

# Backup Resource Pooling in $(M : N)^n$ Fault Recovery Schemes in GMPLS Optical Networks

Kotikalapudi Sriram\*, David W. Griffith, SuKyoung Lee, and Nada T. Golmie

National Institute of Standards and Technology (NIST)  
100 Bureau Drive, Stop 8920 Gaithersburg, MD, 20899, USA.

\*Email: ksriram@nist.gov

## ABSTRACT

In resilient optical networks, there is a tradeoff between the amount of resources allocated for protection versus the probability that a failed working path can not be recovered, known as protection blocking probability. Often the network topology permits multiple protected groups of working paths (WPs) to share protection bandwidth and other network resources. The Common Control and Measurement Plane (CCAMP) working group in the IETF has defined an  $(M : N)^n$  shared recovery scheme, in which defined  $n$  WP groups each consisting of  $N$  WPs and  $M$  backup paths (BPs) share some or all of the BP resources. In this paper, we present an analytical model that predicts protection blocking probability as a function of BP resource sharing for this shared recovery scheme. We also propose an algorithm that efficiently manages BP resources while doing protection assignments. We provide numerical results that highlight the benefits and tradeoffs involved. Our analytical model can assist in providing engineering guidelines to service providers so that they can effectively allocate resources and manage protection and restoration in their networks.

**Keywords:** Performance, Protection, Restoration,  $(M : N)^n$ , GMPLS, CCAMP

## 1. INTRODUCTION

There is a growing awareness on the part of major service providers and carriers that optical networks must be as resilient as possible to failures and sabotage, while using resources efficiently. This requires careful planning and allocation of network resources (e.g., wavelengths, regenerators, switching ports, etc.) for protection purposes. Most failure events are localized and correlated; the classic example is “backhoe fade,” in which a co-located group of fibers or fiber bundles is severed. Because of this, it is possible to collect multiple disjoint working paths into a protection group that shares a pool of recovery resources. Because local, correlated failures will affect only one of the group’s working paths, the backup resources can be shared without reducing the availability of a backup path when a failure occurs.

Recently, vendors of IP/WDM switches have started to provide restoration for optical WANs by using the GMPLS protocol with the functions of group protection and sharing.<sup>1</sup> The IETF is continuing to extend GMPLS protocols to support additional capabilities. In particular, the Common Control and Measurement Plane (CCAMP) working group has recently proposed a framework for an  $(M : N)^n$  shared recovery scheme,<sup>2</sup> which operates in the following way. Each of the  $n$   $(M : N)$  protection groups in an  $(M : N)^n$  recovery scheme has  $N$  working paths (WPs) and a total of  $M$  backup paths (BPs). Some of the  $M$  BPs in each  $(M : N)$  group are shared with other protection groups while the rest are dedicated only to that particular group. Implementation details, such as the degree of sharing and other management issues, are left to individual vendors. The  $n$  protection groups in a  $(M : N)^n$  recovery scheme can, in general, each have a different degree of QoS in terms of the level of protection that they support. This can be done by using different values of  $M$  and  $N$  in different groups while the number of shared BPs is fixed at  $K$ . With this arrangement, we can allow the various protection groups to operate at different (protection related) bandwidth/resource efficiency levels. In this paper, we consider only the case where  $M$  and  $N$  are the same for all the protection groups that compose a given recovery scheme. In designing such a scheme, we need to consider the tradeoff between restorability and the limitation of network

---

This research was partially supported by the Laboratory for Telecommunications Sciences (LTS), the Defense Advanced Research Projects Agency (DARPA), and the National Communications System (NCS).

resources. Intelligent resource sharing across protection groups is necessary for providing high protection levels with economical use of resources. While it is clear that increasing the degree of sharing reduces the amount of restoration overhead while increasing the probability of blocking in the event of multiple uncorrelated failures, a qualitative assessment of the issues associated with creating a particular recovery scheme can provide important insights to carriers, service providers, and customers.

As the Internet evolves to be more robust with higher availability and resilience, the underlying IP over WDM (or GMPLS) network has to support both mission-critical services and traditional best-effort Internet services over a common infrastructure. It could guarantee the recovery of all the lightpaths carrying mission-critical services by using dedicated backup resources (e.g., 1+1,1:1 protection). Several recent studies have focused on the trend in higher guarantees for recovery of even best-effort Internet traffic<sup>3-6</sup>; these studies evaluate the performance of known recovery schemes or attempt to integrate the different schemes across multiple layers, to support heterogeneous traffic with hierarchical protection levels. These approaches adopt several rather simple schemes rather than exploit the functions of group protection and resource sharing which are integral to GMPLS. Other recent work, such as,<sup>7</sup> has considered the performance of shared mesh recovery schemes relative to that of 1+1 protection, but they have considered only the general case where unlimited sharing of protection bandwidth is allowed as long as the working parents are SRLG-disjoint. Some other recent papers<sup>8,9</sup> have studied (1:1) protection with sharing, and they have focused on the routing efficiency and provisioning. We aim to investigate the effect of the degree of sharing on the overall restorability of the WPs that use the resource pool, in order to provide design guidelines for  $(M : N)^n$  recovery schemes.

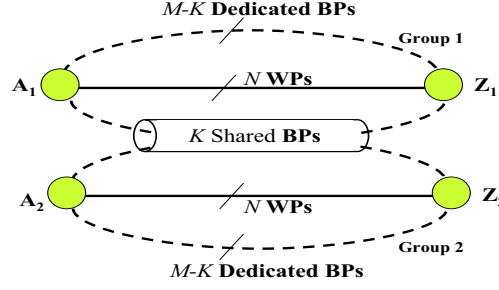
In this paper, we present an analytical model for prediction of the protection blocking probability for  $(M : N)^n$  shared recovery schemes. Our analytic model aims to help the network operator to utilize network resources efficiently while protecting the largest possible number of connections. We also propose an algorithm to efficiently manage BPs while doing protection assignments. The set of BPs that are dedicated to a particular protection group would be used before the shared BPs to recover from failures. When a protection group's dedicated set of  $M - K$  BPs is exhausted, any additional BP requests would overflow to the group of  $K$  shared BPs. The sharing mechanism allows the network to respond to uncorrelated failures while economically using the protection resources. The model can assist in providing engineering guidelines to service providers for resource allocation and management of protection and restoration. Further, we demonstrate that when the optimum resource management policy is not used, the lower bound is tight, and hence is a good approximation for the protection blocking probability. The model can be used to predict performance and manage tradeoffs associated with various system parameters values.

In Section 2, we present a detailed description of the  $(M : N)^n$  recovery scheme and some algorithms for management of BPs. In Section 3, we present the analytical models for upper and lower bounds for the probability of protection blocking. In Section 4, we consider wavelength conversion for increasing the effective size of the shared protection resource pool. In Section 5, we present and discuss numerical results showing various performance tradeoffs. Finally, in Section 6, we provide conclusions and discuss future extensions of this work.

## 2. DESIGN AND OPERATION OF THE $(M : N)^n$ PROTECTION SCHEME

$M : N$  protection has been defined for both span recovery and edge-to-edge path recovery. In this scheme,  $N$  working paths (or spans) are protected by  $M$  protection paths (or spans). The  $M + N$  paths/spans are collectively known as  $M : N$  protection group. Low priority traffic, known as Extra Traffic, may be carried over the protection resources during regular (non-failure) operations. If a failure occurs, GMPLS signaling is used to inform the span or path end-points of the failure event. The endpoints carry out an exchange of messages that switch normal traffic from the affected working spans or paths to a set of protection spans or paths. Obviously, if more than  $M$  working paths fail, at least one will be denied use of the group's protection resources. This phenomenon is known as protection blocking.

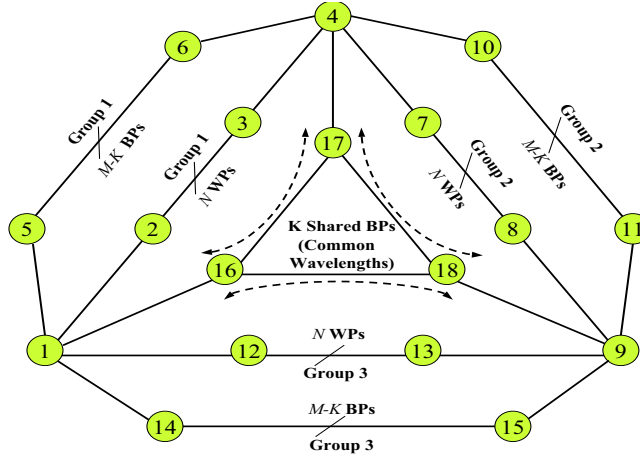
The basic description of the  $(M : N)^n$  recovery scheme can be simply stated as  $(M : N)$  protection for  $n$  groups of WPs, wherein some or all of the BPs may be shared across the  $n$  groups. As shown in Figure 1, there can be  $K$  shared BPs between two groups of  $N$  WPs and  $M - K$  dedicated BPs for each group. Here,  $K$  can vary from 0 (no sharing) to  $M$  (100% sharing). Thus, the arrangement of Figure 1 is an example of  $(M : N)^2$  protection.



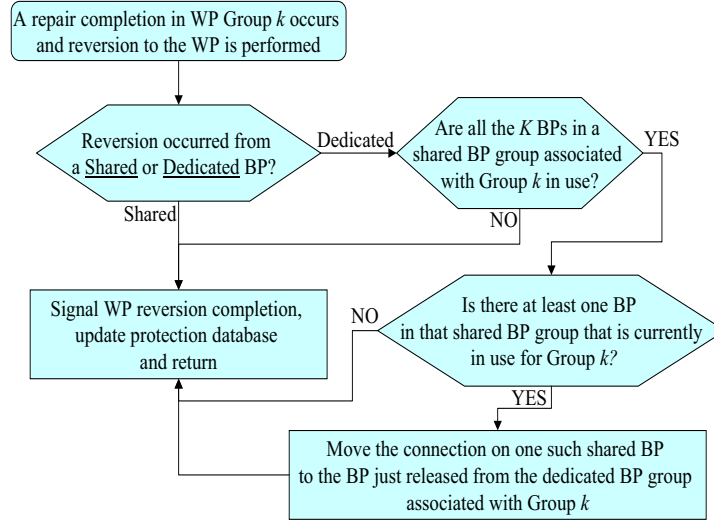
**Figure 1.** An illustration of  $(M : N)^2$  protection

For the case of  $(M : N)^n$  with  $n \geq 3$ , there can be a similar arrangement with  $M - K$  dedicated BPs for each of the  $n$  groups while  $K$  BPs are in a shared common pool of BPs. In Figure 2, we illustrate a network topology with  $(M : N)^3$  protection arrangement. If it is assumed that no wavelength conversion is permissible in the central part of the network at nodes 16, 17, 18 where  $K$  shared BPs are shown. This restricts the number of shared BPs to exactly  $K$ . Thus for this network, the  $(M : N)^3$  recovery scheme can be precisely represented as three WP groups with  $K$  shared BPs and  $M - K$  dedicated BPs per group (just a straightforward extension of Figure 1 for  $n = 3$ ). It may be noted here that there are some subtleties in the BP sharing related to the  $(M : N)^n$  recovery scheme for  $n \geq 3$ ; these subtleties arise due to wavelength conversion capability in the shared backup paths or a network topology that may permit wavelength reuse in the shared backup paths. We will address these subtleties in Section 4.

When a protection request arrives from Group  $k$ , a dedicated BPs is allocated (if available), and a shared BP is allocated only if all the dedicated BPs for Group  $k$  are exhausted at the time of request arrival. Figure 3 is the description of an algorithm for release of BPs from the shared group in the event that a BP from a corresponding dedicated group is relinquished. Sometimes a BP from the dedicated set of BPs for Group  $k$  may be relinquished while all the shared BPs are occupied. In this case, it is desirable from the service provider's point of view to move an existing BP allocation of Group  $k$  in the shared group (if any) to the just released dedicated BP. This results in lower protection blocking and lower network cost. The algorithm of Figure 3 is generally applicable for the general case, i.e., any values of  $M$ ,  $N$  and  $n$ .



**Figure 2.** An example topology for  $(M : N)^3$



**Figure 3.** Algorithm for release of shared backup paths

### 3. PERFORMANCE ANALYSIS OF $(M : N)^N$ SCHEME WITH PROTECTION RESOURCE SHARING

We focus on an analytical model for the  $(M : N)^n$  recovery scheme with  $M - K$  dedicated BPs per group of  $N$  WPs and  $K$  shared BPs across all  $n$  groups of WPs. To describe the analytical model, let us define the following parameters:

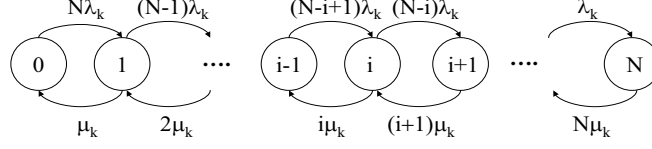
- $n$ : number of protection groups that have shared (overlapping) BPs
- $N$ : number of WPs in each of the  $n$  protection groups
- $M$ : total number of BPs available for the  $N$  working paths in each protection group
- $M - K$ : number of dedicated BPs available for the  $N$  working paths in each of the  $n$  protection groups
- $K$ : number of shared BPs available for the  $n$  protection groups
- $\lambda_k$ : rate of transition of each WP in Group  $k$  from working to failed state (per hour)
- $\mu_k$ : rate of repair of a failed WP in Group  $k$  (per hour)
- $f_k$ : probability that a given WP in Group  $k$  is failed and waiting for repair

The bandwidth efficiency,  $E$ , for the  $(M : N)^n$  recovery scheme in consideration is

$$E = \frac{nN}{n[N + (M - K)] + K}. \quad (1)$$

$E$  is the ratio of the total working bandwidth to the total working and protection bandwidth assigned to the  $(M : N)^n$  recovery scheme. In computing  $E$  here, we have assumed that the WPs and BPs are all approximately of the same length for the protection groups in consideration. However, the expression for  $E$  can be modified to include varying path lengths for the WPs and BPs. Additional simulation and analytical results, including such modification, are presented in a follow-up report.<sup>10</sup>

The failure probability,  $f_k$ , for a WP in Group  $k$  is given by,  $f_k = \frac{\lambda_k}{\lambda_k + \mu_k}$  ( $k = 1, 2, \dots, n$ ) where there are  $n$  protection groups. Each WP is assumed to be disjoint from all other WPs within each of the protection



**Figure 4.** State transition diagram for a protection group  $k$

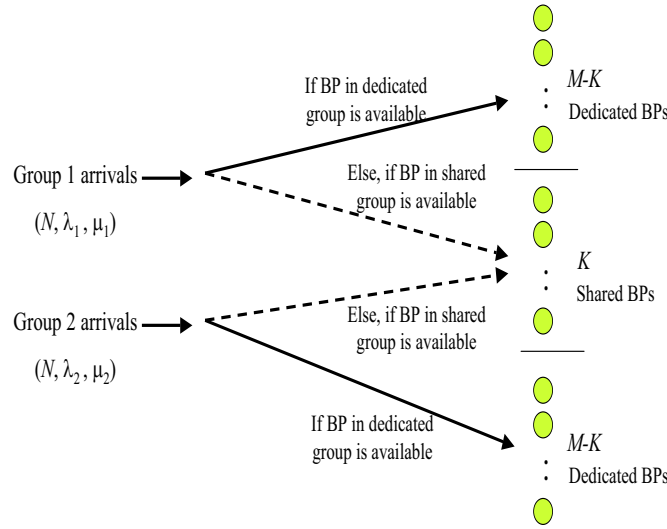
groups, and the transitions between working and failed states are assumed to follow independent exponential time distributions. Therefore, the state transition diagram in Figure 4 describes the state transitions for the two groups ( $k=1,2$ ). The independent failure assumption is valid if the WPs are SRLG disjoint or for the case when failures occur due to independent wavelength channel faults. The general case of correlated failures within WP groups is addressed in.<sup>10</sup> The probability of being in state  $i_k$  for Group  $k$  (i.e.,  $k$  of the  $N$  WPs are currently in failed state) is given by the binomial distribution as follows:

$$q_{k,i_k} = \binom{N}{i_k} (f_k)^{i_k} (1 - f_k)^{N-i_k}, \quad i_k = 0, 1, \dots, N \quad (2)$$

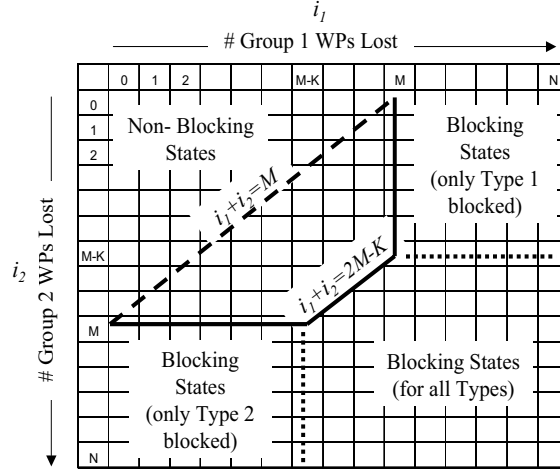
We assume that the failures in the  $n$  Groups of WPs are independent of each other. Hence, the probability that combined state of Groups  $1, 2, \dots, n$  is  $\bar{i} = (i_1, i_2, \dots, i_n)$  is given by

$$p(\bar{i}) = \prod_{k=1}^n q_{k,i_k} \quad k = 1, 2, \dots, n \quad (3)$$

The stochastic model for protection blocking analysis can be explained based on Figures 5 and 6. These figures are for the case of  $n = 2$ . The generalization to higher values of  $n$  will be discussed later. From Figure 5, we can surmise that no blocking occurs if both groups 1 and 2 are in states  $i_k \leq M$  with the added constraint of  $i_1 + i_2 \leq M$ . When these constraints are met, a BP request is successfully accommodated whether it is from group 1 or group 2. Similarly, blocking of arrival(s) from either group occurs if both groups are in states  $i_k > M$  with the added constraint that  $i_1 + i_2 > 2M - K$ . Further, it can be seen that blocking occurs only for group 1



**Figure 5.** Stochastic model for  $(M : N)^2$  protection



**Figure 6.** Enumeration of states for the protection blocking analysis

arrivals if the system is in a state where  $i_1 > M$  and  $i_2 \leq M - K$ . Similarly, blocking occurs only for group 2 arrivals if the system is in a state where  $i_2 > M$  and  $i_1 \leq M - K$ . Figure 6 shows the various blocking/non-blocking regions identified above. There is an additional set of states that lie within the trapezoid in Figure 6. We have talked about all the regions in Figure 6 except the trapezoidal area, which we will now proceed to discuss.

The trapezoidal area in Figure 6 needs consideration only if the algorithm of Figure 3 for reallocation of BPs is not used. In this study, we assume that this algorithm is used and hence all the states inside and on the boundary of the trapezoidal region of the state-space in Figure 6 are non-blocking. However, we provide upper and lower bounds for the protection blocking probability for the case when the algorithm of Figure 3 is not used. For the case without use of the algorithm, we derive the upper bound by considering that the non-blocking set of states are defined only by  $i_k \leq M$  with the added constraint of  $i_1 + i_2 \leq M$ . Under this assumption, every state in the trapezoidal region is a blocking state. The protection blocking probability that we derive for the case where the algorithm is used serves as a tight lower bound for the case when the algorithm is not used. The tightness of this lower bound (for the case where the reallocation algorithm is not used) is partly due to the mean repair time being much smaller than the mean time before failure; hence, the probability is rather small that the shared  $K$  BPs are all in use while there is availability of dedicated BPs for either group. To further understand this, recall that a shared BP is allocated only when all the dedicated BPs for a group have been exhausted. Overall, it is to be expected that the probability is rather small for either WP group to be using several shared BPs while its own dedicated BP group has multiple vacancies.

Considering the case of  $n = 2$ ,  $i_1 + i_2$  is the total offered number of requests for BP allocation when the system is in state  $(i_1, i_2)$ . It may be noted that the requests arrive one at a time when a WP failure event happens, and also depart (i.e., release a BP) one at a time when a WP repair event happens. In other words, the model does not allow multiple failures or repairs to occur at a given instant in time. If the system is in state  $(i_1, i_2)$ ,  $i_1 + i_2$  cumulative requests have been received and are still waiting for repair. Let  $R_o$  represent the mean offered number of requests:

$$R_o = \sum_{i_1=0}^N \sum_{i_2=0}^N (i_1 + i_2) p(i_1, i_2) = \sum_{i_1=0}^N i_1 q_{1,i_1} + \sum_{i_2=0}^N i_2 q_{2,i_2} = (f_1 + f_2)N \quad (4)$$

With the help of the enumeration of blocking states as shown in Figure 6, we can write the equation for the average number of blocked backup path requests as follows, by summing over each of the regions where blocking

occurs:

$$\begin{aligned}
R_B = & \sum_{i_1=M}^N \sum_{i_2=0}^{M-K-1} a_1(i_1, i_2) p(i_1, i_2) + \sum_{i_1=0}^{M-K-1} \sum_{i_2=M}^N a_2(i_1, i_2) p(i_1, i_2) \\
& + \sum_{\substack{i_1=M-K \\ i_1+i_2 \geq 2M-K}}^N \sum_{\substack{i_2=M-K \\ i_1+i_2 \geq 2M-K}}^N (a_1(i_1, i_2) + a_2(i_1, i_2) + K) p(i_1, i_2),
\end{aligned} \tag{5}$$

where  $a_k(\bar{i}) = i_k - M$  for  $k = 1, 2$ . From equations 4 and 5, the blocking probability is

$$P_B = \frac{R_B}{R_o}. \tag{6}$$

For the case without use of the reallocation algorithm, the above is a tight lower bound as explained before, and the upper bound is derived as follows. The upper bound on average number of blocked backup path requests is

$$R_{BU} = \sum_{\substack{i_1=0 \\ i_1+i_2 \geq M}}^N \sum_{\substack{i_2=0 \\ i_1+i_2 \geq M}}^N (i_1 + i_2 - M) p(i_1, i_2), \tag{7}$$

where  $p(i_1, i_2)$  is given by equation 3 when  $n = 2$ . Then, the upper bound on the blocking probability can be expressed as

$$P_{BU} = \frac{R_{BU}}{R_o}. \tag{8}$$

This upper bound,  $P_{BU}$ , is primarily of theoretical interest and gives the worst case blocking probability. This value would arise only if several shared BPs used by Groups  $k$  were consistently not relinquished due to excessively large repair times while several of the dedicated BPs of the same group have long been relinquished and are unused. However, the probability of such occurrence is very low. The blocking probability as given by above equations 5 and 6 is the main result of this analysis.

Now we proceed to provide the expressions for the probability of protection blocking for  $n = 3$ . Once this is understood, the same for  $n \geq 4$  can be easily derived. For the case of  $n = 3$ , the enumeration of various blocking states (similar to Figure 6 for  $n = 2$ ) is provided using Table 1. The logic for this table is fundamentally similar to that used in explaining Figure 6. In this case, there are regions of state-space where (1) requests from none of the 3 groups are blocked, (2) requests from only one of the 3 groups are blocked, (3) requests from only two of the 3 groups are blocked, and (4) requests from any of the 3 groups are blocked. Seven possible regions of state-space where blocking occurs are enumerated and their corresponding numbers of blocked requests for each state  $\bar{i} = (i_1, i_2, i_3)$  are listed in Table 1. The entire state-space is given by  $\bar{i} = \{(i_1, i_2, i_3); 0 \leq i_1 \leq N, 0 \leq i_2 \leq N, 0 \leq i_3 \leq N\}$ .

Now with the help of the enumeration of blocking states as shown in Table 1 and  $p(\bar{i})$  as given by equation 3 for  $n = 3$ , we can write the equation for the average number of blocked requests for backup paths as follows:

$$\begin{aligned}
R_B = & \sum_{i_1=M}^N \sum_{i_2=0}^{M-K-1} \sum_{i_3=0}^{M-K-1} a_1(\bar{i}) p(\bar{i}) + \sum_{i_1=0}^{M-K-1} \sum_{i_2=M}^N \sum_{i_3=0}^{M-K-1} a_2(\bar{i}) p(\bar{i}) \\
& + \sum_{i_1=0}^{M-K-1} \sum_{i_2=0}^{M-K-1} \sum_{i_3=M}^N a_3(\bar{i}) p(\bar{i}) + \sum_{\substack{i_1=M-K \\ i_1+i_2 \geq 2M-K}}^N \sum_{\substack{i_2=M-K \\ i_1+i_2 \geq 2M-K}}^N \sum_{i_3=0}^{M-K-1} (a_1(\bar{i}) + a_2(\bar{i}) + K) p(\bar{i}) \\
& + \sum_{\substack{i_1=0 \\ i_2+i_3 \geq 2M-K}}^{M-K-1} \sum_{\substack{i_2=M-K \\ i_2+i_3 \geq 2M-K}}^N \sum_{\substack{i_3=M-K \\ i_2+i_3 \geq 2M-K}}^N (a_2(\bar{i}) + a_3(\bar{i}) + K) p(\bar{i}) + \sum_{i_1=M-K}^N \sum_{\substack{i_2=0 \\ i_1+i_3 \geq 2M-K}}^{M-K-1} \sum_{\substack{i_3=M-K \\ i_1+i_3 \geq 2M-K}}^N (a_1(\bar{i}) + a_3(\bar{i}) + K) p(\bar{i}) \\
& + \sum_{\substack{i_1=M-K \\ i_1+i_2+i_3 \geq 3M-2K}}^N \sum_{\substack{i_2=M-K \\ i_1+i_2+i_3 \geq 3M-2K}}^N \sum_{\substack{i_3=M-K \\ i_1+i_2+i_3 \geq 3M-2K}}^N (a_1(\bar{i}) + a_2(\bar{i}) + a_3(\bar{i}) + 2K) p(\bar{i}).
\end{aligned} \tag{9}$$

**Table 1.** Affected groups and number of blocked backup path requests ( $n = 3$ )

Affected groups	Condition satisfied by state vector $(i_1, i_2, i_3)$	Number of blocked requests for backup paths
Group 1 only	$i_1 \geq M; i_2, i_3 < M - K$	$a_1(\vec{i}) = i_1 - M$
Group 2 only	$i_2 \geq M; i_1, i_3 < M - K$	$a_2(\vec{i}) = i_2 - M$
Group 3 only	$i_3 \geq M; i_1, i_2 < M - K$	$a_3(\vec{i}) = i_3 - M$
Group 1 or 2 only	$i_1, i_2 \geq M - K; i_3 < M - K \ni i_1 + i_2 \geq 2M - K$	$a_1(\vec{i}) + a_2(\vec{i}) + K$
Group 2 or 3 only	$i_2, i_3 \geq M - K; i_1 < M - K \ni i_2 + i_3 \geq 2M - K$	$a_2(\vec{i}) + a_3(\vec{i}) + K$
Group 1 or 3 only	$i_1, i_3 \geq M - K; i_2 < M - K \ni i_1 + i_3 \geq 2M - K$	$a_1(\vec{i}) + a_3(\vec{i}) + K$
All groups	$i_1, i_2, i_3 \geq M - K \ni i_1 + i_2 + i_3 \geq 3M - 2K$	$a_1(\vec{i}) + a_2(\vec{i}) + a_3(\vec{i}) + 2K$

The probability,  $P_B$ , of requests for BPs blocked is given by

$$P_B = \frac{R_B}{R_o}, \quad (10)$$

where  $R_o = \sum_{i_1=0}^N \sum_{i_2=0}^N \sum_{i_3=0}^N (i_1 + i_2 + i_3) p(\vec{i}) = (f_1 + f_2 + f_3)N$ .

For the case without use of the reallocation algorithm (as per flowchart of Figure 3), the above is a tight lower bound on blocking probability for  $n = 3$  (see explanation given earlier in this section for  $n = 2$ ), and the upper bound is

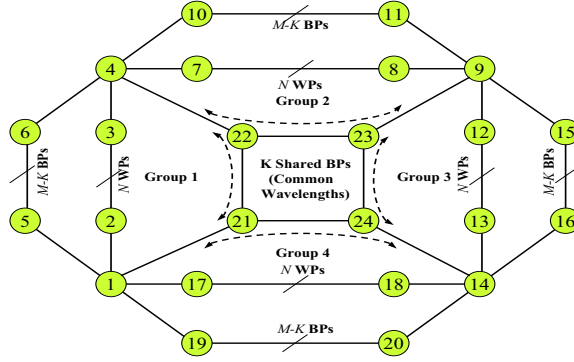
$$P_{BU} = \frac{\sum_{i_1=0}^N \sum_{i_2=0}^N \sum_{i_3=0}^N (i_1 + i_2 + i_3 - M) p(\vec{i})}{R_o}. \quad (11)$$

The generalization of protection blocking probability for any larger  $n$  (i.e.,  $n \geq 3$ ) follows quite easily by reapplying, for the larger  $n$ , the logic and steps used in the construction of Table 1, and then the derivations follow similar to those for  $n = 3$ .

#### 4. NETWORK TOPOLOGIES WITH WAVELENGTH REUSE

In Section 2, we described the  $(M : N)^n$  recovery scheme for a class of applicable network topologies, in which there is symmetric sharing of protection resources. This class of topologies is characterized by  $n$  WP groups having exactly  $K$  BPs in a shared pool and there are  $M - K$  BPs that are dedicated for each WP group. This model is generally applicable for the case of  $n = 2$  and for  $n \geq 3$  without wavelength conversion (see Section 2). However, some subtleties arise due to (1) the existence of wavelength conversion (WC) capability on the shared backup paths, or (2) a network topology that may permit wavelength reuse in the portion of the network that contains the shared backup paths.

Let us reconsider the network configuration in Figure 2 of Section 2. Now let us assume that, in this network with  $(M : N)^3$  protection, wavelength conversion is allowed at one of the three interior nodes (i.e., nodes 16, 17, and 18) over which the shared BPs are setup. In this case, each group has  $M - K$  dedicated and  $K$  shared BPs but the total number of shared BPs across the three groups of WPs can be in the range of  $K$  to  $1.5K$ , depending on the way they are used. If one of the protection groups has many successive failures and it consumes all  $K$  shared BPs as a result, then the other two groups have no shared BPs available. Thus the limit on the usable number of BPs in this mode of usage is  $K$ . On the other hand, if each protection group uses exactly  $K/2$  shared BPs, then a total of  $1.5K$  shared BPs are usable for the same topology. The larger amount of shared BPs is realized due to suitable use of wavelength conversion and reuse at one of the three interior nodes (namely, nodes 16, 17 and 18). For example, let us say  $K = 6$  with wavelengths 1 through 6 available for the shared BPs. In one viable example, Group 1 can use wavelengths 1,3,5 over path 1-16-17-4, Group 2 can use wavelengths 2,4,6 over path 4-17-18-9, and simultaneously Group 3 can use wavelengths 2,4,6 from node 1 to node 16 and convert these to wavelengths 1,3,5 at node 16 and thus use wavelengths 1,3,5 from node 16 to node 9 via node 18. For this



**Figure 7.** An example topology for  $(M : N)^4$

form of usage with wavelength conversion, the total number of shared BPs adds up to 9 ( $= 1.5K$ ). In another example of usage, a total of 8 ( $> K$  but  $< 1.5K$ ) shared BPs would be available for the three groups collectively if one group uses 4 while the other two groups use 2 each (again with the help of WC at one of nodes 16, 17 or 18). Thus, with WC capability, the size of the shared BP pool available to the three groups is effectively larger than  $K$ . Accordingly, the overall blocking probability for protection requests for the network of Figure 2 is lower (for a given  $K$ ) if wavelength conversion is permitted in the subnetwork containing the BPs as compared to the case when wavelength conversion is not permitted.

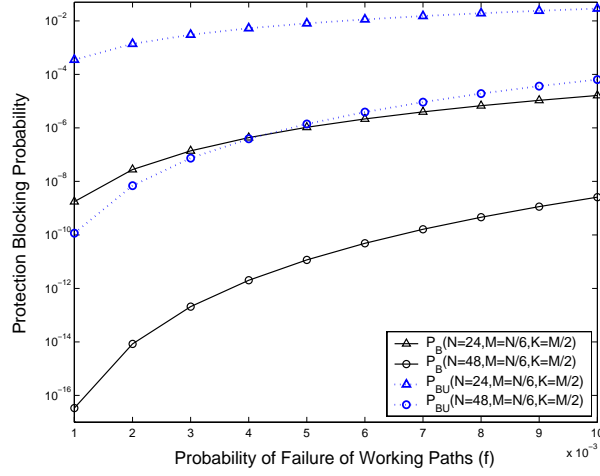
Let us consider another network configuration as shown in Figure 7 with  $(M : N)^4$  protection. In this case, wavelength reuse on shared BPs is possible between Groups 1 and 3 as well as between Groups 2 and 4 simply because network topology permits the two subsets of shared BPs to be disjoint. So if Groups 1 and 3 each use  $K$  wavelengths for shared BPs, they would use  $2K$  BPs in total. The same situation exists if Groups 2 and 4 use  $K$  shared BPs each. Groups 1 and 3 can each use the same  $K - j$  wavelengths while Groups 2 and 4 each can use the remaining  $j$  wavelengths, again resulting in a total of  $2K$  BPs in use. However, any two adjacent groups (e.g., Groups 1 and 2, Groups 2 and 3) can only share up to  $K$  BPs or wavelengths between them. We propose that our model for  $(M : N)^n$  protection as described in Section 3 can be applied to this case with an effective BP pool size,  $K_{\text{eff}}$ , which can be derived based on the relative arrival rates of requests from different WP groups. We defer further study on the subject of effective values of  $K$  to a future paper.

The next section includes some numerical results where the benefits of wavelength conversion are shown quantitatively in terms of lower protection blocking probability.

## 5. NUMERICAL RESULTS AND DISCUSSION

To provide numerical examples based on our analytical model, we vary various system or traffic parameter values and discuss the impact of those variations on the protection blocking probability. We also examine the effect of various architecture/algorithmic choices such as topology and use of wavelength conversion. To generate the results, we assume that all protection groups are statistically identical and independent so that the average durations of failures and the average BP request inter-arrival times are identical for all groups. Thus, the failure probability  $f_k = f$  for all groups ( $k = 1, 2, \dots, n$ ). It is a modeling assumption that there is negligible probability of a backup path failure while being used to provide protection. We consider two different values of the working path failure probability,  $f$ , are considered, namely, 0.005 and 0.01 (except in Figure 8). Assuming a mean repair time of 4 hours, these failure probabilities correspond to approximately one failure per WP every 33 days and every 16.5 days, respectively.

In Figure 8, we consider the  $(M : N)^2$  scheme and plot the protection blocking probability for a range of values of  $f$  which corresponds to the load offered to the BP resource pool. Two different values of  $N$  are considered, with  $M = N/6$  and  $K = M/2$ . Figure 8 also shows the upper bound on the protection blocking probability,  $P_{BU}$ , for the case when the BP reallocation algorithm (see flowchart of Figure 3) is not used. For the case when this algorithm is used, the blocking probability is just  $P_B$  as shown in the figure. As we showed in

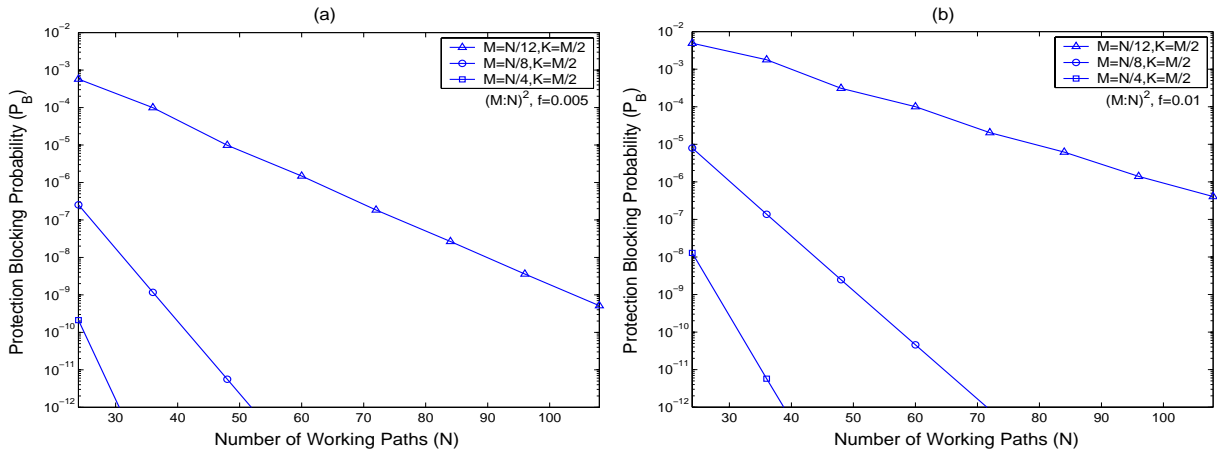


**Figure 8.** Protection blocking probability under varying offered load

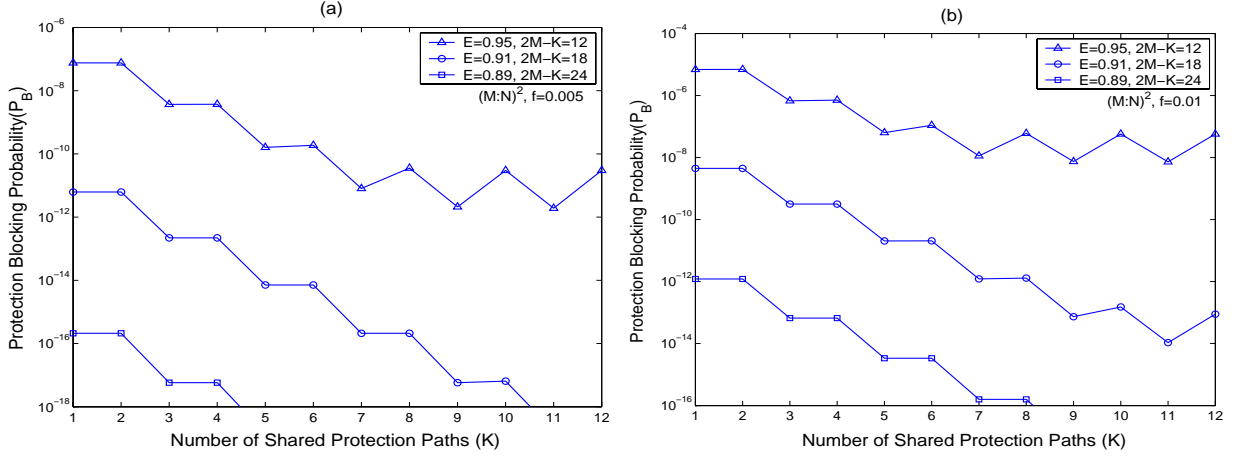
Section 3,  $P_B$  serves as a tight lower bound when the algorithm is not used. In the remainder of the numerical examples, we assume the use of the algorithm and hence use only  $P_B$  (and not  $P_{BU}$ ) to discuss the performance of the  $(M : N)^n$  recovery scheme for various cases of interest.

We plot the protection blocking probability as a function of  $N$  in Figure 9(a), wherein the sensitivity to the values of  $M$  and  $K$  is shown for  $f = 0.005$ . In this example, the numbers of dedicated BPs,  $M - K$ , and shared BPs,  $K$ , for protection are equal ( $M - K = K = N/2i$ ,  $i = 4, 8, 12$ ) and increase proportionately with  $N$ . The protection blocking probability shows steep drops (orders of magnitude) as a function of increasing number of BPs for a fixed  $N$ . In Figure 9(b),  $f$  has been increased to 0.01 from 0.005. For increased values of WP failure probability (0.01 vs. 0.005), the protection blocking probability typically goes up by more than an order of magnitude, but the same trends hold as in Figure 9(a).

It is generally of interest to study the sensitivity of protection blocking behavior to protection group and backup pool size while the bandwidth efficiency is held fixed. The bandwidth efficiency,  $E$ , of the  $(M : N)^n$  scheme was given in equation 1. In Figures 10(a) and 10(b), we vary the value of shared number of BPs,  $K$ , while keeping  $E$  constant. This is done by choosing  $M$  for each  $K$  in such a way that  $2M - K$  remains a constant (approximately). The multiplicative factor of two prevents our keeping  $2M - K$  exactly constant over all values

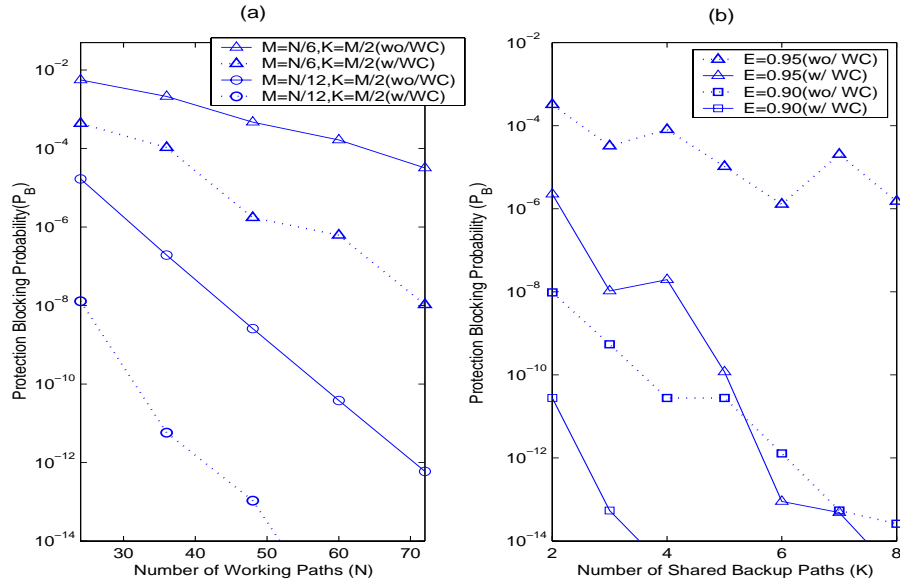


**Figure 9.** Protection blocking probability vs.  $N$ : (a) for  $f = 0.005$  and (b) for  $f = 0.01$



**Figure 10.** Protection blocking probability vs.  $K$ : (a) for  $f = 0.005$  and (b) for  $f = 0.01$

of  $K$ . For slight changes in efficiency values ( $E$  ranging from 0.95 to 0.91 to 0.89), the protection blocking probability dramatically drops by orders of magnitude. This is expected because what seem to be slight drops in  $E$  are actually associated with significant increases in values of  $K$ , and as we have seen in Section 3,  $P_B$  is sensitive to the number of shared BPs,  $K$ . Comparing Figures 10(a) and 10(b) we note that, for an increased value of WP failure probability (0.01 vs. 0.005), protection blocking probability typically increases by more than an order of magnitude (as observed before for Figures 9(a) and 9(b)). In Figures 11 (a) and (b), we show numerical results for the case of  $(M:N)^3$  scheme. The results are based on equations 9 and 10. The illustrative network topology used here is that of Figure 2. We consider the following two cases: (1) without the use of wavelength conversion (WC) and (2) with the use of WC. The case without WC is not topology dependent but the case with WC is somewhat topology dependent (see discussions in Section 4). The effective shared BP pool size becomes greater than  $K$  for the case where WC is used, and hence the values of  $P_B$  are smaller for this case than for the case where WC is not used, while all other parameters are equal (see Figures 11 (a) and (b)). The



**Figure 11.** (a) Protection blocking probability vs.  $K$  ( $f = 0.01, (M:N)^3$ ) (b) Protection blocking probability vs.  $K$  ( $f = 0.01, (M:N)^3$ )

wavy nature of the plots (in Figures 10(a), 10(b), 11(a) and 11(b)) is due to the rounding effects in getting the nearest integer values for  $M$  while  $K$  is varied and  $E$  is approximately held constant. Figures 11 (a) and (b) indicate that enabling WC in the shared BPs results in reductions in  $P_B$  by two orders of magnitude or better as compared to the case without WC, even though the number of wavelengths allocated to shared BPs is the same,  $K$ , in both cases.

## 6. CONCLUSIONS AND FUTURE WORK

We have presented an analytical model that describes the performance of  $(M : N)^n$  shared recovery schemes. The model provides a general expression for the probability of protection blocking, which is useful for network sizing and traffic engineering. It also allows the network operator to understand the effect of various network and traffic parameters on protection performance. With the help of numerical studies, we have computed the performance sensitivities to the number of backup paths (shared and/or dedicated) as well as to failure rates of working paths. We have also presented an algorithm to manage BP resources so that the restoration blocking probability is minimized. The numerical results show that there is a significant benefit to allowing wavelength conversion in the portion of the network that contains the shared BPs so that the allocated wavelengths can be used more efficiently to effectively provide a larger number of BPs than otherwise possible.

Network simulation studies of the  $(M : N)^n$  scheme with protection resource sharing, including the effect of correlated failures within WP groups, will be reported in a forthcoming report.<sup>10</sup> This work can be also further extended to include the possibility of BP failures while they are in service protecting failed WPs. Although those are rare events, they may be included in the model for greater accuracy. We will also use simulations of a dynamic restoration and provisioning environment to capture additional scenarios and extensions. This model in its present form can be used even for the case when protection is provided not on a per path basis but per span or per lightpath segment. For the latter cases, the model can be applied span-wise or segment-wise. The details of how this will be done are items for further study. Another item for future study is determining the extensions to GMPLS signaling protocols to support path protection with shared backup resources in a distributed routing environment.

## REFERENCES

1. J. P. Lang, and J. Drake, "Mesh Network Resiliency Using GMPLS", *Proceedings of IEEE*, vol.90, no.9, p. 1559-1564, Sep.2002.
2. D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G. Li, B. Rajagopalan, and Y. Rekhter, "Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)", *Internet Draft*, draft-papadimitriou-ccamp-gmpls-recovery-analysis-03.txt, November 2002.
3. J. Wang, L. Sahasrabudde, B. Mukherjee, "Path vs. Subpath vs. Link Restoration for Fault Management in IP-over-WDM Networks: Performance Comparisons Using GMPLS Control Signaling", *IEEE Commun. Mag.*, p. 2-9, Nov. 2002.
4. S.D. Maesschalck, D. Colle, A. Groebbens, C. Develder, I. Lievens, P. Lagasse, M. Pickavet, and P. Demeester, "Intelligent Optical Networking for Multilayer Survivability", *IEEE Commun. Mag.*, p. 42-49, Jan. 2002.
5. P. Laborci T. Cinkler, "IP over WDM Configuration with Shared Protection", *Optical Networks Magazine*, vol.3, no.5, p. 21-33, Sep/Oct. 2002.
6. A. Autenrieth, A. Kirstadter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS", *IEEE Commun. Mag.*, Jan. 2002.
7. R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S. Chaudhuri, and K. Bala, "Capacity Performance of Dynamic Provisioning in Optical Networks," *Journal of Lightwave Technology*, Vol. 19, no. 1, pp. 40-48, January 2001.
8. G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient Distributed Path Selection for Shared Restoration Connections," *Proceedings of IEEE Infocom 2002*, pp. 140-149.
9. O. Hauser, M. Kodialam, and T. V. Lakshman, "Capacity Design of Fast Path Restorable Optical Networks," *Proceedings of IEEE Infocom 2002*.
10. K. Sriram, D. W. Griffith, S. Klink, and N. Golmie, "A Network Simulation Study of Backup Resource Pooling in  $(M : N)^n$  Fault Recovery Schemes," NIST Technical Report, in preparation (2003).