On Partial Protection in Groomed Optical WDM Mesh Networks

Jing Fang[1], Mahesh Sivakumar[2], Arun K. Somani[1] and Krishna M. Sivalingam[2]*
[1] *Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011*
[2] *Department of CSEE, University of Maryland, Baltimore County, Baltimore, MD 21250*

Abstract

In this paper, we consider the problem of survivable network design in traffic groomed optical WDM mesh networks with sub-wavelength capacity connections. In typical survivable network designs, individual sessions are provided either full protection or no protection. We consider a quality of protection (QoP) framework where a connection is provided partial protection, i.e. when a link failure occurs on the primary path, the protection bandwidth provided on the backup path is less than or equal to the primary bandwidth. Each connection request specifies the primary bandwidth and a minimum backup bandwidth required. The network will guarantee at least the minimum backup bandwidth and, if capacity is available, higher backup bandwidth up to the primary path's bandwidth. The advantage of such a model is that it can reduce backup capacity requirements based on connection needs leading to lower blocking probability and lower network costs. We consider two scenarios: (i) a network with static traffic and formulate the problem of providing partial protection in groomed networks as an Integer Linear Program (ILP); and (ii) a network with dynamic traffic that is analyzed using discrete-event simulation models. The results quantify the gain in blocking probability for different partial protection scenarios.

1 Introduction

Optical networking has shown remarkable progress in the past few years with developments in wavelength division multiplexing (WDM) and in transport technology [14]. In this paper, we consider a wide area network based on an optical WDM mesh topology. We also assume that a circuit-switched model is used, where an end-to-end optical lightpath is set up to satisfy a given connection request. Further, since a majority of the traffic streams supported by the network typically require only a fraction of the wavelength capacity, multiple connections are carried on a given wavelength leading to sub-granularity lightpath allocations [21]. This is defined as *traffic grooming*. A survey of related work on traffic grooming in optical WDM mesh networks can be found in [11, 21].

We also consider another important aspect of network design, namely survivability. Network monitoring statistics indicate that failures are not an uncommon occurrence in backbone networks [5]. Hence, fault-tolerance or survivability is an important consideration for such high capacity networks. There are several unique and interesting challenges that arise when survivability is considered for groomed networks. Some of these include scalability since several sub-wavelength connections have to be restored under failure and also the possibility that the different connections on a wavelength might require different protection guarantees.

In this paper, we consider a quality of protection (QoP) framework where individual requests specify their protection needs in different ways [2, 17]. The paper proposes a *partial protection* model that enables the provision of variable protection bandwidth to connections. In the proposed framework each connection is provided *partial protection*, i.e. when a failure occurs on the primary path, the protection bandwidth provided on the backup path is less than or equal to the primary bandwidth. Each connection request specifies the primary bandwidth and a minimum backup bandwidth. The network will guarantee at least the minimum backup bandwidth and, if capacity is available, higher backup bandwidth up to the primary path's bandwidth. Note that the availability of traffic grooming facilitates this concept since it allows provisioning of sub-wavelength capacity to each connections. The advantage of this model is that it can reduce backup capacity requirements based on connection needs leading to lower blocking probability and lower network costs. Note that SONET *Virtual Concatenation (VCAT)* techniques could also provide partial protection by using traffic splitting at the source [1, 20] so that when failures occur on any of the sub-streams, traffic can still be carried on the other streams.

We consider two different scenarios for applying the partial protection model: (i) a network with static traffic and formulate the problem of providing partial protection in groomed networks as an Integer Linear Program (ILP); and (ii) a network with dynamic traffic that is analyzed using discrete-event simulation models. The results quantify the gain in blocking probability for different partial protection scenarios.

---

*Part of the research was supported by NSF grant No. ANI-0322959 and ANI-0323374.

2 Background and Related Work

An elaborate review of survivability techniques for WDM networks is omitted here due to space constraints but survey articles may be found in [5, 12]. Survivability in traffic groomed mesh networks supporting sub-wavelength granularity connections has only recently received some attention. Some of this work is summarized below.

In [6], the authors studied the static traffic model for groomed mesh networks with protection requirements. They modeled the problem as an ILP with the objective function designed to reduce the overall network cost. The traffic grooming problem for survivable WDM networks was studied in [8] for shared protection and three schemes namely protection-at-lightpath (PAL) level, mixed protection-at-connection (MPAC) level, and separate protection-at-connection (SPAC) level were proposed. The same problem was studied in [9] for dedicated protection and two approaches, protection-at-lightpath (PAL) level and protection-at-connection (PAC) level, were studied. The problem of provisioning dynamically established multi-granularity traffic streams with protection requirements was studied in [15] and two schemes namely *Mixed Primary-Backup Grooming Policy (MGP)* and *Segregated Primary-Backup Grooming policy (SGP)* were proposed.

Most survivability mechanisms proposed for optical WDM networks aim at providing 100% failure recovery guarantee in the event of a single failure [10]. The inefficient resource utilization with proactive approaches reduces the the network's overall ability to provision demand for more connections. *Quality-of-Protection (QoP)* aims to bridge the gap between the two well known protection grades, fully guaranteed and no-guaranteed connections. This can be achieved by using multiple protection grades for connections based on the amount of bandwidth utilized in protecting them (example: guaranteed protection, best-effort protection etc.). Upon a failure, the probability that a connection will recover from a failure is determined by its desired QoP. While QoP in wavelength-routed mesh networks has been addressed in detail [2, 4, 7, 17], its implication on networks capable of carrying sub-wavelength granularity connections remains an open research question.

In terms of technologies to support traffic grooming, there are two options: electronic traffic grooming [22] and optical traffic grooming [11]. In electronic traffic grooming, each switching node consists of an optical switching fabric and an electronic SONET grooming fabric that consists of SONET Add-Drop Multiplexers (SADMs) and electronic switching fabrics. This type of grooming is feasible with current commercially available products, but has the disadvantage of requiring opto-electronic conversion at intermediate grooming nodes. With optical traffic grooming, a single wavelength is organized as a time-division multiplexed frame that consists of time slots [18]. Accordingly, in a *TDM wavelength routing network*, the establishment of a connection requires the assignment of time slots in addition to routing and wavelength assignment [13]. The switching is done at the time-slot level entirely in the optical domain and connections are assigned a set of time slots within each frame based on their specified requests. This technology allows end-to-end all-optical transmission but is still in early stages of development. The proposed techniques in this paper can work with both optical and electronic grooming technologies.

3 The Partial Protection Model

In this paper, we investigate the problem of Quality of Protection (QoP) enabled design of circuit-switched survivable grooming networks. We consider the proactive protection model where backup capacity is assigned when a connection is set up. Each connection is provided a *primary path* and a link-disjoint *backup path* that will be used to protect against link failures along the primary path. We do not consider node failures in this paper.

In particular, we study the problem of maximizing the protection bandwidth provided to each low-speed connection in a groomed optical WDM mesh network. In order to enable QoP, we introduce the notion of *partial protection* that provisions survivable connections with varying protection grades in the network. With partial protection, the primary paths are given the requested bandwidth, but the bandwidth provided to protection paths will vary in accordance to the minimum protection guarantee specified by each request.

The connection request for a given source-destination pair (i, j) specifies a primary bandwidth of d_{ij} units and a minimum protection bandwidth of b_{ij} units. The actual assigned capacity on backup path will be c_{ij} where $b_{ij} \leq c_{ij} \leq d_{ij}$ and c_{ij} represents the actual protection bandwidth provided to the connection between i and j. The network will guarantee the minimum protection bandwidth when failure occurs and will attempt to provide additional protection bandwidth depending on current network conditions. The objective of this work is to maximize c_{ij} for each (i, j), and thus, to optimize the QoP provided for each connection. Such a design would be extremely useful in cases where the network cannot afford full protection to every connection. We consider two different scenarios where this model can be applied.

For the *static traffic* scenario, the network designer is provided with the network topology and a traffic matrix with all the connections and their bandwidth requirements specified. The goal is then to design the network to either minimize the overall cost to support all the connections or to maximize the number of admitted connections for the given resource constraints (i.e. number of wavelengths on each link, etc.).

For the *dynamic traffic* scenario, traffic requests arrive dynamically based on some stochastic arrival process. The goal of the network is to allocate lightpath resources for each connection while meeting the primary and protection bandwidth requirements. The objective is to maximize the number of admitted connections by using efficient routing and wavelength assignment techniques.

4 Static Traffic Scenario

We consider network design for a network with a pre-specified traffic matrix. The study in [3] proposed exact integer linear programming (ILP) formulations for survivable design in WDM grooming networks based on primary backup multiplexing and dedicated backup reservation. These formulations can be modified to solve the partial protection problem in grooming networks. However, a direct modification makes the formulations nonlinear due to the fact that the capacity allocated to backups is unknown in the case of partially protected connections. If we reconsider the motivation for partial protection in grooming networks, the problem can be solved differently. The main reason for adopting partial protection is that the network may not have enough wavelength resources to provide full protection for each request. In other words, we may not want to provision an extra wavelength just to provide more than the minimum capacity required for protection. Based on the above fact, the partial protection problem can be divided into two sub-problems as follows:

Resource Minimization: Given a network topology and a set of point-to-point demands and their link disjoint primary and backup routes, provision each connection request m with a primary capacity d_m and a backup capacity b_m in such a way that the total number of wavelength links used is minimized.

Protection Maximization: Given the initial grooming solution from above step, optimally distribute the residual network capacity to provide better protection to some, if not all, of the requests.

Each subproblem can be formulated as an ILP optimization problem. For capacity allocation, both primary backup multiplexing and dedicated backup reservation can be applied. The study in [3] showed that while backup multiplexing is computational expensive for WDM grooming networks, dedicated backup reservation performs fairly well and becomes affordable due to the fact that the wavelength utilization is significantly improved by the grooming capability. Hence, we present a two-phase ILP formulation with dedicated backup reservation.

Link Primary Sharing: One simple and effective way of assigning backup capacities is to reserve dedicated capacity for each backup path. While choosing primary paths, instead of simply choosing the shortest path, we try to *minimize* the total *link-primary-sharing* (MLPS). The link-primary-sharing is defined as: $s_{ij} = max(0, P_{ij} - 1)$, where s_{ij} denotes the link-primary-sharing of link (i, j) and P_{ij} denotes the total number of primary paths that utilize link (i, j). s_{ij} can be viewed as the penalty assigned to link (i, j) when it is used by more than one primary path.

Assumptions:

1. The network is a single-fiber irregular mesh network.

2. A connection request cannot be divided into several low-speed connection requests and routed separately from the source to the destination. The data traffic on a connection request should always follow the same route.

3. The transceivers in a network node are fixed, and hence wavelength continuity constraint still applies.

4. Each grooming node has unlimited multiplexing and demultiplexing capability. This means that the network node can multiplex/demultiplex as many low-speed traffic streams to a lightpath as needed, as long as the aggregated traffic does not exceed the lightpath capacity.

Notations: The problem inputs and system parameters are:

- The number of nodes in the network is N, number of wavelengths carried by each fiber is W, and the capacity of each wavelength is C (assuming each wavelength has the same capacity). In this paper, we choose C to be OC-48.
- A physical topology $G_p = (V, E)$ consisting of a weighted unidirectional graph, where V is the set of network nodes, and E is the set of physical links (edges). Nodes correspond to network nodes and links correspond to the fibers between nodes.
- A traffic matrix $D_{N \times N} = \{d_m\}$, where d_m indicates the required capacity of low-speed traffic requests in units of OC-1.
- A guaranteed backup capacity matrix $B_{N \times N} = \{b_m\}$, where b_{ij} is the guaranteed backup capacity, or in other words, the lower bound of the backup capacity for request m.
- The capacity weight of link (i, j), denoted by w_{ij}^c, which is a positive real number and can be regarded as a measure of capacity consumption per wavelength on the link. These weights are used to differentiate links from the capacity cost point of view.
- The sharing cost of link (i, j), denoted by w_{ij}^s, which is a positive real number and can be treated as a measure of the link primary sharing penalty s_{ij}.
- $i, j = 1, 2, \ldots, N$: Node identifier.
- $w = 1, 2, \ldots, W$: Wavelength identifier.
- $m, n = 1, 2, \ldots, N \times (N-1)$: Number assigned to each demand (s-d pair); s_m and t_m respectively denote the source and the destination node of demand m.

- K: Number of alternate routes between every s-d pair; $K = 2$ in this model.
- $p, r = 1, 2, \ldots, KW$: Number assigned to a path for each s-d pair. A path has an associated wavelength (lightpath). Each route between every s-d pair has W wavelength continuous paths. The first $1 \leq p, r \leq W$ paths belong to route 1 and $W + 1 \leq p, r \leq 2W$ paths belong to route 2.

The following notations are for path-related information:

- $\delta^{m,p}$: Path indicator that takes a value of one if (m, p) is chosen as a primary path; zero otherwise (binary variable).
- $\gamma^{n,r}$: Path indicator that takes a value of one if (m, r) is chosen as a restoration path; zero otherwise (binary variable).
- $L_{ij}^{m,p}$: Link indicator that takes a value of one if link (i, j) is used in path (m, p); zero otherwise (data).
- $W_w^{m,p}$: Wavelength indicator that takes a value of one if wavelength w is used by the path (m, p); zero otherwise (data).

The following variables are used to represent wavelength assignment:

- $p_{ij,w}^m$: binary variable, 1 if wavelength w on link (i, j) is used by primary path of demand m; 0 otherwise.
- $r_{ij,w}^m$: binary variable, 1 if wavelength w on link (i, j) is used by backup path of demand m; 0 otherwise.
- $u_{ij,w}$: binary variable. Wavelength usage indicator. 1 if wavelength w on link (i, j) is used by any primary or backup path for any request; 0 otherwise.
- λ_{ij}: nonnegative integer, total number of wavelengths required on link (i, j).
- $\alpha_{ij,w}$: nonnegative integer, total capacity assigned to primary paths on wavelength w on link (i, j).
- $\beta_{ij,w}$: nonnegative integer, total capacity reserved for backup paths on wavelength w on link (i, j).
- c_m: capacity assigned to the backup path of request m.

4.1 ILP formulation I: Resource Minimization

Objective Function: *Minimize the total wavelength-links as well as total link-primary-sharing:*

$$min \sum_{(i,j)\in E} (w_{ij}^c \times \lambda_{ij} + w_{ij}^s \times s_{ij}). \tag{1}$$

Here, w_{ij}^c is set to one and hence, the summation of the first term gives the value of total wavelength-links that are exploited in the network. By changing the value of w_{ij}^s, we can change the weight of the second term in the objective function; $w_{ij}^s = 3$ in our experiments.

Constraints:

1. On physical route variables:
   A lightpath can carry traffic for a s-d pair only if it is in the physical route of this request.

$$p_{ij,w}^m = \sum_{p=1}^{KW} \delta^{m,p} L_{ij}^{m,p} W_w^{m,p} \tag{2}$$

$$r_{ij,w}^m = \sum_{r=1}^{KW} \gamma^{n,r} L_{ij}^{m,r} W_w^{m,r} \tag{3}$$

$$\delta^{m,p}, \gamma^{n,r} \in \{0, 1\} \tag{4}$$

2. On path indicators:
   One and only one path will be assigned as a primary(backup) path for each request.

$$\sum_{p=1}^{KW} \delta^{m,p} = 1 \tag{5}$$

$$\sum_{r=1}^{KW} \gamma^{n,r} = 1 \tag{6}$$

3. On topology diversity of primary and backup paths:
   Primary and restoration paths of a given demand should be link disjoint.

$$\sum_{p=1}^{W} \delta^{m,p} = \sum_{r=W+1}^{KW} \gamma^{n,r} \tag{7}$$

$$\sum_{p=W+1}^{KW} \delta^{m,p} = \sum_{r=1}^{W} \gamma^{n,r} \tag{8}$$

4. On wavelength capacity variables:
   Primary capacities are aggregated. Backup capacities are aggregated when dedicated backup reservation is applied. In other words, for each wavelength on a particular link, the total capacity used by the primary paths is the summation of the capacity of all the primary paths that takes this wavelength on the particular link. Similarly, the total backup capacity for each wavelength on a link can be obtained.

$$\alpha_{ij,w} = \sum_m d_m p_{ij,w}^m \tag{9}$$

$$\beta_{ij,w} = \sum_m b_m r_{ij,w}^m. \tag{10}$$

   For each wavelength on a particular link, the sum of primary capacities and backup capacities should not exceed the total wavelength capacity.

$$\alpha_{ij,w} + \beta_{ij,w} \leq C \tag{11}$$

5. On fiber capacity constraints:
   The number of wavelengths used on a fiber should not exceed the total number of wavelengths carried by the

fiber. The second set of equations (equation (14)) together set $u_{ij,w} = 1$, if $x_{ij,w} \geq 1$, and zero otherwise. $x_{ij,w}$ counts the number of primary and backup paths that use wavelength w on link (i, j), and λ_{ij} counts the number of wavelengths used on link (i, j). Recall that we assume single-fiber links.

$$x_{ij,w} = \sum_m (r^m_{ij,w} + p^m_{ij,w}) \tag{12}$$

$$u_{ij,w} \leq x_{ij,w} \tag{13}$$

$$KN(N-1)u_{ij,w} \geq x_{ij,w} \tag{14}$$

$$u_{ij,w} \in \{0,1\} \tag{15}$$

$$\lambda_{ij} \geq \sum_w u_{ij,w} \tag{16}$$

$$\lambda_{ij} \leq W \tag{17}$$

$$\tag{18}$$

6. On link-primary-sharing:
   s_{ij} is nonnegative and defined as:

$$s_{ij} \geq \sum_m \sum_w p^m_{ij,w} - 1 \tag{19}$$

$$s_{ij} \leq \sum_m \sum_w p^m_{ij,w} \tag{20}$$

4.2 ILP formulation II: Protection Maximization

After solving the ILP formulation in Section 4.1, it is guaranteed that each request m is allocated a primary with bandwidth d_m and its minimum protection requirement b_m. However, it is still possible that there are fractional wavelength resources unused in parts of the network. The second step is then to optimally allocate the residual capacity to the connections so that some if not all the requests can obtain better protection than their minimum requirements. In addition to the path and wavelength indicator variables, the new input variable here is:

- c_m: capacity assigned to the backup path of request m.

Objective: *Protection Optimization:* As stated before, we use $c_m - b_m$ to indicate the quality of the protection, where $b_m \leq c_m \leq d_m$. w^p_m is the weight assigned to the request m.

$$max \sum_m (w^p_m \times (c_m - b_m)) \tag{21}$$

Constraints: On wavelength capacity variables, with primary and backup capacities aggregated:

$$\sum_m (d_m \times P^m_{ij,w} + c_m \times R^m_{ij,w}) \leq C \tag{22}$$

$$b_m \leq c_m \leq d_m \tag{23}$$

4.3 ILP Numerical results

We use CPLEX Linear Optimizer 7.0 [19] to solve the two ILP formulations developed above. The experiments are performed on a 10-node network topology with 14 bidirectional links.

Experiment I: For the first experiment, we use the traffic matrix shown in Table 1, which consists of 23 randomly generated requests. We also assume that each link has a single fiber that carries 2 wavelengths. As presented in the study in [3], with full protection, 33 wavelength-links are needed for carrying this traffic. We present the detailed solution here in Table 2. As can be seen, although 2 wavelengths are used in the network, wavelength 2 is only used by two requests on their primary paths. As a result, wavelength 2 is not fully utilized on those corresponding links.

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	12	1	0	0	0	0	0
2	1	0	0	0	0	0	0	0	0	12
3	0	3	0	0	0	0	0	0	0	0
4	0	0	0	0	3	1	0	3	12	12
5	0	0	0	0	0	0	0	0	1	0
6	0	0	3	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	3+1	0
8	1	0	12(2)	0	0	0	1	0	0	0
9	0	3	0	0	12	3(2)	0	0	0	0
10	3	0	0	0	0	0	0	0	0	0

Table 1. Traffic Matrix for the 10-node-14-link network: 23 requests.

For partial protection, the minimum backup capacity required for each connection is defined as follows.

$$b_m = \lceil c_m \times P_{ratio} \rceil \tag{24}$$

where P_{ratio}, referred as the *protection ratio*, is the minimum protection bandwidth guaranteed to each connection.

In this experiment, $P_{ratio} = 0.6$. The paths and the wavelengths selected are given in Table 3. With partial protection, a total of 28 wavelength-links are required. Further, only one wavelength is used in the network. Note that some of the requests are fully protected or are provided with capacity greater than their minimum requirement.

Experiment II: For the second experiment, 50 requests were randomly generated as shown in Table 4. When the number of wavelengths per link is 3, there is no solution for full protection ($P_{ratio} = 1$). When the protection ratio is reduced to 0.5 ($P_{ratio} = 0.5$), ILP-I (*resource minimization*) gives a solution of 59 wavelength-links with all backup paths given their minimum capacity of 6. Based on the results obtained from *resource minimization*, we performed

s-d	Primary Path	Backup Path
pair	Path(wave)(cap)	Path(wave)(cap)
9-2	9-10-8-5-1-2 (w_1) (3)	9-7-6-2 (w_1) (3)
3-2	3-2 (w_1) (3)	3-4-7-6-2 (w_1) (3)
7-9	7-9 (w_1) (3)	7-8-10-9 (w_1) (3)
8-7	8-7 (w_1) (1)	8-6-7 (w_1) (1)
9-6	9-7-6 (w_1) (3)	9-10-8-6 (w_1) (3)
2-1	2-1 (w_1) (1)	2-6-1 (w_1) (1)
1-4	1-6-7-4 (w_1) (12)	1-2-3-4 (w_1) (12)
4-9	4-7-9 (w_1) (12)	4-3-2-6-8-10-9 (w_1) (12)
10-1	10-9-7-6-1 (w_1) (3)	10-8-5-1 (w_1) (3)
4-8	4-7-8 (w_1) (3)	4-3-2-6-8 (w_1) (3)
4-5	4-7-8-5 (w_1) (3)	4-3-2-1-5 (w_1) (3)
8-1	8-5-1 (w_1) (1)	8-6-1 (w_1) (1)
9-5	9-7-8-5 (w_1) (12)	9-10-8-6-1-5 (w_1) (12)
5-9	5-8-7-9 (w_1) (1)	5-1-6-8-10-9 (w_1) (1)
8-3	8-7-4-3 (w_2) (12)	8-6-2-3 (w_1) (12)
7-9	7-9 (w_1) (1)	7-8-10-9 (w_1) (1)
2-10	2-6-8-10 (w_1) (12)	2-3-4-7-9-10 (w_1) (12)
9-6	9-7-6 (w_1) (3)	9-10-8-6 (w_1) (3)
4-6	4-7-6 (w_1) (1)	4-3-2-6 (w_1) (1)
6-3	6-2-3 (w_2) (3)	6-7-4-3 (w_1) (3)
8-3	8-6-2-3 (w_1) (12)	8-7-4-3 (w_1) (12)
1-5	1-5 (w_1) (1)	1-6-8-5 (w_1) (1)
4-10	4-7-8-10 (w_1) (12)	4-3-2-6-7-9-10 (w_1) (12)

Table 2. Solution with full protection: 33 wavelength links are needed.

s-d	Primary Path			Backup Path		
pair	Path	*w*	*cap*	Path	*w*	*cap*
9-2	9-7-6-2	w_1	3	9-10-8-5-1-2	w_1	**3**
3-2	3-2	w_1	3	3-4-7-6-2	w_1	**3**
7-9	7-9	w_1	3	7-8-10-9	w_1	**3**
8-7	8-7	w_1	1	8-6-7	w_1	**1**
9-6	9-10-8-6	w_1	3	9-7-6	w_1	**3**
2-1	2-1	w_1	1	2-6-1	w_1	**1**
1-4	1-2-3-4	w_1	12	1-6-7-4	w_1	**12**
4-9	4-7-9	w_1	12	4-3-2-6-8-10-9	w_1	8
10-1	10-9-7-6-1	w_1	3	10-8-5-1	w_1	**3**
4-8	4-7-8	w_1	3	4-3-2-6-8	w_1	2
4-5	4-7-8-5	w_1	3	4-3-2-1-5	w_1	2
8-1	8-5-1	w_1	1	8-6-1	w_1	**1**
9-5	9-7-8-5	w_1	12	9-10-8-6-1-5	w_1	**12**
5-9	5-8-7-9	w_1	1	5-1-6-8-10-9	w_1	**1**
8-3	8-6-2-3	w_1	12	8-7-4-3	w_1	8
7-9	7-9	w_1	1	7-8-10-9	w_1	**1**
2-10	2-6-8-10	w_1	12	2-3-4-7-9-10	w_1	**9**
9-6	9-7-6	w_1	3	9-10-8-6	w_1	**3**
4-6	4-7-6	w_1	1	4-3-2-6	w_1	**1**
6-3	6-2-3	w_1	3	6-7-4-3	w_1	**3**
8-3	8-7-4-3	w_1	12	8-6-2-3	w_1	**12**
1-5	1-5	w_1	1	1-6-8-5	w_1	**1**
4-10	4-7-8-10	w_1	12	4-3-2-6-7-9-10	w_1	**12**

Table 3. Solution with partial protection ($P_{ratio} = 0.6$): 28 wavelength-links are needed.

protection maximization to try and distribute the residual capacity among the backup paths. The results show that some of the requests were able to obtain full protection when the residual capacity was optimally distributed. The connection requests that obtained full protection are shown in Table 5.

5 Design for dynamic traffic

The two-phase ILP formulation presented in Section 4 is designed for use with a static traffic model. The formulation on resource minimization subproblem can be viewed as a general version of the ILP formulation proposed in [3] which has been shown to be impractical for use with larger networks that have dynamic traffic demands. This section deals with an algorithm that can be used for partial protection design in WDM grooming networks with dynamic traffic patterns.

For the dynamic traffic scenario, the network topology and the number of wavelengths per link are provided. Connection requests arrive to the network based on a stochastic process. Each request specifies the primary bandwidth and the minimum protection bandwidth. The network attempts to provision each connection request based on the current network resource availability. The goal is to minimize the connection blocking probability, i.e. maximize the number of admitted connections. The system performance is determined by several factors including routing, wavelength assignment, grooming policy and grooming capabilities of the nodes. In the following sections, we present our proposed mechanisms for handling dynamic traffic demands.

5.1 Shortest-available-least-congested routing

We use the two-phase design to solve the partial protection problem to the dynamic case too, wherein *resource minimization* is achieved with the *shortest-available* routing strategy for primary path allocation, and *protection maximization* is realized by looking for the *least-congested route* as the backup path. If the capacity of a path p on wavelength w is the minimum free capacity available in w on each link of p, the least congested path is the one with maximum free capacity on one or more of its wavelengths. In case of a tie among the wavelengths, the FIRST-FIT algorithm is used to select one.

The network topology is represented by a graph $G = G(V,E)$ where, V and E refer to the nodes and links in

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	12	12	0	12	0	0	12
2	0	0	0	12	0	0	0	0	0	12(2)
3	12(2)	12	0	0	12	12(2)	0	12	12(2)	0
4	0	12	0	0	0	0	12	12	12	12
5	12(2)	0	0	0	0	12	12(2)	0	0	0
6	0	0	12	12	0	0	0	12(2)	12(2)	0
7	0	0	0	12	0	0	0	0	12(3)	12
8	12	12	12	0	0	0	12	0	0	0
9	0	0	12(2)	0	0	0	0	0	0	0
10	12	0	12(2)	12	0	12	12	0	12	0

Table 4. Traffic Matrix for the 10-node-14-link network: 50 requests. $12(i)$ indicates that there are i requests of OC-12 for the $s-d$ pair.

s-d	Primary Path			Backup Path		
pair	Path	*w*	*cap*	Path	*w*	*cap*
10-9	9-7-6-2	w_3	12	10-8-7-9	w_2	**12**
7-10	7-9-10	w_1	12	7-8-10	w_1	**12**
8-1	8-6-1	w_2	12	8-5-1	w_1	**12**
6-8	6-8	w_1	12	6-7-8	w_3	**12**
1-7	1-6-7	w_1	12	1-5-8-7	w_3	**12**
6-3	6-2-3	w_1	12	6-7-4-3	w_3	**12**
3-5	3-2-1-5	w_3	12	3-4-7-8-5	w_1	**12**

Table 5. Solution with partial protection ($P_{ratio} = 0.5$): Connection requests that achieved full protection after protection maximization.

the network, respectively. The path establishment for an incoming connection m between source s and destination d, is explained in Algorithm 1.

The capacity reserved on the backup path (b_{sd}) is min(e_m, d_m). The main idea of this design is to give higher priority to path-length when selecting a primary path, and higher priority to path-capacity when choosing the backup path. This would minimize the resources used for allocation of primary paths and maximize the bandwidth allocated to protection paths. Searching for a backup path in the reduced graph with the primary path removed guarantees that the backup path is link-disjoint with respect to the primary path.

5.2 Simulation Model

We conducted simulations for a 10-node 14-link network topology and the 20-node 32-link ARPANET topology, with $W = 16$ wavelengths per link. Here, we only present results from the ARPANET topology, since similar trends were seen for the other topology.

Session request arrivals at each node is modeled as a

```
Shortest-available-least-congested($s, d, d_m, b_m$)

  $s$: source for request $m$
  $d$: destination for request $m$
  $d_m$: primary bandwidth required for connection $m$.
  $b_m$: minimum protection bandwidth required for connection $m$.
  STEP 1. Compute $k$ alternate paths between $s$ and $d$ as candidate routes for the primary (denote this set $P$).
  STEP 2. Select the shortest available path $p_{sd} (p_{sd} \in P)$ that has the required bandwidth $d_m$, as the primary for $m$.
  if no such path exists then
    Connection blocked due to primary blocking. Return FAILURE
  end if
  STEP 3. Remove all the links $l_{sd} (l_{sd} \in p_{sd})$ to form the reduced graph $G^{'}(V, E^{'})$ where $E^{'} = E - \{l_{sd}\}$.
  STEP 4. Find $b$ alternate paths in $G^{'}$ that at least have a bandwidth of $b_m$. Denote this set as $B$.
  if $B$ is empty then
    Delete $p_{sd}$ from the candidate path list $P$.
    if $P$ is empty then
      Connection blocked due to backup blocking. Return FAILURE.
    else
      Go to STEP 2.
    end if
  end if
  STEP 5. Select the least congested path in $B$ as the backup for $p_{sd}$. Denote this $b_{sd}$, and the backup capacity available on $b_{sd}$ as $e_m$. Return $p_{sd}$, $b_{sd}$ and $e_m$.
```

Algorithm 1: The Shortest-available-least-congested Routing Algorithm.

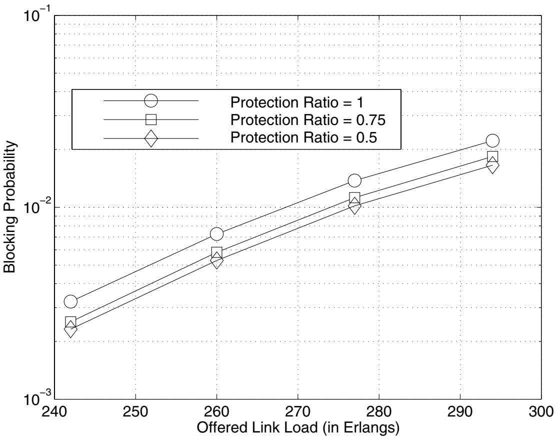
Poisson process with rate λ; the destination of each request is selected from the set of all other nodes based on a uniform distribution. Session durations are negative exponentially distributed with a mean of $1/\mu$. Hence, the Erlang load offered to a node is $\rho = \lambda/\mu$. The offered link load is calculated as $\rho_l = (N \times h/E)\rho$ where h is the average hop-length in the network. All wavelengths are assumed to have the same capacity of OC-48 (2.488 Gbps). The bandwidth requested by incoming connections takes values of OC-3, OC-12 or OC-24 and their distribution follows a ratio denoted by $(r_3 : r_{12} : r_{24})$. The probability that an incoming connection would request OC-3 is given by $r_3/(r_3 + r_{12} + r_{24})$ and so on. For instance, if the bandwidth requests are uniformly distributed among the three granularities, the ratio would be 1:1:1. For the primary paths, we choose $k = 3$ (i.e., 3 alternate paths) and for backups, we choose $b = 3$ (i.e., 3 candidate paths for backup).

For each system parameter combination, simulations were run with 10 different random number seeds with each run having 1 million connection requests. The values plotted here represent the average of the 10 simulation runs.

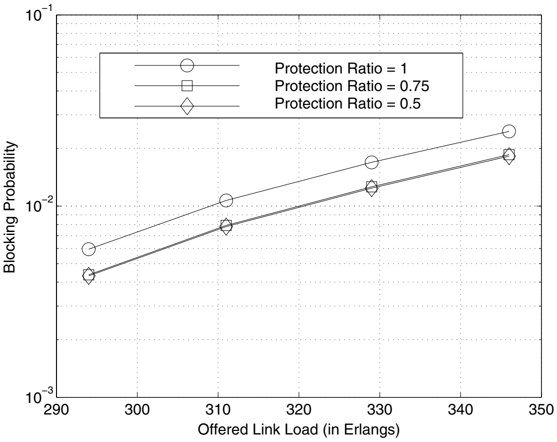
5.3 Performance Evaluation

We first quantify the effect of providing partial protection on the blocking performance of the network. Figure 1(a) plots the blocking probability for varying link loads (ρ_l) for the case when the bandwidth requests of connections are distributed in the ratio 1:3:4. Figure 1(b) presents the case when the bandwidth requests are distributed in the ratio 3:3:4. The values chosen for P_{ratio} vary between 0.5 and 1, which are respectively equivalent to 50% and 100% protection bandwidth. As seen in the figures, the blocking probability reduces with reduction in protection ratio and increases with increase in load. This is expected since with lower protection bandwidth requirements, more residual capacity is likely to be available for use, allowing more connections to be established. This also shows that the proposed algorithm utilizes the residual capacity effectively by selecting the least congested route for the backups. For instance, assume that we wish to operate the system with a maximum blocking probability of 10^{-2}. From Figure 1(b), the maximum possible load for this case is seen to be approximately 309 Erlangs and 320 Erlangs for $P = 1.0$ and $P = 0.75$ respectively.

Figure 2 presents the per-granularity blocking performance for connections with bandwidth requests of OC-12 and OC-24 for the ratio 1:3:4. Connections requesting OC-3 bandwidth did not have any blocking. The figure shows that, when the protection ratio reduces, the blocking performance of connections that require OC-12 worsens while that of connections requiring OC-24 improves. In earlier work [16], it was observed that higher granularity connections often faced higher blocking probability. However, our results here show that the reverse is possible using partial protection. For example, the blocking probability for OC-12 connections increases from 0.000007 to 0.000014 for load value of 260 Erlangs; while it reduces for OC-24 connections from 0.007248 to 0.005270. Thus, this mechanism could play a significant role in providing fairness to the blocking performance of different bandwidth classes. A similar trend is seen for the 3:3:4 case and is not included here due to lack of space.



(a) *Capacity requests distributed in the ratio 1:3:4*



(b) *Capacity requests distributed in the ratio 3:3:4*

Figure 1. Blocking performance vs. load for ARPANET topology.

Figure 3 presents the percentage of connections that were provided full protection for varying protection ratios and load, for the ratio of 1:3:4. Note that with $P_{ratio} = 1$, connections are only accepted if they can be given full protection and hence, all accepted connections will have full protection. With decrease in protection guarantees, not all connections achieve full protection but as seen, more than 99% of the connections achieve full protection at all loads, even when connections are only guaranteed 50% protection bandwidth ($P_{ratio} = 0.5$).

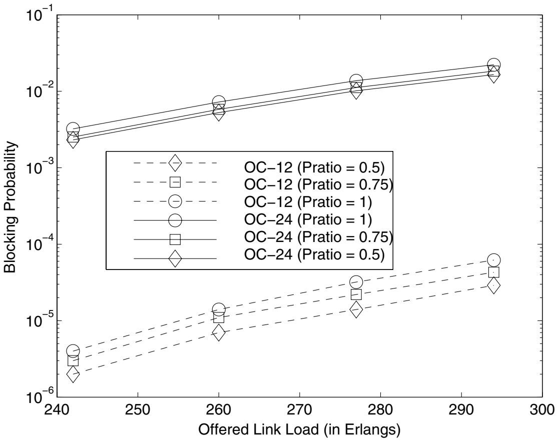


Figure 2. Blocking performance of individual bandwidth classes vs. load for the case when connection bandwidth requests are distributed in the ratio 1:3:4.

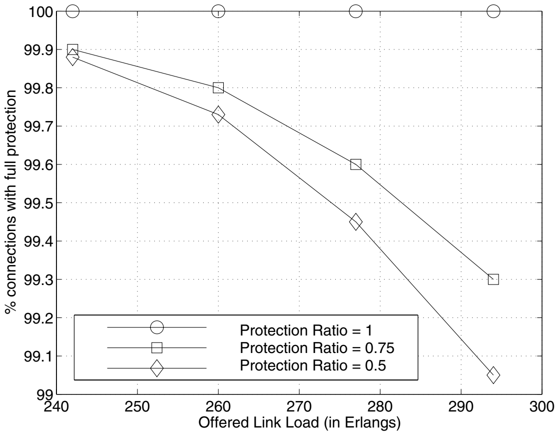


Figure 3. Percentage of connections that received full protection vs. load for the case when connection bandwidth requests are distributed in the ratio 1:3:4.

LOAD (IN ERLANGS)	P−RATIO	PRIMARY CAPACITY (OC−1 EQUIVALENT)	BACKUP CAPACITY (OC−1 EQUIVALENT)
294	1.0	1.395E+07	1.395E+07
	0.75	1.399E+07	1.398E+07
	0.5	1.399E+07	1.398E+07
	1.0	1.384E+07	1.384E+07
311	0.75	1.391E+07	1.389E+07
	0.5	1.391E+07	1.390E+07
329	1.0	1.369E+07	1.369E+07
	0.75	1.379E+07	1.377E+07
	0.5	1.380E+07	1.378E+07
346	1.0	1.350E+07	1.350E+07
	0.75	1.365E+07	1.361E+07
	0.5	1.366E+07	1.362E+07

Table 6. Total primary and backup capacity vs. protection ratio for different link loads.

Table 6 presents the total capacity assigned to primaries and backups for various loads and protection ratios for the ratio 3:3:4. At low loads, the network is able to provide full protection to most of the connections and hence, the total primary and backup capacity are similar for all protection ratios. However, at moderate to high loads, the network is not only able to accept more connections with lesser protection guarantees but also better utilize the network resources and provide more primary and backup capacities than the case when the network guarantees full protection to all connections.

6 Conclusions

In this paper, we studied the problem of enabling partial protection in the design of survivable WDM grooming networks. With partial protection, the backup capacity reserved for a connection would be a fraction of the primary bandwidth requirement. The objective of our design was to admit as many connections as possible with minimum protection requirements before exploiting more wavelengths for additional protection capacity. We considered networks with static and dynamic traffic demands. For static traffic, we decomposed the design problem into two subproblems, namely *resource minimization* and *protection maximization*, and formulated each as an integer linear programming optimization problem. We used the two-phase design idea for dynamic traffic scenario, and proposed a routing scheme called *shortest-available-least-congested* algorithm to deal with the problem of routing partially protected requests in dynamically groomed networks. The results for both static and dynamic traffic scenarios show that partial protection is a useful compromise when the network resources are limited and hence not sufficient to provide full protection for every request.

References

[1] L. Choy. Virtual concatenation tutorial: enhancing SONET/SDH networks for data transport. *Journal on Optical Networking*, 1(1), Jan. 2002.

[2] M. Clouqueur and W. Grover. Mesh-restorable networks with enhanced dual-failure restorability properties. In *Proc. SPIE OPTICOMM*, Boston, MA, July 2002.

[3] J. Fang and A. K. Somani. Enabling Subwavelength Level Traffic Grooming in Survivable WDM Optical Network Design. In *Proc. IEEE GLOBECOM*, pages 2761–2766, San Francisco, CA, Dec. 2003.

[4] O. Gerstel and G. Sasaki. Quality of protection (QoP): a quantitative unifying paradigm to protection service grades. In *Proc. SPIE OPTICOMM*, pages 12–23, Denver, CO, Aug. 2001.

[5] W. D. Grover. *Mesh-based Survivable Networks*. Prentice-Hall, 2003.

[6] A. Lardies, R. Gupta, and R. A. Patterson. Traffic grooming in a multi-layer network. *Optical Networks Magazine*, 2(3):91–99, May 2001.

[7] G. Mohan and A. K. Somani. Routing dependable connections with specified failure restoration guarantees. In *Proc. IEEE INFOCOM*, pages 1761–1770, Tel-Aviv, Israel, Apr. 2000.

[8] C. Ou, K. Zhu, and *et al.* Traffic grooming for survivable WDM networks - shared protection. *IEEE Journal on Selected Areas in Communications*, pages 1367–1383, November 2003.

[9] C. Ou, K. Zhu, and *et al.* Traffic grooming for survivable WDM networks - dedicated protection. *Journal of Optical Networking*, pages 50–74, January 2004.

[10] R. Ramaswami and K. N. Sivarajan. *Optical Networks: A Practical Perspective*. Morgan Kaufmann, 2 edition, 2001.

[11] M. Sivakumar, R. Shenai, and K. Sivalingam. A survey of grooming techniques for optical wavelength division multiplexed WDM networks. Technical report, University of Maryland, Baltimore County, 2003.

[12] M. Sivakumar, R. Shenai, and K. M. Sivalingam. Protection and restoration for optical WDM networks: A survey. In K. Sivalingam and S. Subramaniam, editors, *Emerging Optical Network Technologies*. Springer Publishers, 2004.

[13] M. Sivakumar and S. Subramaniam. A Performance Evaluation of Time Switching in TDM Wavelength Routing Networks. In *Proc. Broadband Optical Networking Symposium*, San Jose, CA, Oct. 2004.

[14] K. Sivalingam and S. Subramaniam, editors. *Emerging Optical Network Technologies*. Springer Publishers, Boston, MA, 2004.

[15] S. Thiagarajan and A. Somani. Traffic Grooming for Survivable WDM Mesh Networks. In *Proc. SPIE OPTICOMM*, pages 54–65, Denver, CO, Aug. 2001.

[16] S. Thiagarajan and A. K. Somani. Capacity Fairness of WDM Networks with Grooming Capabilities. *SPIE Optical Networks Magazine*, 2(3):24–32, May/June 2001.

[17] C. Vijayasaradhi and C. S. R. Murthy. Routing differentiated reliable connections in single and multi-fiber WDM optical networks. In *Proc. SPIE OPTICOMM*, pages 24–35, Denver, CO, Aug. 2001.

[18] B. Wen and K. Sivalingam. Routing, wavelength and time-slot assignment in time division multiplexed wavelength-routed optical WDM networks. In *Proc. IEEE INFOCOM*, pages 1442–1450, New York, NY, June 2002.

[19] www.cplex.com. ILOG CPLEX: High-performance software for mathematical programming and optimization, 2005.

[20] Y. Ye, C. Assi, S. Dixit, and M. A. Ali. A simple dynamic integrated provisoning/protected scheme in IP over WDM networks. *IEEE Communications Magazine*, pages 174–182, Nov. 2001.

[21] K. Zhu and B. Mukherjee. A review of traffic grooming in WDM optical networks: Architectures and challenges. *Optical Networks Magazine*, 4(2), Apr. 2003.

[22] K. Zhu and B. Mukherjee. Survivable traffic grooming in WDM mesh networks. In *Proc. of IEEE OFC*, Atlanta, GA, Mar. 2003.