

On Failure Dependent Protection in Optical Grooming Networks

Srinivasan Ramasubramanian
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ 85721
srini@ece.arizona.edu

Abstract

Resiliency to link failures in optical networks is becoming increasingly important due to the increasing data rate in the fiber. Path protection schemes attempt to guarantee a backup path for a connection upon a failure in the network, thereby reducing the recovery time for a connection. In this paper, we develop a failure dependent path protection scheme that dynamically assigns a primary path and backup paths, one for each failure that would affect the primary path. A connection established on the primary path will be re-established on its backup path only if a failure in the network affects the connection. We evaluate the performance of our developed protocol and compare with an alternative approach based on sub-graph routing that achieves high network utilization and low blocking probability at the cost of re-establishing connections even if the failure in the network does not affect the primary path of the connection. We observe that up to a factor of eight reduction in the number of reconfiguration scenarios is achieved with less than 10% reduction in effective network utilization and less than 3% reduction in fairness metrics for tolerating any single link failure in NSFNET and ARPA-2 networks. The failure dependent protection approach developed in this paper is also applicable to any general failure scenarios that are modeled as shared risk link group failures.

1. Introduction

Optical 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 Gbps (OC-768) with each wavelength shared by connections with much lower capacity like 155 Mbps (OC-3) or 622 Mbps (OC-12). As the optical processing and buffer technologies are not mature currently to achieve routing individual packets in runtime, optical networks of today and those in the near future are ex-

pected to employ connection-oriented service paradigm. In such backbone networks, the major network operation is to establish a connection between source-destination pairs on-demand and release them when the connection is not 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 on every link of the chosen path depending on the requirement of the call. Path selection can be carried out in several ways. If a source-destination pair has one pre-selected path, then it is referred to as *fixed-path* approach. If a path is selected depending on the network status from a pre-selected set of candidate paths, then it is referred to as *dynamic path selection*. The set of candidate paths remain the same at all times and do not change with the network status. If the candidate paths are chosen based on the network status, the path selection process is referred to as *exhaustive routing*. Channel assignment refers to allocation of specific resources on every link of a chosen path, for example: (a) fiber, wavelength, and time slot assignment on the links in a WDM grooming network; and (b) fiber and wavelength assignment in a multi-fiber wavelength-routed network. Irrespective of the path selection or channel assignment strategy employed in the network, obtaining information along a path to assess the availability of resources to establish the connection becomes the fundamental requirement. Information collection in WDM grooming networks involve identifying availability of resources on the links along with the grooming capability of intermediate nodes on a specific path to identify resource availability on the path.

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 in-

stant. 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. In this paper, we consider only protection schemes as they typically have faster recovery times as compared to restoration schemes.

1.1. Taxonomy of protection schemes

Protection schemes proposed thus far in the literature can be classified as either link protection (LP) or path protection (PP). 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 scenario where the link that is connected to the source fails. Path protection schemes, in general, attempt to provide a backup path from the source to destination that may be independent of the working path. In case of a failure, the source node must establish the connection on the backup path.

Path protection schemes may be classified into two categories based on their knowledge on the link failure. A backup path that can be used for any link failure on the working path must be link-disjoint with the working path. Assignment of such a backup path does not require precise knowledge of the link failure, hence are referred to as *failure-independent path protection* (FIPP). Alternatively, a connection may be assigned more than one backup path depending on the failure scenario. Upon a failure, the source node establishes a new connection on the path corresponding to the failure scenario. Such an approach requires the precise knowledge of the failure in the network, hence are referred to as *failure-dependent path protection* (FDPP).

In order to achieve efficient utilization of network resources, multiplexing of resources across primary and/or backup paths 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 assigned to that shared resource.

1.2. Prior work and motivation

Dynamic connection establishment has been extensively studied in the context of wavelength-routed WDM networks

[1, 2, 3, 4, 5]. However, this issue has received very little attention in the context of WDM grooming networks until recently [6, 7]. Similarly, survivable routing has also received significant interest in the context of wavelength-routing networks, however it is in its early stages of research in the context of grooming networks. In [7], we have developed a framework for connection establishment in optical networks employing traffic grooming and heterogeneous switching architectures. The framework, referred to as Methodology for Information Collection and Routing in Optical Networks (MICRON), outlines a representation mechanism for link information as a matrix, 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 this paper, we develop a dynamic failure dependent path protection approach using the MICRON framework.

One approach to failure dependent path protection is to decompose a network into multiple networks to mimic each failure scenario. In [8], every network is decomposed into $L + 1$ networks, where L is the number of links in the network, to protect a connection against any single-link failure. While one network has all the links intact, the remaining L networks have a distinct link removed. Every request is provided a connection on each of these $L+1$ networks. If a connection could be established in all the networks then the request is accepted, otherwise, it is rejected. Such an approach has been shown to achieve good network utilization, however, it is achieved at the cost of having to switch the connections to backup paths upon a link failure even though the primary path of a connection is not affected by the failure. Such scenarios would occur due to a chain reaction in the network where a failed connection has a backup path whose links are currently being used for primary paths by other connections. In [8], the authors consider the number of reconfiguration scenarios as number of backup paths that are not the same as the primary path, however, reconfigurations may be required even when the paths are the same but the subtrunk (fiber, wavelength, and time slot) assignments are different. We observe that the number of failure scenarios that would necessitate switching to backup connections for a connection is extremely high compared to the number of failure scenarios that would affect the primary connection itself. The large number of reconfigurations will create a network-wide “chaos” that could effectively affect the reconfiguration time.

Our goal in this paper is to develop a methodology to assign primary and backup paths to requests such that the connections are switched to backup paths only if a failure in the network affects the primary connection. We develop a failure dependent protection (FDP) strategy based on our earlier work on the MICRON framework that achieves the above goal with a modest reduction in network perfor-

mance. The FDP methodology assigns primary and backup connections that could tolerate one SRLG failure at a given time.

It is worth noting that the backup paths assigned for connections may be useful for network management purposes during day-to-day network operation. Consider a regular (say weekly or monthly) maintenance of links that would render the link unusable for a few hours. Hence, connections routed along the particular link will have to be re-routed on the backup paths for the maintenance interval. It is often of interest to limit the extent of reconfiguration required in the network, thus limiting the disruption of service. Even if one were to assume rare link failures, which unfortunately is not true in real networks, the protection algorithms play a vital role from the view point of network management as well.

1.3. Organization

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 failure dependent protection (FDP) methodology using the framework. The performance of the FDP methodology is compared against the $L + 1$ protection scheme on NSFNet and ARPA-2 networks considering homogeneous and heterogeneous grooming architectures for the nodes. The performance results are discussed in Section 4. Our conclusions on this study is presented in Section 5.

2. Network Model

We 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. The elements of Ψ denote distinct set of links that may fail, i.e. if ψ_1 and ψ_2 are two elements of Ψ , then $\psi_1 \neq \psi_2$.

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). We use the terminology of time slots in this paper, however, the developed protocols are applicable to CDMA systems as well. The access to a wavelength is di-

vided 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 $1 \leq t \leq T$. For example, the tuple $(1, 1, 2, 1)$ (read from right to left) denotes first time slot in a frame on the second wavelength of the first fiber on the first link. 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) [9]. 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 a node. We illustrate the notion of trunks with an example. Consider a WDM grooming network where every link has four fibers, three wavelengths per fiber and two time slots per frame ($F = 4$, $W = 3$, $T = 2$). Fig. 1 shows the channels on a link. The shapes of the figures represent the time slots and the shades of the shapes represent wavelengths.

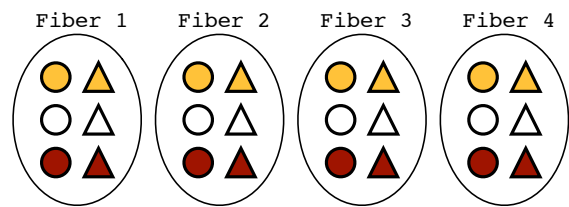


Figure 1. Representation of twenty four channels in a link having four fibers, three wavelengths per fiber, and two time slots per wavelength. Shapes represent time slots, shades represent wavelengths, number of shapes of a certain shade represents the number of fibers.

If time slot interchange and wavelength conversion are not permitted, a node i views a link ℓ as $W \times T$ trunks where each wavelength and time slot combination (w, t) forms a trunk. Every trunk has F channels as shown in Figure. 2(a). If time slot interchange is permitted, but not wavelength

conversion, a node i views a link ℓ as W trunks, where each wavelength forms a trunk. Every trunk has $F \times T$ channels as shown in Fig. 2(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 t on the link l forms a trunk. Every trunk has $F \times W$ channels as shown in Fig. 2(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 Fig. 2(d). A node with such a capability is referred to as a *full grooming node*.

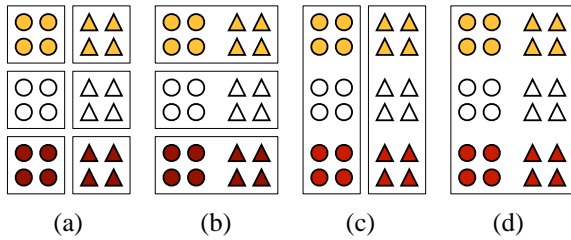


Figure 2. Possible grouping of channels in a link as trunks. (a) Each wavelength and time slot combination forms a trunk; (b) Each wavelength is a trunk; (c) Each time slot is a trunk; and (d) The link is a trunk.

Fig. 3 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 *sub-trunk*.

A call arriving in the network requires a connection to be established from a source to destination. Connection establishment involves selection of a path and assigning channels on the path such that the channel on one link can be

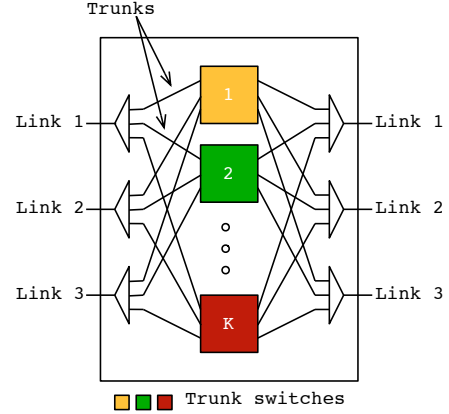


Figure 3. Node architecture in a Trunk Switched Network.

switched to the successive link on the path by the node connecting the links. In a TSN, connection establishment consists of three steps: (1) selecting a path; (2) assigning a sub-trunk on every link, or equivalently assigning a trunk at every node; and (3) assigning one or more channels depending on the call requirement on every sub-trunk on every link. Hence, a connection in a network is represented by a sequence of link and sub-trunk pair, or equivalently as a sequence of node and trunk pair. If every node in the network employs full permutation switching for every trunk, then any channel that falls within the selected sub-trunk on a link can be chosen for establishing a connection.

In addition to the *working* path, one or more backup paths are assigned to the connection to tolerate any single SRLG failure. The number of backup paths will be the same as the number of failure scenarios that will affect the primary path of the connection. In case of a failure, the affected calls will continue on their respective backup paths. We assume that there will be at most one SRLG failure at any given time.

3. Failure Dependent Protection using MICRON Framework

We employ the MICRON framework [7] to collect network information and establish connections. We develop failure dependent routing technique based on this framework to tolerate any single SRLG failure at a given instant of time. The following sub-sections describe in detail the information stored for each link, the computation of available capacity for working and backup path establishment, and path selection strategies.

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 .

Let S_ℓ and P_ℓ be matrices where the elements of the matrices denote the total number of channels and number of channels occupied by working connections, respectively, in each subtrunk. Let $G_\ell(\psi)$ be a matrix where the elements denote the number of channels in a subtrunk that are currently occupied by working connections that would fail due to 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. Let $B_\ell(\psi)$ be a matrix where the elements denote the number of backup channels required in a subtrunk in case of an SRLG failure 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 , $n_{xy} = \max_\psi m_{xy}(\psi)$.

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

$$P_\ell - G_\ell(\psi) + B_\ell(\psi) \leq S_\ell. \quad (1)$$

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.

3.2. Available capacity information

The channel availability information of a link ℓ is represented as a matrix A_ℓ , where the elements of the matrix represent the channel availability information of the subtrunks. 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 (1) for all failure scenarios in Ψ . Hence, the availability matrix of a link for a working path computation is obtained as:

$$A_\ell = S_\ell - P_\ell - \max_{\psi \in \Psi} [B_\ell(\psi) - G_\ell(\psi)]. \quad (2)$$

Note that if an element of A_ℓ is non-zero, it implies that the specific sub-trunk has free channels that may be assigned

to a working connection without compromising on network resiliency.

In order to assign a channel on a subtrunk Θ_{xy}^ℓ on link ℓ to overcome a failure ψ , it is sufficient that the link occupancy satisfies Equation (1) only for ψ . In order to obtain routing for the backup connection for a failure ψ , the availability matrix of a link is computed as:

$$A_\ell = S_\ell - P_\ell - B_\ell(\psi) + G_\ell(\psi). \quad (3)$$

It is worth noting that the above assignment only takes into account only those connections that would be re-assigned in case of failure ψ . Hence, backup multiplexing is inherent to the above computation for available capacity.

As every node in the network is assumed to employ full-permutation switching for each trunk, the channels within a trunk at a node are indistinguishable. Equivalently, the channels within a sub-trunk 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 Equations 2 and 3 are replaced with 1. We employ such a matrix representation in this paper.

3.3. Path information

The information about a certain path from node i to k that are not physically connected by a fiber can be obtained by combining the link information in the path. The matrix representation for a path is defined in a manner similar to that of a link. A path matrix from node i to k through j is obtained as a matrix multiplication of individual path segments A_{ij} and A_{jk} as:

$$A_{ik} = A_{ij}A_{jk} \quad (4)$$

We employ a generalized version of matrix multiplication to compute the path metric. An element a_{xy}^{ik} (the superscript ik denotes the matrix to which the element belongs to) is obtained as:

$$a_{xy}^{ik} = (a_{x1}^{ij} \otimes a_{1y}^{jk}) \oplus (a_{x2}^{ij} \otimes a_{2y}^{jk}) \oplus \dots \oplus (a_{xK_j}^{ij} \otimes a_{K_j y}^{jk}) \quad (5)$$

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. In this paper, we employ the *AND* operation for \otimes and *OR* operation for \oplus . Thus, the matrices along the path represent the connectivity information only.

In order to reduce the computational complexity associated with computing the path information matrix, we employ a vector called Path Information Vector (PIV). The path information vector at a node k for a path p with source

i and destination k , denoted by V_{ik} is of dimension $1 \times K_k$. V_{ik} is obtained as a product of the path information vector at the source node and the information matrix of the path connecting nodes i and k as: $V_{ik} = U_i A_{ik}$, where U_i denotes the path information matrix at the source node which is always set as a unit row vector.

Assume that the path from node i to k that passes through node j . Re-writing the above equation gives the relationship between the PIV vectors at node j and node k .

$$V_{ik} = U_i A_{ik} = U_i A_{ij} A_{jk} = V_{ij} A_{jk} \quad (6)$$

The matrix-vector multiplication employed above is similar to the generalized matrix multiplication proposed earlier in the paper with the operator tuple (\otimes, \oplus) . The elements of PIV at a node indicates specific properties about paths that end at a certain trunk.

3.4. Path selection and sub-trunk assignment

The path information vector can be used to select a suitable path from a given source-destination pair. We employ Dijkstra's shortest path algorithm that uses PIV and hop length. Every path that is considered in the Dijkstra's algorithm is first checked for availability of resources (at least one non-zero entry in the PIV) followed by minimum hop length. Hence, paths that does not have resources are not considered for connection establishment although they might have shorter hop lengths. We refer to such a path selection as Available Shortest Path (ASP) approach. Based on our earlier study [10], we observe that ASP is an efficient path selection algorithm as it attempts to use less resources in the network. Hence, we adopt the ASP scheme for selecting the working and backup paths in this paper.

We employ first-fit sub-trunk assignment for working and backup paths. The channel assignment is performed from the destination to source by selecting the first available trunk at each node on the path. For a detailed discussion on the working of first-fit sub-trunk assignment with MICRON framework, the readers are referred to [7].

3.5. Connection establishment and release

We assume that the network is 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. We assume that 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.

Upon 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 below:

1. Update the available capacity matrix on every link for primary path assignment as shown in Equation 2. The non-zero entries are replaced by 1 to achieve binary-valued matrix elements.
2. Obtain a path employing the ASP approach and a sub-trunk assignment on the path. If a path or sub-trunk assignment cannot be obtained the request is rejected. Go to Step 6.
3. The request has a specific primary path and a sub-trunk assignment on the primary path. Let $\mathcal{L}_{\mathcal{R}}$ denote the links through which the connection is routed and let (x_{ℓ}, y_{ℓ}) denote the sub-trunk assignment on link $\ell \in \mathcal{L}_{\mathcal{R}}$. 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 every $\psi \in \Psi_{\mathcal{R}}$, obtain a backup path.
 - (a) Update the available capacity matrix on every link for backup path assignment corresponding to SRLG failure ψ as shown in Equation 3. The non-zero entries are replaced by 1.
 - (b) Remove every link $\ell \in \psi$ from the network.
 - (c) Obtain a backup path and sub-trunk assignment for the path. If a backup path or sub-trunk assignment cannot be obtained, the request is rejected. Go to Step 6. Otherwise, let $\mathcal{L}_{\mathcal{R}}^{\psi}$ denote the links through which the backup path for failure ψ passes through and let $(x_{\ell}, y_{\ell})^{\psi}$ denote the sub-trunk assignment on link $\ell \in \mathcal{L}_{\mathcal{R}}^{\psi}$.
 - (d) Add every link $\ell \in \psi$ to the network.
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 sub-trunk assignments are also obtained on primary and backup paths.
 - (a) Update the capacity used by the primary connections on the corresponding sub-trunks 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 $\ell \in \mathcal{L}_{\mathcal{R}}$.
 - (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 $G_{\ell}(\psi)$ for every link $\ell \in \mathcal{L}_{\mathcal{R}}$ and every SRLG failure $\psi \in \Psi_{\mathcal{R}}$.

- (c) 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 $B_\ell(\psi)$ for every link $\ell \in \mathcal{L}_R^\psi$ and every $\psi \in \Psi_R$.

6. Exit.

When a connection is terminated, the link capacities must be released. Step 5 of the connection establishment procedure is employed for connection release, however, instead of adding the request capacity to the matrices, they are subtracted.

The above connection management scheme ensures that sufficient conditions (Equations 2 and 3) for recovering from single-link failures are obeyed. Satisfying the sufficient condition for primary path assignment also guarantees that a connection will be re-routed only when an SRLG failure affects the primary path of the connection.

4. Performance Evaluation

The performance of the FDP methodology developed in this paper is compared against the $L + 1$ protection strategy on the NSFNet and ARPA-2 networks. The topology of the networks are shown in Figure 4. Every link in the network employs two uni-directional fibers, each consisting of sixteen wavelengths and eight time slots per wavelength. Thus, a total of 128 channels constitute a link.

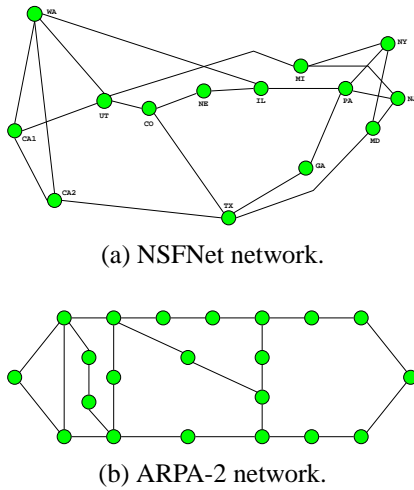


Figure 4. Network topologies considered for performance evaluation.

We consider two scenarios of network architectures. In the first architecture, all the nodes are wavelength-level

grooming nodes. We refer to this architecture as *homogeneous*. In the second architecture, nodes can be one of three types: wavelength-level grooming node, time slot level grooming node, and full-grooming node. For the two networks considered, nodes with degree four are assigned as full-grooming nodes, those with degree three are assigned as time slot level grooming nodes, and those with degree two are assigned as wavelength level grooming nodes.

We model a single link failure scenario in the network as SRLG failures in which each SRLG group has exactly one link. Upon an SRLG failure, both the fibers in a link fail. We assume that the network can have at most one SRLG failure at any given instant.

Requests arrive at the nodes according to Poisson process with rate λ and have an exponential holding time with unit mean. 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 request has one channel capacity requirement and all requests are assumed to require protection against any single SRLG failure.

The networks employ available shortest path (ASP) [10] with first-fit wavelength assignment for both FDP and $L + 1$ protection methodologies.

We compute the number of reconfiguration scenarios for a connection as the the number of SRLG failures that would necessitate the connection established on the primary path to be switched to a backup path. Note that if the backup path is the same as the primary path and the subtrunk assignments on both the paths are the same, then the connection need not be re-established. Hence, the above metric computes the number of SRLG failures for which the backup path and subtrunk assignment on the backup are not the same as the primary path and subtrunk assignment on the primary path.

Tables 1 and 2 show the average number of reconfiguration scenarios for a connection in the NSFNET and ARPA-2 networks, respectively. As expected, it is observed that FDP scheme outperforms $L + 1$ methodology significantly. Note that the ratio of this metric to the number of SRLG failures $|\Psi|$ denotes the probability that a connection is switched to a different path and/or subtrunk assignment upon a random SRLG failure.

Tables 3 and 4 show the length of the primary path of accepted connections. For a single link failure scenario considered in this study, the number of reconfiguration scenarios under FDP scheme is the same as the average primary path length of the accepted connections. This metric shows an increasing trend at first and then decreases for FDP methodology. The reason for such a trend is that as

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L+1	FDP	L+1
1000	2.12	17.28	2.12	16.78
1100	2.19	17.60	2.18	17.10
1200	2.27	17.84	2.28	17.48
1300	2.30	17.98	2.37	17.70
1400	2.33	18.08	2.42	17.86
1500	2.32	18.18	2.44	17.92
1600	2.31	18.27	2.44	17.98

Table 1. Number of reconfiguration scenarios in the NSFNet network.

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L + 1	FDP	L+1
500	3.42	18.52	3.42	22.36
600	3.42	19.28	3.44	22.74
700	3.45	19.68	3.50	22.92
800	3.47	19.96	3.54	23.06
900	3.45	20.18	3.52	23.14
1000	3.41	20.28	3.47	23.20

Table 2. Number of reconfiguration scenarios in the ARPA-2 network.

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. Under the $L + 1$ methodology, the number of reconfiguration scenarios is much higher than the average primary path length of the connections. The number of reconfiguration scenario increases with increase in traffic (for the range of traffic considered here). The reason for such a behavior is again due to the ASP routing algorithm. With increase in load, ASP routing attempts to find paths that may be longer, hence the chances of the backup paths being different from the primary path increases. The path length of the connections established through $L + 1$ approach shows a steadily decreasing trend. The reason for such a trend is because the $L + 1$ approach treats the different networks independent of each other. Thus, establishment of a connection in a network corresponding to a failure scenario does not increase the path length of a connection established in the network without failures. Such an independence is not true for FDP scheme.

The above decrease in the number of reconfiguration scenarios for a connection is achieved at the cost of other performance measures such as blocking probability, network

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L+1	FDP	L+1
1000	2.12	2.10	2.12	2.10
1100	2.19	2.10	2.18	2.10
1200	2.27	2.10	2.28	2.10
1300	2.30	2.09	2.37	2.09
1400	2.33	2.08	2.42	2.08
1500	2.32	2.06	2.44	2.07
1600	2.31	2.05	2.44	2.06

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

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L+1	FDP	L+1
500	3.42	3.41	3.42	3.42
600	3.42	3.41	3.44	3.41
700	3.45	3.36	3.50	3.37
800	3.47	3.30	3.54	3.32
900	3.45	3.24	3.52	3.27
1000	3.41	3.19	3.47	3.22

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

utilization, and fairness. Figures 5 and 6 show the blocking probability of connections under FDP and $L + 1$ approaches for both homogeneous and heterogeneous cases. It is observed that $L + 1$ approach has a better performance in blocking probability than FDP approach.

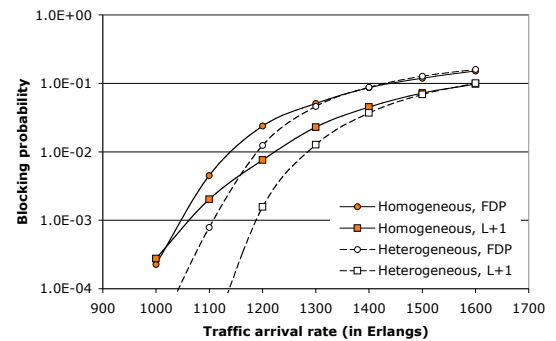


Figure 5. Blocking probability in the NSFNET network.

The performance difference is prominent in the case of NSFNET network while it is not in the ARPA-2 network. The NSFNET network has better connectivity than the ARPA-2 network, hence the path length distribution for

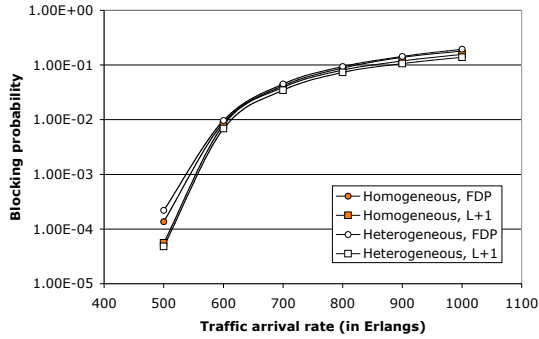


Figure 6. Blocking probability in the ARPA-2 network.

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 next shortest path between any two node-pairs in NSFNET network is less as compared to that in ARPA-2 network. As the shortest path length between node pair increases, the minimum amount of resources required in the network to accommodate a connection increases, thereby reducing the avenues 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.

We compute the resources utilized in the network through *effective network utilization* [10]. 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 the accepted requests only, while the offered load is computed as the effective network utilization over all requests.

Tables 5 and 6 show the effective network utilization for NSFNET and ARPA-2 networks, respectively. It is observed that the FDP has a lower utilization as compared to $L+1$ approach. The difference in utilization increases with an increase in the network load. Network utilization difference under high blocking scenarios do not give meaningful results, therefore, we restrict our considerations to those network loads that have a blocking probability values of 20% or less. For the highest arrival rate of traffic considered in this study (1600 Erlangs for NSFNET network and 1000 Erlangs for ARPA-2 network), the percent-

age reduction in network utilization under FDP scheme as compared $L+1$ approach are 7.24, 7.59, 4.21, and 8.87 for homogeneous NSFNET, heterogeneous NSFNET, homogeneous ARPA-2, and heterogeneous ARPA-2 networks, respectively. It is observed that with less than 10% loss in network utilization, it is possible to reduce the number of reconfiguration scenarios significantly.

Arrival Rate	Offered Load	Homogeneous		Heterogeneous	
		FDP	L+1	FDP	L+1
1000	0.373	0.372	0.373	0.373	0.373
1100	0.410	0.407	0.409	0.409	0.410
1200	0.448	0.435	0.443	0.441	0.446
1300	0.484	0.454	0.471	0.458	0.477
1400	0.523	0.467	0.493	0.470	0.499
1500	0.559	0.478	0.510	0.477	0.514
1600	0.596	0.487	0.525	0.487	0.527

Table 5. Effective network utilization in the NSFNet network.

Arrival Rate	Offered Load	Homogeneous		Heterogeneous	
		FDP	L+1	FDP	L+1
500	0.257	0.256	0.257	0.256	0.257
600	0.308	0.304	0.305	0.304	0.305
700	0.359	0.338	0.340	0.337	0.342
800	0.411	0.360	0.365	0.358	0.370
900	0.462	0.374	0.386	0.372	0.395
1000	0.513	0.387	0.404	0.380	0.417

Table 6. Effective network utilization in the ARPA-2 network.

Finally, we compare the average shortest-path length of the requests that are accepted in the network. 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 an increase in the offered load. The flatter this metric remains with increasing load, the fairer the routing algorithm is. Tables 7 and 8 show the average shortest path length of the accepted requests. The performance reduction in fairness due to FDP is less than 1% for NSFNET network and 2.5% for ARPA-2 network at the highest arrival rate considered here.

It is also worth noting that besides reducing the number of reconfiguration scenarios for a connection, the approach

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L+1	FDP	L+1
1000	2.10	2.10	2.10	2.10
1100	2.10	2.10	2.10	2.10
1200	2.09	2.10	2.10	2.10
1300	2.07	2.09	2.08	2.09
1400	2.06	2.08	2.07	2.08
1500	2.04	2.06	2.05	2.07
1600	2.02	2.05	2.04	2.06

Table 7. Average shortest path length of accepted requests in the NSFNet network.

Arrival Rate	Homogeneous		Heterogeneous	
	FDP	L+1	FDP	L+1
500	3.42	3.41	3.42	3.42
600	3.40	3.41	3.40	3.41
700	3.35	3.36	3.36	3.37
800	3.29	3.30	3.29	3.32
900	3.21	3.24	3.21	3.27
1000	3.14	3.19	3.14	3.22

Table 8. Average shortest path length of accepted requests in the ARPA-2 network.

developed in this paper also reduces the primary connection setup time significantly (by a factor more than that by which the number of reconfiguration scenarios is reduced). The number of backup paths computed by our approach depends on the number of SRLG failures that affect the primary path as compared to the $L + 1$ approach where $L + 1$ backup paths need to be computed irrespective of the number of SRLG failures that would affect the connection on the primary path.

5. Conclusion

In this paper, we have developed a failure dependent protection approach that assigns primary and backup paths to requests in order to tolerate any single-link failure in an optical grooming network with heterogeneous grooming architectures. The proposed approach reassigns a primary connection to its backup path only if a link failure affects the primary connection. We demonstrate that up to a factor of eight times reduction in the number of reconfiguration scenarios is achieved with less than 10% reduction in effective network utilization and less than 3% reduction in fairness metrics for tolerating any single link failure in NSFNET and ARPA-2 networks. The failure dependent protection approach developed in this paper is also applica-

ble to any general failure scenarios that could be modeled as SRLG failures.

Acknowledgments

The research presented in this paper is supported in part by National Science Foundation under grant ANI-0325979. We would like to thank Prof. Nathan Goodman of the Electrical and Computer Engineering Department at University of Arizona for allowing us to use his computing facilities for our simulations.

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, J. Jue, L. Sahasrabudde, R. Ramamurthy, and B. Mukherjee, "Dynamic lightpath establishment in wavelength-routed WDM networks," *IEEE Communications*, pp. 100–108, September 2001.
- [3] S. Ramamurthy and B. Mukherjee, "Fixed alternate routing and wavelength conversion in wavelength-routed optical networks," in *Proceedings of the Global Telecommunications Conference, GLOBECOM'98*, Sydney, Australia, November 1998, pp. 2295–2303.
- [4] E. D. Lowe and D. K. Hunter, "Performance of dynamic path optical networks," in *IEE-Proceedings of Optoelectronics*, August 1997, pp. 235–239.
- [5] 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.
- [6] 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'02*, June 2002.
- [7] R. Srinivasan, "MICRON: A framework for connection establishment in optical networks," in *Proceedings of OPTICOM*, October 2003, pp. 139–150.
- [8] 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*, February 2003, pp. 327–346.
- [9] 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*, pp. 202–215, January 2002.
- [10] R. Srinivasan and A. K. Somani, "Request-specific routing in WDM grooming networks," in *Proceedings of IEEE International Conference on Communications (ICC 2002)*, April 2002, pp. 2876–2880.