A New Analytical Model of Shared Backup Path Provisioning in GMPLS Networks

SuKyoung Lee, David Griffith and N. Song

Abstract- **As GMPLS and its supporting set of protocols develop into a viable control plane for optical networks, an important function that they will need to support will be the protection and restoration function that has been a major feature of legacy optical networks. A network with a robust set of protection and restoration mechanisms will be able to support data traffic while allowing faster recovery from failures than can be obtained using layer 3 rerouting. Several models have been proposed for protection with GMPLS using shared backup paths. This previous work has not investigated the effect on recovery time critical to the service or the number of backup paths that are required to meet a desired level of performance. Using both recovery time and recovery blocking probability, we have developed a new analytic model for GMPLS-based recovery in $M:N$ protection groups. Furthermore, we show that smaller backup paths can be reserved by capturing the effect of multiple failures in the case of $M:N$ shared protection with revertive mode in an optical network with a GMPLS control plane.**

Keywords—**GMPLS, Shared Backup Path, Multiple-failure**

I. Introduction

Protection of traffic is growing in importance and especially recovery schemes that can provide fast restoration at layers above the optical layer. MPLS-based recovery has been pointed out as strong candidate in this area and may be motivated by the notion that there are inherent limitations to improving the recovery times of current routing algorithms. Since GMPLS is likely to be the technology of choice in the future IP-based transport network, it is necessary that MPLS be able to provide protection and restoration of traffic. Furthermore, a protection mechanism using GMPLS could enable IP traffic to be put directly over WDM optical channels, without an intervening SONET layer, while still emulating SONET resiliency features. This would facilitate the construction of IP-over-WDM networks. For restoration in IP over WDM network, even if link-layer restoration such as mesh restoration is recommended to achieve low latencies, IP level restoration, based on GMPLS recovery is employed in the event that link-layer restoration fails.

It is generally desirable to have protection and restoration schemes that are bandwidth efficient. In GMPLS-based recovery, it is important to increase network reliability by providing necessary resources in time as well as enabling a fast response to faults. In this paper, a new backup path provisioning scheme is proposed in order to reflect this tradeoff between resource utilization and reliability upon GMPLS-based recovery.

There have been many proposals in the IETF (Internet Engineering Task Force) to standardize methods of signaling and provisioning GMPLS networks to achieve protection against failures. However, to support the routing of backup paths for $M:N$ path protection, new extensions must be added to the current GMPLS routing extensions. In particular, there must be a mechanism to advertise backup path bandwidth and processing rules must be defined for bandwidth accounting when backup path requests arrive at a node. Therefore, we investigate an analytic model of restoration time in the case of $M:N$ shared protection. Also, we analyze the restoration request failure probability numerically for the case that multiple faults occur upon a path in $M:N$ protection with revertive mode. Furthermore, in our scheme, a protection priority could be used as a differentiating mechanism for premium services that require high reliability. That is, guaranteed services could be pro-

This work was supported, in part, by the National Institute of Standards and Technology (NIST), the Advanced R&E Activity (ARDA), the Laboratory for Telecommunications Sciences (LTS) MENTER project, the Defense Advanced Research Projects Agency (DARPA) Fault Tolerant Networks (FTN) program, and the National Communications System (NCS).

vided in terms of continuity of services maintained by GMPLS-based recovery around network failures.

II. GMPLS Signaling and QoS Support

The main objective of any recovery scheme is to operate in a cost-effective manner while minimizing service interruptions to the customer. Providing a high degree of reliability (or equivalently, a low probability of service disruptions) is expensive and tends not to scale well. For this reason, any carrier that operates a wide-area optical backbone network needs to be able to support a variety of service classes in which the degree of protection is tied to the price of the service [1]. For instance, [2] proposed a multi-tiered service model in which the basic (least expensive) service receives no protection support, while more expensive service options feature some various combinations of routing around areas with a relatively high probability of network failure and dedicating backup paths for automatic failover switching of the data stream.

There are mainly two levels of recovery mechanisms: rerouting and protection switching. While rerouting is defined as the real-time establishment of appropriate resources to recover affected traffic, protection switching involves the establishment of pre-calculated replacement resources. In the latter scheme, the pre-calculated backup paths can be either shared or dedicated:

- 1+1: As dedicated facility recovery, traffic is passing through both the working and backup paths. Upon failure detection, the traffic on the backup path becomes the active traffic. Therefore, the resources on both the backup and the working paths are fully reserved. It is the fastest protection switched recovery mechanism, but also the most expensive in terms of resources.
- $1:N$: As semi-dedicated facility recovery, N working paths are protected using a backup path. the traffic is rerouted to the spare resource after the failure has occurred. $1:1$ protection is a special case of $1:N$ protection.
- $M:N$: As shared facility restoration, M protection entities are shared among N working resources. The most common notion $M:N$ path protection is to route N node-disjoint primary paths and pre-establish M backup paths that are node disjoint from the primary paths.

In this paper, we concentrate on the $M:N$ shared path protection method. Using GMPLS signaling [3], this method is done by indicating the LSP (Label Switched Path) is of type Secondary in the protection field of the Generalized Label Request. Backup LSPs are used for fast switchover when primary LSPs fail. Although the resources for the backup LSPs are pre-allocated, lower priority traffic may use the resources with the caveat that the lower priority traffic will be preempted if the primary LSP fails. If lower priority traffic is using resources along the secondary LSPs, the end nodes may need to be notified of the failure in order to complete the switchover. Therefore, even if the backup path is pre-signaled, it takes time to switch the traffic to the backup path allowing preemption. Actually, in a differentiated services scenario, the need for preemption becomes more compelling. Moreover, in the emerging optical internetworking architectures, where some protection and restoration functions may be migrated from the optical layer to data network elements such as gigabit and terabit LSRs (label switching routers) to reduce costs, preemptive strategies can be used to reduce the possible chances of rerouting for high priority traffic trunks under failure conditions.

GMPLS introduces a new Notify message to the signaling protocols so that LSP failures can be reported to the ingress or some other node responsible for error recovery. The setup of the primary LSP should indicate that the LSP initiator and terminator wish to receive Notify messages using the Notify Request object (RSVP Notify message) [4]. Upon receipt of the Notify messages, the source and destination nodes switch the traffic from the primary LSP to the backup path. Notify messages may provide faster error reporting than the normal error notifications since they can contain information about multiple failed LSPs, and because they are sent direct to the consumer. Note that this function is initially only specified for RSVP-TE signaling and not CR-LDP. The Protection Object is also proposed to indicate specific protection attributes of an LSP [4] and [?].

Moreover, for protection, backup path management and proper management of bandwidth on the backup path is necessary. In our scheme, the management system would control each path differently in accordance

TABLE I

Protection level example

Service level	Protection plan
Gold	Dedicated protection: $1+1$, $1:1$
Silver	Shared protection: $M:N$, $1:n$
Bronze	Rerouting

with its service class maintaining the different protection resource pools. Especially, the recovery manager needs to ensure that the amount of protection resources designed for each path belonging to higher priority service is sufficient for the traffic to be protected within this service class. The priorities may be implemented for allocating shared resources under multiple failure case.

Protection bandwidth capacity could be considered as the main cost of recovery QoS. Under multiple failure case, more than one connection can claim shared resources. Thus, it is possible that a protection path may not be successfully activated when multiple and concurrent failure events occur. In this case, shared protection bandwidth capacity may be requested by more than one failed connection and the protection path can be activated only for some of them. In order to support all the connections with the failures, enough capacity can be reserved in advance. However, this reservation will result in wasting the resources in network. Therefore, it is desirable to support priority based allocation of shared resources during restoration signaling. In the proposed scheme, the protection manager allocates different capacity in accordance with the restoration failure probability requested by the service class. The class with higher priority such as real-time traffic ought to request lower restoration failure probability.

To differentiate the protection level of each path, the field Service Type (8 bits) in Generalized Label Request can be used. Similar to Service Type defined in [6], this field indicates a class of service. Thus, a carrier may specify a range of different classes of service (e.g. gold, silver, bronze) with different types of recovery plans where there could exist no recovery, 1+1 protection, shared protection and etc. as can be seen the protection level example in Table I.

III. Backup Path Provisioning

In protection, network can quickly utilize pre-provisioned backup resources for recovery from a resource failure along the working (primary) path. That is, backup path can be setup simultaneously with the primary path to guarantee fast switching to the protection path. In accordance with the level of recovery guarantee, the resources along the backup path can be exclusively deployed (dedicated path), or they can be shared among multiple backup paths. Meanwhile, at the time when the fault occurs, the network state is not static, i.e. the number of occupied backup paths and the number of faults are different. Actually, some amount of protocol signaling is required at the time of failure. This varies from simply propagating the error from the point of detection to the point of recovery, to the full signaling of the backup path. Thus, it is usually difficult to predict how much backup paths will be necessary for the shared backup path case. In spite of this difficulty, it is not desirable to use real-time (e.g. rerouting) approach for some high priority services since the approach requires time to compute the alternate path after failure is detected and hence is likely to be slower. In consideration of the tradeoff among restoration time and pre-provisioned resource, we will analyze the restoration time to provision the shared backup path efficiently before a failure happens.

In this section, we investigate the number of enough backup paths to recover the data on the working paths based on a model for the recovery signaling time. The number of attempts depends on current network status. (e.g. how many backup paths are used and if the resources are available in the backup path.)

A. Restoration Time Analysis

The time taken from the instant a link fails to the instant the backup path of a connection traversing the failed path is enabled, could be defined to be the protection-switching time for the connection. Our restoration time analysis concentrates on this protection-switching time. As soon as a failure occurs and is detected on a working path, an attempt will be made to restore the working path. We assume that the control network is reliable, i.e., does not incur message losses.

Assume that there is an infinite number of feasible backup paths $\{P_1, P_2, \ldots\}$ for attempts. The backup paths will be attempted in the order numbered until the restoration is successfully made. For the i^{th} attempt to a backup path P_i, it take time t_i to check if the path P_i is available for the restoration. And assume that these times $t_1, t_2, \ldots$ are independent and identically distributed (i.i.d.) random variables having a distribution $F_t(t)$.

Let a path with a failure need K attempts until the restoration is successfully made. That is, the first $k-1^{th}$ attempts find that the paths $P_1, P_2, \cdots$ are not available but the k^{th} attempt finds that the path P_k is available for restoration. Then the restoration time T_r, which is required for finding an available path to restore a working path with failure, is

$$T_r = t_1 + t_2 + \cdots + t_K \qquad k \geq 1 \tag{1}$$

It is also assumed that each attempt is successful with probability p, that is, each backup path is available for restoration with probability p. Thus, the expected number of attempts that will be required to activate a backup path is

$$\begin{aligned} E[K] &= \sum_{K=1}^{\infty} K(1-p)^{K-1}p \\ &= \frac{1}{p}. \end{aligned} \tag{2}$$

Since each attempt takes a random time t which is distributed according to $F_t(t)$, the expected time for each attempt is expressed as

$$E[t] = \int_0^{\infty} t \, dF_t(t). \tag{3}$$

From Eq. 2 and 3,

$$E[T_r] = E[K]E[t] \tag{4}$$

where we can apply renewal theory [7] according to the assumption that $t_1, t_2, \cdots$ are i.i.d.. For the case where t_k is exponentially distributed with mean $1/\mu$, the average T_r becomes $\frac{1}{p\mu}$ from the above Eq. 4.

Each traffic flow will have its own restoration time limit. The network QoS manager could use the result from Eq. 4 as a constraint on the requested restoration time. The average restoration time is indicative of the expected amount of data lost during a failure. That is, during the time required to activate the backup path and switch the traffic over to it, the affected connection will experience data (and revenue) losses. For example, a sudden disconnect during an active transaction in a network of ATM machines or other systems can cause uncertain states from which the end application may not recover, causing failure of the transaction. Thus, it is imperative to facilitate seamless handover of data so that information loss is minimized.

B. Number of Backup Path

To prevent excessive resource usage for backup paths, and to meet the implicit service provider requirement of improving network resource utilization so as to increase the number of potential future demands that can be protected, it is important to determine the appropriate number of backup paths to be shared.

When a failure occurs, up to K attempts will be made to find a backup path. If the K^{th} attempt fails, then the restoration attempt is considered to have failed and a new working path must be created for the customer. Thus, regardless of whether the restoration attempt succeeds, the system will spend $T_{k\leq K}$ units of time trying to set up a backup path, where

$$\begin{aligned} E[T_{k\leq K}] &= pE[t] + 2(1-p)pE[t] + \cdots \\ &+ (K-1)(1-p)^{K-2}pE[t] \\ &+ K(1-p)^{K-1}E[t] \\ &= \frac{1-(1-p)^K}{p}E[t]. \end{aligned} \tag{5}$$

As the probability of successful backup path activation, p, approaches unity, then $E[T_{k\leq K}] \to E[t]$, behaving as $E[t]/p$ for values of p near unity. Conversely, we can use L'Hôpital's Rule to show that $\lim_{p\to 0} E[T_{k\leq K}] = KE[t]$.

Suppose that as part of the SLA that the carrier has with the customer, there is an upper limit ϵ on the restoration time. This would be requested by a service class with shared backup protection (e.g. Silver class in Table I). Thus the restoration time must satisfy

$$E[T_{k\leq K}] \leq \epsilon. \tag{6}$$

Inserting InEq. 6,

$$\frac{(1-(1-p)^K)}{p}E[t] \le \epsilon. \tag{7}$$

The above InEq. can be expressed as

$$1 - \frac{\epsilon}{E[t]}p \le (1-p)^K. \tag{8}$$

Thus,

$$\frac{\ln(1-\frac{\epsilon}{E[t]}p)}{\ln(1-p)} \ge K \tag{9}$$

From InEq. 9, the minimum number of shared backup paths can be computed satisfying the requested restoration time of the service class.

Note that if $\epsilon \ge E[T_r] = E[k]E[t]$, where $E[k] = 1/p$ is the mean number of attempts required to establish a backup path, then the argument of the natural logarithm in the numerator of the upper bound in Eq. 9 will be negative. As $\epsilon \to E[T_r]$ from below, assuming that p is a constant, the upper bound on K becomes arbitrarily large. What this means in practical terms is that no limit needs to be imposed on the maximum number of backup path activation attempts if the network operator is willing to wait at least the average restoration time.

For premium services, the network operator may also want to guarantee a certain probability of restoration success in the event of a failure. In other words, we may demand that the probability of restoration failure after K attempts does not exceed some limit, δ. So we require

$$P[\text{failure}] = (1-p)^K \le \delta, \tag{10}$$

which implies that

$$K \ge \frac{\ln(\delta)}{\ln(1-p)} \tag{11}$$

must be the minimum number of restoration attempts. If we choose values for δ and ϵ such that

$$\frac{1-\delta}{p}E[t] \le \epsilon,$$

where $1-\delta$ is the probability that the restoration will succeed in K or fewer path setup attempts, then we will restrict K to lie within a range of values given by

$$\frac{\ln(\delta)}{\ln(1-p)} \le K \le \frac{\ln(1-\frac{\epsilon}{E[t]}p)}{\ln(1-p)}. \tag{12}$$

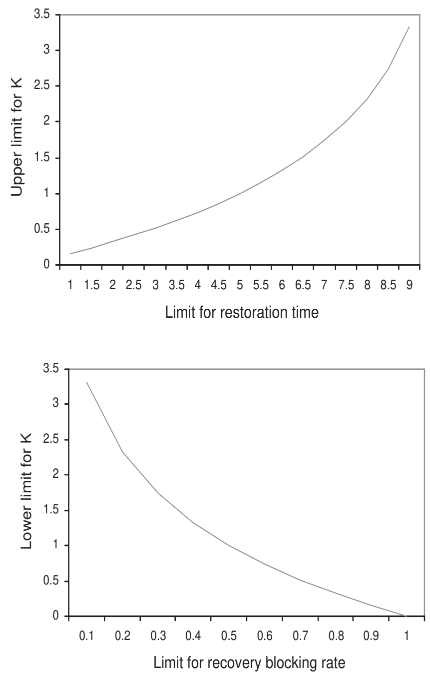

Fig. 1. Range for the number of backup paths

As can be seen in Fig. 1, ISP (Internet Service Provider)s can refer the above range in accordance with the requested QoS for recovery time and recovery blocking probability. Normally, if the customers's traffic is so critical, then one would (to meet the SLA) assign a separate (or at least shared) backup path for this particular LSP. If the network is properly designed and used, the situation where no backup LSP is available, when the primary LSP fails, should not arise. In the event a new service request comes in and a backup cannot be found (and reserved) due to bandwidth exhaustion or for whatever reason, then the request (with protection LSP) should be denied. If the customer agrees to an unprotected LSP service, then depending upon the SLA, "best effort" service in the event of a node/link failure could be provided. If the unprotected LSP service cannot be provided also, then the request for this service is also denied, and depending upon the SLA only "best effort" service may be provided.

IV. Path with Multiple Failures

In MPLS recovery, there are two modes, revertive and non-revertive. For revertive mode, traffic is automatically switched back from the recovery path to the original working path as soon as the working path recovers to a fault-free condition. In this paper, we consider n-to-m protection with revertive mode [8]. In n-to-m protection, up to n working paths are protected using m recovery paths which should be diversely routed.

We assume that a mechanism for detecting and isolating multiple failures is in place in the network. This analysis can also be applied to GMPLS protection where one of fundamentally most urgent needs is to increase the number of WDM channels considering today's growth rate of bandwidth demand.

To do the analysis, we can use some of the theoretical framework developed in [9] for detecting and isolating multiple failures in WDM networks.

A. Blocking Probability Analysis

In our model, we assume that the following paths cannot be restored to another backup path for next fault before switching back to its original working path:

- The path which has been using a recovery path since previous fault
- The path which is already in the restoration operation due to previous fault

For the two cases above, a higher-layer rerouting mechanism will be used to set up an alternate connection path. This approach is slower than the protection switching mechanism and so we use it only as a last resort. The procedure associated with the activation of a backup path is as follows:

1. A fault occurs on a working path.
2. MPLS-based recovery mechanism detects the fault.
3. Fault Indication Message is sent.
4. *if* a backup path is in use
then Perform rerouting function.
else Perform M:N protection function.

In this anaylsis, we will use the following assumptions:

- There are N backup paths and $M > N$ working paths in a $M : N$ protection domain.
- λ is the fault occurrence rate in a working path.

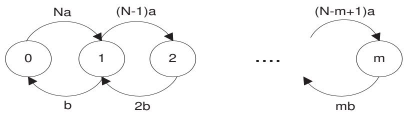

Fig. 2. State diagram for multiple failures(a=λ, b=μ)

- The time for traffic to revert from a backup path to its original working path is exponentially distributed with rate μ.
- π_i is the steady state probability that i backup paths are used. In the state diagram (Figure 2), state i corresponds to i backup paths being in use, and a transition from state i to state $i+1$ occurs with rate $(N-i)\lambda$ for $i < m$.

Let n_f be the number of restoration requests by a fault occurrence upon a working path, n_r be the number of restoration completions (the number of accepted restoration requests), n_a be the number of restoration failures because the working path is already using a recovery path, and n_b be the number of restoration failures because no backup path is available. It is clear that

$$n_f = n_r + n_a + n_b. \tag{13}$$

¿From the first assumption, the effective fault occurrence rate per working path can be defined as

$$\lambda_f = \frac{n_f - n_a}{n_f}\lambda. \tag{14}$$

This λ_f is used to determine the number of necessary backup paths, not λ. Let p_f be the restoration failure probability and p_f^* be the failure probability that excludes the blocked restoration requests due to using a recovery path. We have

$$p_f = \frac{n_b}{n_f}, \qquad p_f^* = \frac{n_b}{n_f - n_a}. \tag{15}$$

If $p_f = p_f^*$ $(n_a = 0)$ then the system can be described using the Erlang distribution, while $p_f \neq p_f^*$ $(n_a > 0)$ leads to an Engset distribution.

We derive the probability p_f^* from the state diagram in Figure 2. For $1 \leq i \leq m$, from [7],

$$\begin{aligned}\pi_i &= \frac{(N-i+1)\lambda_f}{i\mu}\pi_{i-1} \\ &= \frac{\lambda_f^i \prod_{j=1}^{i}(N-j+1)}{i!\mu^i}\pi_0\end{aligned}$$

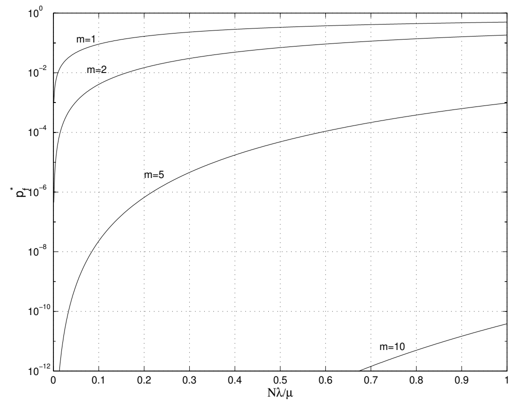

Fig. 3. Loss probabilities for Engset system with $N = 10$ for various values of m.

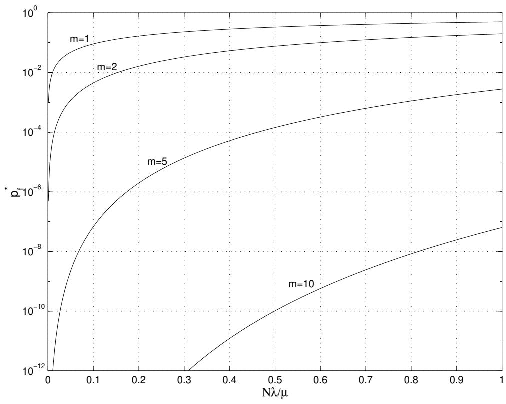

Fig. 4. Loss probabilities for Engset system with $N = 100$ for various values of m.

$$= \binom{N}{i} \left(\frac{\lambda_f}{\mu}\right)^i \pi_0. \tag{16}$$

Using the above Eq. 16 and the fact that $\pi_0 + \pi_1 + \cdots + \pi_m = 1$, the probability p_f^* can be expressed as

$$p_f^* = \pi_m = \frac{\binom{N}{m} \left(\frac{\lambda_f}{\mu}\right)^m}{\sum_{0 \le i \le m} \binom{N}{i} \left(\frac{\lambda_f}{\mu}\right)^i} \tag{17}$$

If the system can be described using the Erlang distribution, then we can compute $p_f = p_f^*$, which is the probability that an Erlang system with m states is in State m:

$$p_f = \pi_m = \frac{\rho^m/m!}{\sum_{n=0}^{m} \rho^n/n!}, . \tag{18}$$

where $\rho = \lambda/\mu$ and $\lambda = \lambda_f$.

In Figures 3 and 4 we plot the loss probabilities for $M : N$ protection groups with $N = 10$ and $N = 100$, respectively. Both probabilities are plotted versus the normalized utilization $N\lambda/\mu$, and there is little difference in the plots for small values of m. For a given number of backup paths, in order to have the loss probability be less than some maximum allowable amount, we must have $N\lambda/\mu$ less than some threshold, which can be determined from the graph. If we then increase the number of working paths in the protection group while keeping the number of backup paths fixed, we must make some additional adjustments to the network (such as reducing $1/\mu$, the average reversion time) in order to maintain the original level of performance. In this case, the required reduction in $1/\mu$ is proportional to the increase in the number of working paths.

We also develop expressions for some of the other probabilities related to the system. Defining x to be the expected number of faults that occur while the working path is still using the recovery path,

$$n_a = x n_r. \tag{19}$$

This follows from an examination of Figure 5, which shows a scenario in which the interarrival time between failures is less than the average time required to allow traffic to revert to the original working path. From the figure we see that x is the mean number of failure events per restoration period. Because λ and μ are the respective failure and restoration rates for the path, it follows that $x = \lambda/\mu$. We prove this below for the Markovian case.

If the fault occurrences form a Poisson process with rate λ and the backup path holding times for each

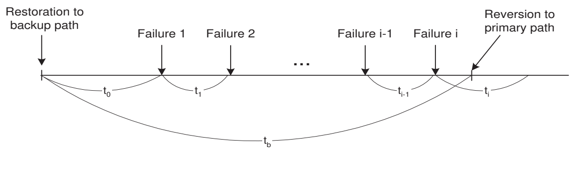

Fig. 5. Time model for multiple failures

fault are exponentially distributed with mean $1/\mu$,

$$\begin{aligned} x &= \sum_{i=1}^{\infty} i \Pr\{T_{i-1} \le t_b < T_{i-1} + t_i\} \\ &= \sum_{i=1}^{\infty} i \int_{t_i=0}^{\infty} \lambda e^{-\lambda t_i} \int_{t=0}^{\infty} \frac{(\lambda t)^{i-1}}{(i-1)!} \lambda e^{-\lambda t} \int_{t_b=t}^{t+t_i} \mu e^{-\mu t_b} \\ &\quad dt_b\, dt\, dt_i \\ &= \sum_{i=1}^{\infty} \frac{i \lambda^i \mu}{(\lambda+\mu)^{i+1}} = \frac{\lambda}{\mu}, \end{aligned} \tag{20}$$

where $T_{i-1} = t_0 + t_1 + t_2 + \cdots + t_{i-1}$ when i faults occur while the connection is using the backup path, as can be seen in Figure 5.

Using Eq.s 13, 15, and 19, we obtain the following probabilities. The loss probability, accounting for failures that occur while traffic is on a backup path, is

$$p_f = \frac{p_f^*}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \tag{21}$$

The probability of restoration request acceptance can be computed as

$$\begin{aligned} p_r &= \frac{n_r}{n_f} \\ &= \frac{1 - p_f^*}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}, \end{aligned} \tag{22}$$

and the probability of restoration failure resulting from using a recovery path is found in a similar manner to be

$$\begin{aligned} p_a &= \frac{n_a}{n_f} \\ &= x p_r \\ &= \frac{(1 - p_f^*)\frac{\lambda}{\mu}}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \end{aligned} \tag{23}$$

¿From the above Eq. 23, we can get the effective fault occurrence rate as

$$\begin{aligned} \lambda_f &= \lambda(1 - p_a) \\ &= \frac{\lambda}{1 + (1 - p_f^*)\frac{\lambda}{\mu}}. \end{aligned} \tag{24}$$

Note that as $x = \lambda/\mu$ vanishes, $p_f \to p_f^*$, as suggested by Eq. 18. Similarly, we can directly show that $p_r \to 1 - p_f$, $p_a \to 0$, and $\lambda \to \lambda_f$ as $x \to 0$.

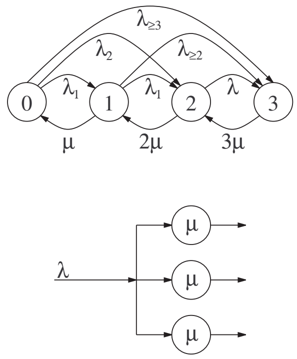

Fig. 6. Sketch and state diagram for $M^X/M/3/3$ system (no buffering). The rates of the form $\lambda_{\ge k}$ denote arrival rates of groups with size of at least k. Thus, for example, $\lambda_{\ge 2} = \lambda \sum_{n=2}^{\infty} c_n = \lambda(1 - c_1)$.

B. Multiple Failures with Batch Arrivals

When a network operator creates protection groups with shared backup resources, it is important to maintain routing diversity among the various working paths in the group, so that a failure event (e.g. a fiber cut) impacts at most one working path. In practice it is not always possible to limit the effects of failure events in this way. If, for instance, several working paths in a $M : N$ group pass through different switching offices that are in close proximity and they are all affected by a catastrophic event (e.g. a major earthquake) simultaneous failure of multiple working paths can occur.

Given the possiblity of multiple failures, we need to develop a model that will allow us to determine the number of backup paths that are required in a protection group to guarantee that the probability of a working path's being unable to find a backup path is less than some maximum acceptable value. We first consider the case where we have a finite number of backup paths and an infinite number of working paths. We model multiple failures using batch arrivals, where the number of arrivals is a discrete random variable X whose probability mass function is

$$c_k = \Pr\{X = k\}.$$

We model the restoration group as a set of N servers each with exponential service times where the average completion rate is μ. The system is fed by a Poisson arrival process with mean inter-arrival time $1/\lambda$. The rate of arrival of batches of size k is $\lambda_k = c_k\lambda$. There is no buffering (i.e. the maximum number of customers allowed in the system is N), so that we have an $M^X/M/N/N$ loss system, which has been analyzed extensively in the literature. A discussion of its properties may be found in [10]. An example of the state flow diagram for this model where $N = 3$ is shown in Figure 6.

The system of stationary balance equations that describe this system is

$$\left\{\begin{array}{l} 0 = -\lambda p_0 + \mu p_1 \\ 0 = -(\lambda + n\mu)p_n + (n+1)\mu p_{n+1} + \lambda \displaystyle\sum_{k=0}^{n-1} p_k c_{n-k}, \\ n = 1, 2, \ldots, N-1 \\ 0 = -N\mu p_N + \lambda \displaystyle\sum_{k=0}^{N-1} \sum_{l=N-k}^{\infty} p_k c_l \end{array}\right. \tag{25}$$

We can get the state probabilities by using the approach given in [11], which is as follows. Recursively solving the balance equations gives

$$p_n = \frac{\lambda}{n\mu} \sum_{k=0}^{n-1} p_k C_{n-k},\ n = 1, 2, \ldots, N, \tag{26}$$

where $C_j = \sum_{m=j}^{\infty} c_m = \Pr\{X \geq j\}$. By defining the sequence $\{g_n\}_{n=0}^{N}$ to be

$$g_n = \left\{\begin{array}{cc} 1, & n = 0 \\ \frac{\lambda}{n\mu} \sum_{k=0}^{n-1} g_k C_{n-k}, & n = 1, 2, \ldots, N \end{array}\right. \tag{27}$$

we can express the state probabilities as

$$p_n = g_n p_0,\ n = 0, 1, 2, \ldots, N, \tag{28}$$

where

$$p_0 = \left[\sum_{n=0}^{N} g_n\right]^{-1}. \tag{29}$$

The metric of interest in this case is the blocking probability, which is the probability that more customers arrive than can be handled by the system. To find the blocking probability for the $M^X/M/N/N$ system, we must compute

$$\begin{aligned} p_B &= \sum_{n=0}^{N} \Pr\{X > N - n | \text{System in State } n\}\, p_n \\ &= p_0 \sum_{n=0}^{N} \left(1 - \sum_{k=1}^{N-n} c_k\right) g_n \\ &= 1 - \frac{\displaystyle\sum_{n=0}^{N}\sum_{k=1}^{N-n} g_n c_k}{\displaystyle\sum_{n=0}^{N} g_n}. \end{aligned} \tag{30}$$

This is the probability that an arriving batch will be unable to be completely serviced, because there are more arrivals in the batch than there are servers available to handle them. In such a situation, at least one of the members of the batch will have to be dropped while the remaining members go into service. Alternatively, we can define a blocking metric that is simply the probability that the system in in State N, which is the probability that no members of an arriving batch will be able to get served. This is

$$p_N = \frac{g_N}{\displaystyle\sum_{n=0}^{N} g_n}. \tag{31}$$

We now plot these metrics using for the case where the batch size X has a geometric distribution. Thus $c_k = a(1-a)^{k-1}$, $0 < a \leq 1$, and the mean batch size is $1/a$. When $a = 1$, we have the $M/M/N/N$ system. For these examples, we have set $a = 0.9$, so that the probability that the batch size is greater than unity is 0.1. For the geometric distribution we can compute C_j as

$$C_j = \sum_{k=j}^{\infty} c_k = (1-a)^{j-1}.$$

Using this, we can determine the elements of the sequence g_n and obtain the state probabilities and the blocking probability metric for the system. For geometrically distributed bulk arrival sizes, the blocking probability of a $M^X/M/N/N$ system is

$$p_B = \frac{\displaystyle\sum_{n=0}^{N} (1-a)^{N-n} g_n}{\displaystyle\sum_{n=0}^{N} g_n}. \tag{32}$$

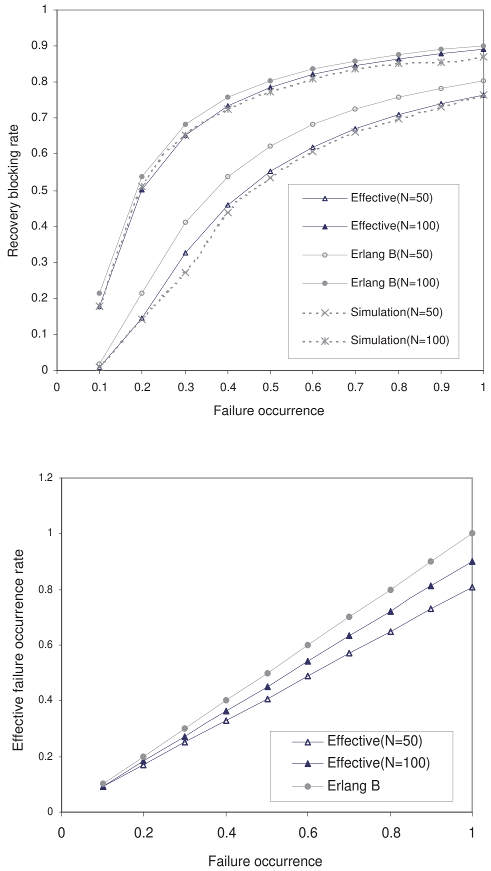

Fig. 7. Impact of multiple failures

V. Performance Evaluation

The performance of the proposed analytical model is analyzed by considering recovery blocking rate, i.e. we characterize optical network services by restorability. It is assumed that a failure occurs with exponential distribution (mean is 10) and recovery time is 1 in the simulation test. Fig. 7 illustrates the impact of the multiple-failure effect comparing our model with the Erlang. In these graphs, $m = 10$ and two sets of curves are considered where one is $N = 50$ and the other is $N = 100$. The first graph in Fig. 7 indicates that our model is consistent with the simulation test. We observe that when N is small, the Erlang model is not appropriate to predict recovery failure probability (restorability) for a GMPLS network with a lower number of failures. As for the second graph, when the

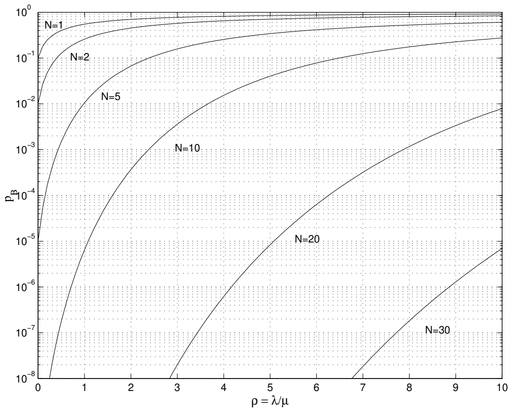

Fig. 8. Probability of blocking for $M^X/M/N/N$ system with geometrically distributed arrival batch sizes and $\Pr\{X > 1\} = 0.1$, versus utilization.

number of failures in a network is small, each working path with failures is likely to send current traffic on a backup path and the subsequent failures are unlikely to get the recovery service. Thus, effective failure occurrence rate per working path also becomes small. When N is large, it is more likely that a failure is unable to use a backup path because there is no free backup path.

In Fig. 8, we have plotted the value of the blocking probability as defined in Eq. 30 and 32 versus λ/μ for various values of N. In Fig. 9 and 10, we respectively show similar plots for p_N as defined in Eq. 31 and for $p_B = p_N$ in the $M/M/N/N$ case, which is given in Eq.18. These metrics are conservative because they assume an infinite pool of working paths. In reality, the number of working paths is limited and the probability that a bulk failure of a given size will occur is dependent on the number of remaining healthy working paths, and will decrease as the pool shrinks.

In examining these plots, we note that there is very little difference in the values obtained for p_B as defined in Eq. 30 versus p_N as defined in Eq. 31, except for values of ρ that are very close to zero. This is because we have defined p_B to the probability that the next arriving batch is unable to be completely served, which for $\rho = 0$ is the probability that $X > N$. The value of p_N, in contrast, tends towards zero as ρ vanishes, as can be seen in Fig. 9. For most values of ρ, we obtain a slightly more conservative metric by using

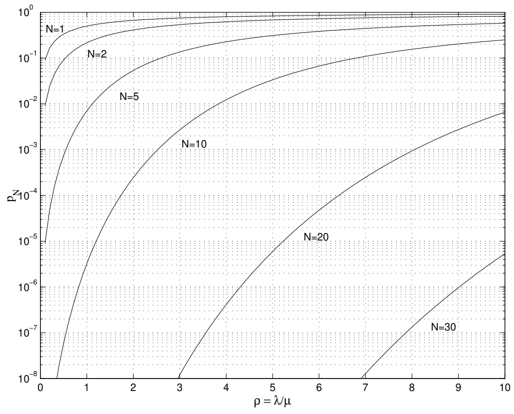

Fig. 9. Probability of being in state N for $M^X/M/N/N$ system with geometrically distributed arrival batch sizes and $\Pr\{X > 1\} = 0.1$, versus utilization.

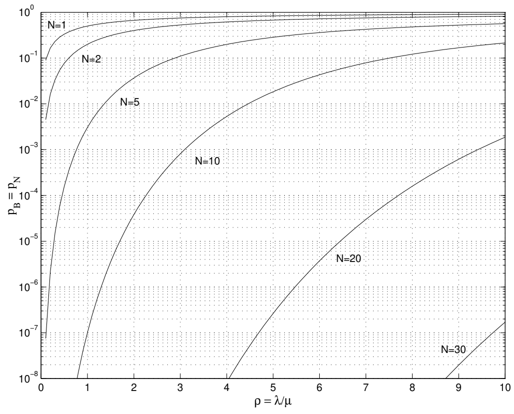

Fig. 10. Probability of blocking for $M/M/N/N$ system with single arrivals only, versus utilization.

Eq. 30.

Using these plots, it is possible to determine the number of backup paths that will guarantee a desired maximum probability that a failed working path that not be switched over. For instance, if failure events occur at an average rate of once every two days (with 1/10 failure events involving multiple failed working paths) while repairs to failed working paths take half a day on average (giving $\rho = 0.5$), a blocking probability of at most 10^{-6} can be guaranteed if the protection group contains at least 9 backup paths.

When we compare Figs. 8 and 9 to Fig. 10, which shows p_N for the case where multiple simultaneous failures never occur, we see that there is little difference in performance between the two systems for small values of N, although the gap between the two metrics increases with decreasing values of ρ. The gap between the metrics for the $M/M/N/N$ and $M^X/M/N/N$ models increases with increasing N; for $N = 20$ the difference is roughly one order of magnitude. Thus, determining bulk arrival statistics becomes an issue when recovery is slow relative to the rate of failures yet a high level of reliability is required.

VI. Conclusion and Future Work

In this paper, we prposed a new analytical model for shared backup path provisioning in GMPLS networks. In our model, protection bandwidth capacity was considered as the main cost of recovery QoS, with the result that different amount of backup resources could be assigned to services with different levels of protection. We have also discussed some of the issues associated with provisioning shared backup paths in networks that use GMPLS as part of their control plane. We have reviewed some of the ways that GMPLS, in combination with other QoS mechanisms, can be used to allow service providers to offer customized levels of protection to their customers. To determine the optimum size of a $M : N$ protection group given timing and QoS constraints, we have developed a simple model that predicts the amount of time required to establish a backup path in situations where working path traffic is successfully switched to a backup path with probability less that one. We have also developed models for $M : N$ protection with reversion for both single failures, which are modeled by an Engset distribution, and batch failures, which are modeled by a $M^X/M/N/N$ system. We used these models to demonstrate that shared protection groups can be sized so that the probability that a backup path is unavailable is less than a desired threshold. We also showed that when multiple simultaneous failures are rare, the single failure model is a good approximation that can be used for protection group sizing. We supported these conclusions with a set of simulations.

We intend to expand on this work by analyzing the effect of network topology on the probability of multiple failure events and by studying switchover delays in more detail. In particular, we are examining the behavior of several restoration signaling algorithms in a variety of failure scenarios.

References

[1] O. Gerstel and R. Ramaswami, "Optical Layer Survivability: A Services Perspective," *IEEE Communications Magazine*, vol. 38, no. 3, pp. 104-113, March 2000.

[2] H. Ishimatsu et al., "Carrier Needs Regarding Survivability and Maintenance for Switched Optical Networks," Internet draft, draft-hayata-ipo-carrier-needs-00.txt, November 2000.

[3] P. Smith, et al, "Generalized MPLS - signaling functional description," *Internet Draft*, draft-ietf-mpls-generalized-mpls-signaling-02.txt, Mar. 2001.

[4] P. Smith, et al, "Generalized MPLS Signaling - RSVP-TE Extensions," *Internet Draft*, draft-ietf-mpls-generalized-rsvp-te-01.txt, Mar. 2001.

[5] P. Smith, et al, "Generalized MPLS Signaling - CR-LDP Extensions," *Internet Draft*, draft-ietf-mpls-generalized-cr-ldp-01.txt, Mar. 2001.

[6] Many, "OIF UNI Signaling Specification", OIF2000.125.3, Feb. 2001.

[7] L. Kleinlock, "Queueing Systems: Theory, vol.I", *John Wiley & Sons*, NewYork, 1975.

[8] V. Sharmai et al, "Framework for MPLS-based Recovery", *IETF Draft*, draft-ietf-mpls-recovery-frmwrk-02.txt, Mar. 2001.

[9] C. Mas and P. Thiran, "An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks," *The IEEE Journal of Selected Areas in Communications*, vol. 18, no. 10, pp. 1900-1911, October, 2000.

[10] M. L. Chaudhry and J. G. C. Templeton, *A First Course in Bulk Queues*, John Wiley & Sons, Inc., 1983.

[11] I. W. Kabak, "Blocking and Delays in $M^{(x)}/M/c$ Bulk Arrival Queueing Systems," *Management Science*, vol. 17, pp. 112-115, 1970.