA-2 networks and compared with FSLP and a failure dependent path protection approach. The performance results are discussed in Section 4. Conclusions are presented in Section 5.

2 Network Model

Consider a WDM grooming network with nodes employing heterogeneous switching architectures. Let \mathcal{N} denote the set of nodes and \mathcal{L} denote the set of physical links in the network. A link $\ell \in \mathcal{L}$ may be either unidirectional or bi-directional in nature. If the bi-directional connectivity between nodes is obtained using dedicated resources for each direction, then it is represented as two unidirectional links. Let Ψ denote the set of Shared Risk Link Groups (SRLG) in the network. An element $\psi \in \Psi$ is a subset of \mathcal{L} that denotes the set of links that may fail due to a failure in one or more shared resources.

Each link is assumed to carry F fibers with W wavelengths per fiber. Each wavelength may be shared by multiple users. Wavelength sharing may be achieved by employing either time or code division multiple access (TDMA or CDMA). The terminology of time slots is employed in this paper, however the techniques developed in this paper are applicable to CDMA systems as well. The access to a wavelength is divided into frames with T time slots per frame. Every slot within a frame is denoted by a 4-tuple, (l, f, w, t) , where $1 \leq l \leq L$, $1 \leq f \leq F$, $1 \leq w \leq W$, and $1 \leq t \leq T$. A *channel* on a link is defined as a collection of a particular time slot across successive frames. Hence, the number of channels in a link is the same as the number of slots in a frame, $F \times W \times T$. Each channel is also represented by a 4-tuple, (l, f, w, t) , similar to the representation of a slot.

2.1 Modeling an optical grooming network

A WDM grooming network with heterogeneous network architecture is modeled as a Trunk Switched Network (TSN) [15]. A TSN is a two-level network model in which every link in the network is viewed as multiple channels.

A node i connected to link ℓ in a TSN groups the channels on the link with similar characteristics into groups called *trunks*. Let K_i denote the number of trunks as viewed by node i and $\chi_{\ell,x}^i$ denote the channels on link ℓ that fall within trunk x . The definition of a trunk at a node depends on the switching resources available at the node. The notion of trunks is illustrated with an example. Consider a WDM grooming network where every link has four fibers, three wavelengths per fiber and two time slots per frame ($F = 4$, $W = 3$, $T = 2$). Figure 3 shows the channels on a link. The shapes of the figures represent the time slots and the shades of the shapes represent wavelengths.

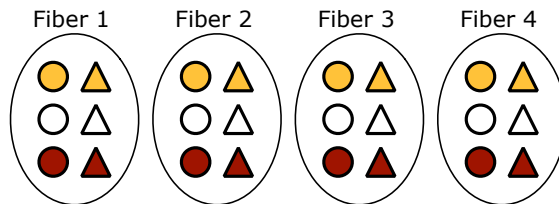


Figure 3. Representation of twenty four channels in a link having four fibers, three wavelengths per fiber, and two time slots per wavelength. Shapes represent time slots, and shades represent wavelengths.

If time slot interchange and wavelength conversion are not permitted, a node views a link as $W \times T$ trunks where each wavelength and time slot combination forms a trunk. Every trunk has F channels as shown in Figure 4(a). If time slot interchange is permitted, but not wavelength conversion, a node views a link as W trunks where each wavelength forms a trunk. Every trunk has $F \times T$ channels as shown in Figure 4(b). A node with such a capability is referred to as a *wavelength-level grooming node*. If full-wavelength conversion is permitted, but not time slot interchange, then each time slot forms a trunk. Every trunk has $F \times W$ channels as shown in Figure 4(c). A node with such a capability is referred to as a *time slot level grooming node*. If both full-wavelength conversion and time slot interchange are permitted, then the entire link is treated as one trunk with $F \times W \times T$ channels, as shown in Figure 4(d). A node with such a capability is referred to as a *full grooming node*.

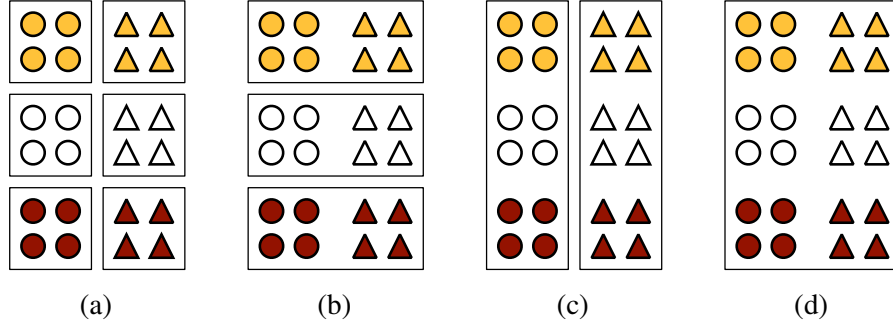


Figure 4. Possible grouping of channels in a link as trunks. (a) Each wavelength and time slot combination forms a trunk; (b) Each wavelength is a trunk; (c) Each time slot is a trunk; and (d) The link is a trunk.

2.2 Node architecture in a TSN

Figure 5 shows the node architecture in a TSN. The node in the figure is assumed to have three links attached to it and views each link as a set of K trunks. The trunks are first de-multiplexed from the link. The trunks from different links are then sent to their respective trunk switches where the channels are switched. We impose trunk-continuity constraint at a node, i.e., a channel in a trunk on a link can be only switched to a channel that falls within the same trunk on another link. Such a restriction stems from an architectural point of view. The complexity of having a switch architecture that would switch the channels across all the links is very high. Therefore, switch design for the near future are likely to be based on simple architectures that would work on a restricted set of channels from every incoming link.

Let Θ_{xy}^ℓ denote the channels on link ℓ , which connects node i and j , that fall within trunk x at node i and trunk y at node j , i.e., $\Theta_{xy}^\ell = \chi_{\ell,x}^i \cap \chi_{\ell,y}^j$. The group of channels that fall within a set Θ_{xy}^ℓ is referred to as a *subtrunk*.

A call arriving in the network require a connection to be established from a source to destination. In addition to the working path, the subtrunk assignment is also done on the backup paths of each link that the primary connection passes through, so that any single SRLG failure can be tolerated. In case of a failure, the calls flowing through the failed link are rerouted along its backup path according to the previously assigned subtrunks. At most one SRLG failure is assumed to be present at any given time.

3 Link Protection using MICRON

This protection strategy developed in this paper employs the Methodology for Information Collection and Routing in Optical Networks (MICRON) framework [11] to collect network information and establish connections. The

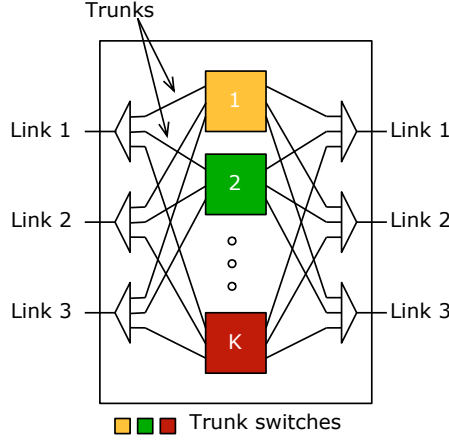


Figure 5. Node architecture in a Trunk Switched Network.

following sub-sections describe in detail the information stored in each link, computation of available capacity for working and backup path establishments for link protection, path selection strategies, and channel establishment.

3.1 Link information

A link ℓ connecting node i to j is represented by one or more matrices, each of which represents a specific information about the link. The matrices of a link that connects node i to j are of dimension $K_i \times K_j$, where K_i and K_j denote the number of trunks at nodes i and j , respectively. An element in row x and column y of the matrix denotes the specific property about the channels that belong to subtrunk Θ_{xy}^ℓ of link ℓ .

Let S_ℓ and P_ℓ be matrices where the elements denote the total number of channels and number of channels occupied by working primary connections, respectively, in each subtrunk. Let G_ℓ^ψ be a matrix where the elements denote the number of channels in a subtrunk that are currently occupied by working connections that would fail in case of the SRLG failure ψ . The channels occupied by the failed primary will become available, therefore, may be used by backup connections. Releasing of capacity occupied by a failed primary has been referred to as “stub-release” in the literature, and has been shown to improve the capacity utilization in the networks. In link protection scheme, as the connection is rerouted along the backup path for the failed link, capacity is not released on the unaffected links traversed by the connection. Let B_ℓ^ψ be a matrix where the elements denote the number of backup channels required in a subtrunk in case of an SRLG failure ψ . Let A_ℓ and A_ℓ^ψ denote the available capacity on link ℓ to when the network has no failures and under failure ψ , respectively. Every link ℓ is assumed to have a backup path for a failure ψ , denoted by \mathcal{Z}_ℓ^ψ . \mathcal{Z}_ℓ^ψ consists of the set of links in the order in which they appear in the path. \mathcal{Z}_ℓ^ψ is obtained by finding a path around the link ℓ after disabling all the links that fail under ψ .

The paper employs a few notations specifically for matrices. The notation $M \leq N$, where $M = [m_{xy}]$ and $N = [n_{xy}]$ are matrices of same dimension, implies for every x and y , $m_{xy} \leq n_{xy}$. Similarly, the notation $N = \max_\psi [M^\psi]$ implies for every x and y , $n_{xy} = \max_\psi [m_{xy}^\psi]$.

When the network does not have any failures, the capacity occupied by the primary connections on a link ℓ is upper bounded by the maximum capacity on the link.

$$P_\ell \leq S_\ell \quad (1)$$

On a failure ψ , the network will be able to re-assign calls to their backup connections if the following condition is

satisfied:

$$P_\ell - G_\ell^\psi + B_\ell^\psi \leq S_\ell \quad (2)$$

Any channel allocation, either for working or backup connection, must not violate the above inequality for any SRLG failure for the network to be resilient to single-link failures. From the above, the capacity available on a link when there are no failures, denoted by A_ℓ is given by:

$$A_\ell = S_\ell - P_\ell \quad (3)$$

Similarly, the available capacity on a link under a failure ψ , denoted by A_ℓ^ψ is given by:

$$A_\ell^\psi = S_\ell - P_\ell - B_\ell^\psi + G_\ell^\psi \quad (4)$$

3.2 Path information

A path in the network, represented as a set of directional links (ordered in the sequence by which it appears in the path), is denoted by \mathcal{P} . The information on a path is obtained by combining the information of the links in the path as:

$$X_{\mathcal{P}} = \prod_{\ell \in \mathcal{P}} X_\ell \quad (5)$$

where \prod denotes generalized matrix multiplication. Note that the direction of the link is evident from the path. If X , Y , and Z are three matrices and $Z = XY$, then an element z_{ij} of the matrix Z is obtained as:

$$z_{ij} = (x_{i1} \otimes y_{1j}) \oplus (x_{i2} \otimes y_{2j}) \oplus \dots \oplus (x_{iC} \otimes y_{Cj}) \quad (6)$$

where C denotes the number of columns of matrix X , or equivalently number of rows of matrix Y .

The operators \otimes and \oplus , denoted as a tuple (\otimes, \oplus) , can be defined in different combinations so that several meaningful results are obtained. It can be observed that when \otimes is integer multiplication and \oplus is integer addition operation, the above equation denotes the traditional matrix multiplication. Some examples of matrix representation of optical grooming networks may be found in [11]. When combining available capacity in particular, the operator tuple (\otimes, \oplus) is set as (min, max).

3.3 Available capacity for routing primary and backup connections

In order to assign a channel on a subtrunk on link ℓ to overcome a failure ψ , it is sufficient that the link occupancy satisfies Equation 2 only for failure ψ . The capacity available on the backup path of a link ℓ when the link fails under failure ψ is computed as:

$$R_\ell^\psi = \prod_{\ell' \in \mathcal{Z}_\ell^\psi} A_{\ell'}^\psi \quad (7)$$

It is worth noting that the above assignment only takes into account those connections that would be re-assigned only in case of failure ψ . Hence, backup multiplexing is inherent to the above computation for available capacity. An element in row x and column y of R_ℓ^ψ indicates if the backup path can be established along that path starting in trunk x and ending in trunk y .

A working connection may be assigned a channel on subtrunk Θ_{xy}^ℓ on link ℓ if the channel occupancy after the assignment still obeys Equation 3. The available capacity for primary path may be computed as A_ℓ . However, such a computation may force the connection to be reconfigured even if its primary path does not fail as the capacity is not guaranteed to exist under a failure. If the connection must not be reconfigured if a link in its primary path does

not fail, then Equation 2 must be satisfied for all failure scenarios in Ψ in addition to satisfying Equation 3. In case of CSLP, while assigning the primary capacity on a link ℓ , apart from ensuring the availability of backup capacity on the backup path for the link, subtrunk assignment consistency must also be ensured, i.e., the trunk assignment should start and end along the backup path similar to the trunk assignment on the link ℓ . The available capacity on link ℓ to route a primary connection, denoted by X_ℓ , is computed as:

$$X_\ell = \min \left(A_\ell, \min_{\psi \in \Psi} A_\ell^\psi, \min_{\psi \in \Psi} R_\ell^\psi \right) \quad (8)$$

A non-zero element in (x_ℓ, y_ℓ) in the above computed availability matrix A_ℓ implies that there is a possible channel assignment on link ℓ and also a channel assignment on the backup path which starts at the trunk x_ℓ and ends at trunk y_ℓ . Such an assignment would guarantee 100% resiliency to an SRLG failure.

As every node in the network is assumed to employ a full-permutation switching for each trunk, the channels within a trunk at a node are indistinguishable. Equivalently, the channels within a subtrunk of a link are also indistinguishable. Therefore, the available capacity matrix may be reduced by treating it as a binary matrix. Equivalently, the non-zero elements of the matrix as obtained in the above equations are replaced with 1. Such a binary matrix representation is employed in this paper.

3.4 Path selection and subtrunk assignment

The path information matrix is used to select a suitable path from a given source-destination pair. In this paper, Extended Dijkstra's shortest path algorithm is employed that uses path availability matrix and hop length. Based on the earlier study [16], shortest path among the set of available paths, referred to as Available Shortest Path (ASP), is observed to be an efficient path selection algorithm as it attempts to use less resources in the network. Hence, ASP is adopted for selecting the working path.

Once a path is selected, the subtrunk assignment for the connection may be done in several ways [11]. In this paper, first-fit subtrunk assignment is employed for working and backup paths. The subtrunk assignment on the working path is computed first, followed by the backup paths such that the subtrunk assignment consistency is satisfied.

3.5 Connection establishment and release

The network is assumed to be managed through a centralized system, or equivalently the network employs link state protocol with every node in the network having up-to-date network state information. While this assumption is employed to understand the working of the proposed connection establishment approach, the proposed approach is amenable to distributed implementation as well. The connections once established may not be reconfigured during the life time of the connection with the exception of the occurrence of an SRLG failure that affects the primary path of the connection.

On arrival of a request \mathcal{R} , the request is first assigned a primary path and then a backup path. The steps involved in the connection establishment process are described in Figure 6. When a connection is terminated, the link capacities must be released. Step 5 of the connection establishment strategy is employed for this purpose, however, instead of adding the request capacity to the matrices, they are subtracted.

3.6 Loop formation

Link protection strategy, either at fiber or connection level, suffers from loop formation that could potentially utilize more resources. An example of loop formation under CSLP is illustrated. Figure7 depicts a scenario where a connection may traverse the same link (in the same direction) twice when a link fails. Link 2 has the

-
1. Update the available capacity matrix on every link for primary path assignment as shown in Equation (8). The non-zero entries are replaced by 1 to achieve binary-valued matrix elements.
 2. Obtain a path employing Extended Dijkstra's Shortest Path algorithm and a subtrunk assignment on the path. If a path or subtrunk assignment cannot be obtained the request is rejected. Go to Step 6.
 3. The request has a specific primary path and a subtrunk assignment on the primary path. Let $\mathcal{P}_{\mathcal{R}}$ denote the links through which the connection is routed and let (x_{ℓ}, y_{ℓ}) denote the subtrunk assignment on link $\ell \in \mathcal{P}_{\mathcal{R}}$. Compute the set of SRLG failures that will affect the connection established on this path. Let $\Psi_{\mathcal{R}}$ denote such an SRLG set.
 4. For calls that require protection, obtain a backup path for every $\psi \in \Psi_{\mathcal{R}}$. For calls that do not require protection, no backup paths are assigned.
 - (a) For every link $\ell \in (\mathcal{P}_{\mathcal{R}} \cap \psi)$,
 - i. Update the available capacity matrix on the links of its backup path corresponding to SRLG failure ψ as shown in Equation 4. The non-zero entries are replaced by 1.
 - ii. Compute the subtrunk assignment on the path $\mathcal{Z}_{\ell}^{\psi}$ such that the assignment starts at trunk x_{ℓ} and ends at trunk y_{ℓ} . If the subtrunk assignment cannot be obtained, the request is rejected. (The connection may be rejected due to loop formation, where a connection may traverse the same link in the same direction twice. The channel assignment may not be performed when only one channel is available on that link. Under such cases, the call is rejected.) Go to Step 6.
 - iii. Compute the backup path $\mathcal{P}_{\mathcal{R}}^{\psi}$ and its subtrunk assignment by replacing every failed link $\ell \in (\mathcal{P}_{\mathcal{R}} \cap \psi)$ with $\mathcal{Z}_{\ell}^{\psi}$ and its subtrunk assignment. Let $\mathcal{P}_{\mathcal{R}}^{\psi}$ denote the links through which the backup path for failure ψ passes through and let $(x_{\ell}, y_{\ell})^{\psi}$ denote the subtrunk assignment on link $\ell \in \mathcal{P}_{\mathcal{R}}^{\psi}$.
 5. Update link capacities. Note that at this juncture, the request has been assigned a primary path and backup paths for all the failures that will affect the primary path. The subtrunk assignments are also obtained on primary and backup paths.
 - (a) Update the capacity used by the primary connections on the corresponding subtrunks on all the links. This operation adds the capacity of the request to the element (x_{ℓ}, y_{ℓ}) of matrix P_{ℓ} for every link $\ell \in \mathcal{P}_{\mathcal{R}}$.
 - (b) Update the capacity gain that would be achieved for all the SRLG failures that would result in the failure of this connection. This operation adds the capacity of the request to the element (x_{ℓ}, y_{ℓ}) of the matrix G_{ℓ}^{ψ} for every link $\ell \in \mathcal{P}_{\mathcal{R}}$ and every SRLG failure $\psi \in \Psi_{\mathcal{R}}$.
 - (c) For calls requiring protection, update the backup capacity required to re-route the connection in case of an SRLG failure. This operation adds the capacity of the request to element $(x_{\ell}, y_{\ell})^{\psi}$ of matrix B_{ℓ}^{ψ} for every link $\ell \in \mathcal{P}_{\mathcal{R}}^{\psi}$ and every $\psi \in \Psi_{\mathcal{R}}$. This step is skipped for calls that do not require protection.
 6. Exit.
-

Figure 6. Steps involved in connection establishment.

path 6–11–12–7 as its backup [Figure7(a)]. A connection established along the primary path 1–2–3–8–12–13 [Figure7(b)] is reconfigured along the path 1–6–11–12–7–3–8–12–13 upon failure of link 2 [Figure7(c)]. Note that the reconfigured connection traverses link 12 in the same direction twice. If sufficient capacity is available, then the connection after reconfiguration under failure of link 2 will occupy two channels on link 12.

There could be an exceptional situation at times to this capacity availability. Note that if link 12 had only one free channel, it will be assumed to be available under the failure of link 2, however, the same channel is used by the primary connection. Under such scenarios, either the connection can be rejected or the backup path can be *trimmed* as 1–6–11–12–13 [Fig. 7(d)], where node I will switch this connection from link 12 to 13. The trimmed path is guaranteed to satisfy the constraint that node I can switch the connection from link 12 to 13 directly still obeying the original channel assignment on link 13. We observed through simulations that such scenarios are very rare. Similar situations may also occur where the backup path may pass through the same (undirected) link in opposite directions.



(a) Link 2 protected by backup path 6–11–12–7. (b) Primary path of a connection along 1–2–3–8–12–13.



(c) Connection after failure of link 2 routed along 1–6–11–12–7–3–8–12–13.

(d) Backup connection after *trimming*.

Figure 7. Example indicating a connection may traverse the same link in the same directional twice under link protection under dynamic primary path computation.

4 Performance Evaluation

The performance of the link protection methodology developed in this paper is evaluated on the NSFNET and ARPA-2 networks. The topology of the networks are shown in Figure 8. The NSFNET network consists of 14 nodes and 22 links. The ARPA-2 network consists of 21 nodes and 26 links. Every link in the network employs four unidirectional fibers (two fiber along each direction), each consisting of sixteen wavelengths and four time slots per wavelength, making it 64 channels per fiber. Thus, a total of 128 channels constitute a link. It has to be noted that two unidirectional fibers are used as spare fibers in FSLP scheme, hence 64 channels constitute a link in this case. This paper considers a network architecture in which all the nodes are wavelength-level grooming nodes. A single link failure scenario in the network is modeled as SRLG failures in which each SRLG group has exactly one link (up to four fibers). On an SRLG failure, the fibers in both directions are assumed to fail. The network can have at most one SRLG failure at any given instant.

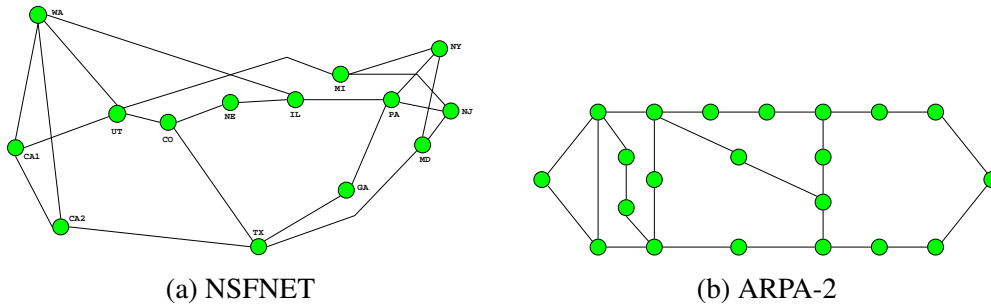


Figure 8. Network topologies considered for performance evaluation.

Requests arrive at the nodes according to Poisson process with rate λ and have an exponential holding time with unit mean. Every request has one channel capacity requirement. The source and destination of a request is assumed to be equally likely among all node pair combinations. Given a non-uniform traffic, it is often difficult to quantify if a certain observation in the network is the effect of the given protection methodology or non-uniform

traffic. Every connection requires protection with a probability p . In this paper, the network performance under two scenarios are studied: (1) $p = 1.0$, where all the connections in the network require protection against a link failure; and (2) $p = 0.5$, where only an average of half the connections require protection against any single-link failure and the other 50% of connections require no protection.

The networks employ available shortest path (ASP) with first-fit wavelength assignment for all the considered protection methodologies. The available shortest path algorithm computes the shortest path among those paths that have sufficient resources for connection establishment.

The performance of CSLP strategy developed in this paper is compared with FSLP and a failure dependent path protection scheme developed in [14], referred to as FDP. The FDP scheme assigns multiple backup paths for a connection, one for each failure scenario under which the primary path of the connection may fail. The FDP scheme also ensures that a connection need not be reconfigured if a link failure does not affect the primary path of a connection. It is worth noting that if a connection establishment strategy attempts to optimize the utilization in the network, then connections may be reconfigured even if their primary paths are not affected. One such approach is studied in [13].

Figure 9 shows the blocking probability of connections under CSLP, FSLP, and FDP approaches for $p = 1.0$ and $p = 0.5$. When $p = 1.0$, there is almost the same blocking probability between CSLP and FSLP. This indicates that the link protection scheme is inherently worse because of the additional resource requirement, hence the avenues for improving performance is slim despite doubling the capacity that is being switched. But when $p = 0.5$, CSLP performs significantly better than FSLP, as expected. Under both the scenarios, the FDP scheme performs the best because it employs path protection. The comparison with the FDP scheme is shown here to indicate the performance that could be achieved if the connections do not have stringent requirement on the recovery time, thereby are protected using path protection strategy.

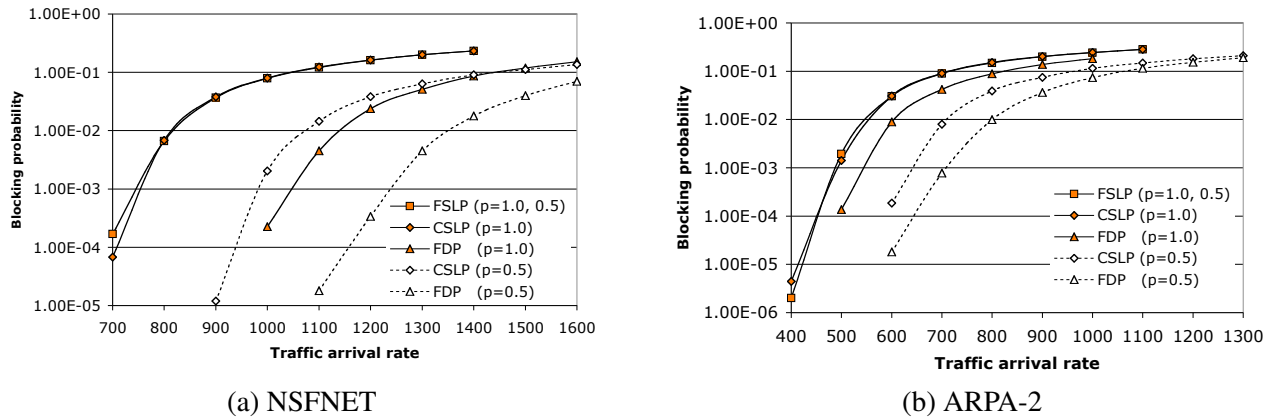


Figure 9. Blocking probability in the NSFNET and ARPA-2 networks.

The performance difference is more prominent in the case of NSFNET network than in ARPA-2 network. The NSFNET network has better connectivity than the ARPA-2 network, hence the path length distribution for a NSFNET network is more uniform than that of ARPA-2 network. In other words, the difference in path lengths between the first and the second shortest path between any two node-pairs in NSFNET network is less as compared to that in ARPA-2 network. As the path length increases, the resources required in the network to accommodate the connection increases, thereby reducing the possibilities for improvement. Such a behavior is also observed in both the networks as the arrival rate of connection increases, where the difference in blocking probability decreases with increasing network load. Path protection schemes, in general, are more efficient than link protection schemes, the difference in performance is highly a factor of the network topology (average path length, link correlation, etc.).

The resources utilized in the network is computed through *effective network utilization* [16]. A request \mathcal{R} for

capacity $C_{\mathcal{R}}$ that is routed along a path with a hop length of H utilizes $C_{\mathcal{R}} \times H$ capacity in the network. However, its effective utilization is only $C_{\mathcal{R}} \times H_s$, where H_s is the shortest path length between the source and destination of the connection. The effective network utilization at any given instant of time is then computed as the sum of the effective utilization of all requests running in the network at that time normalized to the total network capacity, $L \times F \times W \times T$. It is to be noted that the effective utilization is computed over only the accepted requests, while the offered load is computed over all the requests.

Tables 1 and 2 show the effective network utilization for NSFNET and ARPA-2 networks, respectively. It is observed that CSLP offers almost no improvement over FSLP under 100% protection requirement. However, under a mixed traffic scenario an improvement of 24.66% for NSFNET network is observed over FSLP at an arrival rate of 1400. For ARPA-2 network, an improvement of 30.06% for CSLP over FSLP. Under similar situations for the two networks, the improvement in utilization for FDP scheme are 36.73% and 36.71% over FSLP for NSFNET and ARPA-2 networks, respectively. Network utilization difference under high blocking scenarios do not give meaningful results, therefore, network loads that have a blocking probability values of 20% or less are only considered.

Table 1. Effective network utilization in the NSFNET network.

Arrival Rate	Offered Load	FSLP	$p = 1.0$		$p = 0.5$	
			CSLP	FDP	CSLP	FDP
700	0.261	0.261	0.261	–	–	–
800	0.298	0.296	0.296	–	–	–
900	0.335	0.320	0.320	–	0.335	0.335
1000	0.373	0.336	0.336	0.372	0.372	0.373
1100	0.410	0.349	0.348	0.407	0.403	0.410
1200	0.448	0.358	0.358	0.435	0.426	0.447
1300	0.484	0.365	0.365	0.454	0.447	0.482
1400	0.523	0.373	0.372	0.467	0.465	0.510
1500	0.559	–	–	0.478	0.483	0.532
1600	0.596	–	–	0.487	0.512	0.545

Table 2. Effective network utilization in the ARPA-2 network.

Arrival Rate	Offered Load	FSLP	$p = 1.0$		$p = 0.5$	
			CSLP	FDP	CSLP	FDP
400	0.205	0.205	0.205	–	–	–
500	0.257	0.256	0.256	0.256	–	–
600	0.308	0.294	0.294	0.304	0.308	0.308
700	0.359	0.313	0.314	0.338	0.355	0.359
800	0.411	0.325	0.324	0.360	0.389	0.405
900	0.462	0.333	0.333	0.374	0.414	0.439
1000	0.513	0.342	0.340	0.387	0.432	0.459
1100	0.564	0.346	0.347	–	0.450	0.473
1200	0.616	–	–	–	0.465	0.484
1300	0.668	–	–	–	0.481	0.492

Tables 3 and 4 show the length of the primary path of the accepted connections. This metric shows an increasing trend at first and then decreases. The reason for such a trend is that as the load is increased, the available shortest path attempts to find paths that are longer than the shortest path between node pairs. However, beyond a certain threshold, the requests are blocked. The blocking probability of a request increases with increase in the shortest path length between the source and destination, hence reduces the average primary path length of accepted connections. The reason for such a behavior is due to the ASP routing algorithm. The average path length is also an

indicator of the number of failure scenarios under which a connection will be reconfigured to its backup path.

Table 3. Average primary path length in the NSFNET network.

Arrival Rate	FSLP	$p = 1.0$		$p = 0.5$	
		CSLP	FDP	CSLP	FDP
700	2.12	2.10	–	–	–
800	2.19	2.14	–	–	–
900	2.27	2.19	–	2.10	2.10
1000	2.29	2.21	2.12	2.12	2.10
1100	2.29	2.21	2.19	2.15	2.10
1200	2.27	2.20	2.27	2.17	2.13
1300	2.24	2.19	2.30	2.18	2.18
1400	2.21	2.16	2.33	2.18	2.25
1500	–	–	2.32	2.17	2.29
1600	–	–	2.31	2.17	2.31

Table 4. Average primary path length in the ARPA-2 network.

Arrival Rate	FSLP	$p = 1.0$		$p = 0.5$	
		CSLP	FDP	CSLP	FDP
400	3.42	3.42	–	–	–
500	3.46	3.43	3.42	–	–
600	3.55	3.48	3.42	3.42	3.42
700	3.52	3.44	3.45	3.45	3.42
800	3.44	3.37	3.47	3.47	3.47
900	3.36	3.28	3.45	3.44	3.52
1000	3.27	3.20	3.41	3.40	3.51
1100	3.19	3.13	–	3.36	3.49
1200	–	–	–	3.33	3.45
1300	–	–	–	3.30	3.40

Finally, the average shortest-path length of the requests that are accepted in the network is evaluated. Under very low loads, when requests are not rejected, the value of this metric denotes the average shortest path length of all source-destination pairs. With increase in traffic, requests that have to be routed along a longer path experience more blocking as compared to those that require a shorter path. Hence, this metric decreases with increase in offered load. The flatter this metric remains with increasing load, the fairer the routing algorithm is. Tables 5 and 6 show the average shortest path length of the accepted requests. For FSLP and LP, the metric is almost same when $p = 1.0$, but under the mixed traffic scenario, there is more than 10% improvement in fairness at the arrival rate of 1400 requests per second. Also, FDP outperforms LP by 10% when $p = 1.0$ and by less than 2% when $p = 0.5$, at the same arrival rate.

The results presented in this paper indicate that CSLP significantly outperforms FSLP, specifically under mixed traffic scenario. However, even under a 100% protection requirement scenario, FDP performs significantly better than link protection strategies. A trade-off between the speed of restoration and utilization may be achieved if a connection establishment framework can allow for multiple types of protection strategies to be employed in the network at the same time. For example, some traffic that may not have stringent requirements on recovery time may be protected using FDP approach, some that have reasonable recovery time requirements may be protected using failure independent path protection approach (by providing link-disjoint paths, thereby avoiding the need for locating the failed link), and the ones that have stringent recovery time requirements may alone be protected using link protection.

Table 5. Average shortest path length of accepted requests in the NSFNET network.

Arrival Rate	FSLP	$p = 1.0$		$p = 0.5$	
		CSLP	FDP	CSLP	FDP
700	2.10	2.10	–	–	–
800	2.09	2.10	–	–	–
900	2.08	2.08	–	2.10	2.10
1000	2.06	2.06	2.10	2.10	2.10
1100	2.03	2.03	2.10	2.09	2.10
1200	2.01	2.01	2.09	2.08	2.10
1300	1.98	1.98	2.07	2.07	2.01
1400	1.96	1.95	2.06	2.05	2.09
1500	–	–	2.04	2.04	2.08
1600	–	–	2.02	2.03	2.06

Table 6. Average shortest path length for accepted requests in the ARPA-2 network.

Arrival Rate	FSLP	$p = 1.0$		$p = 0.5$	
		CSLP	FDP	CSLP	FDP
400	3.42	3.42	–	–	–
500	3.41	3.41	3.42	–	–
600	3.36	3.37	3.40	3.41	3.42
700	3.28	3.27	3.35	3.41	3.42
800	3.17	3.17	3.29	3.36	3.40
900	3.08	3.08	3.21	3.31	3.37
1000	3.00	3.00	3.14	3.25	3.30
1100	2.92	2.93	–	3.20	3.23
1200	–	–	–	3.15	3.17
1300	–	–	–	3.11	3.11

5 Conclusion

In this paper, a connection establishment approach has been developed that considers the availability of resources on primary and backup paths simultaneously for path selection in order to ensure that the connections can be resilient to a link failure using link protection. The performance of the connection switched link protection (CSLP) is shown to not offer any improvement in performance over fiber switched link protection (FSLP) when all the traffic in the network require protection, thus establishing the inherent deficiency in link protection schemes. Under a mixed traffic scenario, where 50% of the connections require protection, CSLP is shown to perform significantly better than FSLP scheme. In addition, the performance of CSLP and FSLP schemes are compared against a failure dependent path protection (FDP) strategy. FDP is shown to offer the best performance, however has the drawback of an increased recovery time. The connection establishment framework developed for CSLP and FDP may be combined to achieve a framework that would allow multiple protection strategies to be employed in a network.

Acknowledgments

The research presented in this paper is supported in part by National Science Foundation under grant ANI-0325979. Thanks to Prof. Nathan Goodman of the ECE department at University of Arizona for allowing us to use his computing facilities, which greatly reduced the time needed to generate the results presented in this paper.

References

- [1] J. Jue and G. Xiao, "An adaptive routing algorithm for wavelength-routed optical networks with a distributed control scheme," in *Proceedings of the Ninth International Conference on Computer Communications and Networks*, Las Vegas, Nevada, USA, October 2000, pp. 192–197.
- [2] H. Zang, L. Shasrabuddhe, J. P. Jue, S. Ramamurthy, and B. Mukherjee, "Connection management for wavelength-routed WDM networks," in *Global Telecommunications Conference, GLOBECOM'99*, Rio de Janeiro, Brazil, 1999, vol. 2, pp. 1428–1432.
- [3] A. Mokhtar and M. Azizoglu, "Adaptive wavelength routing all-optical networks," *IEEE Transactions on Networking*, vol. 6, no. 2, pp. 197–206, April 1998.
- [4] H. Zang, J. Jue, L. Shasrabuddhe, R. Ramamurthy, and B. Mukherjee, "Dynamic lightpath establishment in wavelength-routed WDM networks," *IEEE Communications*, vol. 39, no. 9, pp. 100–108, September 2001.
- [5] S. Ramamurthy and B. Mukherjee, "Fixed alternate routing and wavelength conversion in wavelength-routed optical networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, pp. 351–367, June 2002.
- [6] E. D. Lowe and D. K. Hunter, "Performance of dynamic path optical networks," *IEE-Proceedings of Optoelectronics*, vol. 144, no. 4, pp. 235–239, August 1997.
- [7] L. Li and A. K. Somani, "Dynamic wavelength routing using congestion and neighborhood information," *IEEE Transactions on Networking*, vol. 7, no. 5, pp. 779–786, October 1999.
- [8] X. Zhang and C. Qiao, "Wavelength assignment for dynamic traffic in multi-fiber WDM networks," in *7th International Conference on Computer Communication and Networks*, Lafayette, LA, USA, 1998, pp. 479–485.
- [9] B. Wen and K. M. Sivalingam, "Routing, wavelength and time-slot assignment in time division multiplexed wavelength-routed optical WDM networks," in *Proceedings of IEEE INFOCOM*, New York, NY, USA, June 2002, vol. 3, pp. 1442–1450.
- [10] K. Zhu and B. Mukherjee, "Traffic grooming in an optical WDM mesh network," *IEEE Journal of Selected Areas in Communications*, vol. 20, no. 1, pp. 122–133, January 2002.
- [11] R. Srinivasan, "MICRON: A framework for connection establishment in optical networks," in *Proceedings of OPTICOMM*, Dallas, TX, USA, October 2003, pp. 139–150.
- [12] W. D. Grover, *Mesh-based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*, Prentice Hall Publishers, New Jersey, 2003.
- [13] M. T. Fredrick and A. K. Somani, "A single-fault recovery strategy for optical networks using subgraph routing," in *Proceedings of the 7th IFIP Working Conference on Optical Network Design and Modelling (ONDM '03)*, Budapest, Hungary, February 2003, pp. 327–346.
- [14] S. Ramasubramanian, "On failure dependent protection in optical grooming networks," in *IEEE International Conference on Dependable Systems and Networks (DSN)*, Florence, Italy, June–July 2004, pp. 475–484.
- [15] R. Srinivasan and A. K. Somani, "A generalized framework for analyzing time-space switched optical networks," *IEEE Journal of Selected Areas in Communications: Special Issue on WDM-based Network Architectures*, vol. 20, no. 1, pp. 202–215, January 2002.
- [16] R. Srinivasan and A. K. Somani, "Request-specific routing in WDM grooming networks," in *Proceedings of IEEE International Conference on Communications (ICC 2002)*, New York, NY, USA, April 2002, pp. 2876–2880.