INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt (in press)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/nem.601

A novel fault management approach for DWDM optical networks

W. Fawaz[1], F. Martignon[2], K. Chen[1] and G. Pujolle[3,*,†]

[1]*University of Paris 13-L2TI Lab 99, Avenue Jean-Baptiste Clement, 93430 Villetaneuse, France.*
[2]*Department of Management and Information Technology, University of Bergamo, Italy.*
[3]*University of Paris 6, LIP6 Laboratory, 8 rue du Capitaine Scott, 75015, Paris, France.*

SUMMARY

Connection availability is considered as a critical metric when providing differentiated services in Wavelength-Division Multiplexing mesh networks. Indeed, one of the major concerns of optical network operators is related to improving the availability of services provided to their highest-class clients. Achieving this objective is possible through managing faults using the different classical protection schemes, namely the so-called dedicated and shared protection schemes. However, the majority of the work concerning protection schemes has considered the primary connections as equally important when contending for the use of the backup resources. As a main contribution in this paper, we therefore propose an improvement of the existing protection schemes through the introduction of relative priorities among the different primary connections contending for the access to the protection path. To evaluate numerically the benefits of the service differentiation feature introduced in our proposal, we first develop a mathematical model, based on which we derive explicit expressions for the average connection availabilities that result from both the classical protection schemes and the proposed priority-aware one. Through this model, we show how the availability of the highest-class clients is improved when deploying the proposed priority-aware protection scheme. Finally, with the same objective in mind, we develop a simulation study, where a given set of connection demands with predefined availability requirements is provisioned using different protection strategies. Through this study, we show that the priority-aware protection strategy satisfies service-availability requirements in a cost-effective manner compared with the classical protection schemes.

1. INTRODUCTION

The revolutionary Wavelength-Division Multiplexing (WDM) technology increases the transmission capacity of fiber links by several orders of magnitude. In wavelength-routed WDM networks, an optical cross-connect (OXC) can switch the optical signal on a WDM channel from an input port to an output port; thus a connection (lightpath) may be established from a source node to a destination node following a path that may span multiple fiber links [1,2]. As WDM continues to evolve, fibers are witnessing a huge increase regarding their carriage capacity, which has already reached the order of terabits per second. Therefore, the failure of a network component (e.g., a fiber link, an optical cross-connect, an amplifier, a transceiver, etc.) can weigh heavily on optical carrier operators due to the consequent huge loss in data and revenue. To obtain an estimate of the different optical components' failure characteristics, Table 1 presents the mean failure rates and failure repair times of various optical network components according to Bellcore (now Telecordia) [1], where Failure-In-Time (FIT) denotes the average number of failures in 10 [9] hours, Tx denotes optical transmitters, Rx denotes optical receivers, and MTTR stands for mean time to repair.

*Correspondence to: Guy Pujolle, University of Paris 6, LIP6 Laboratory, 8 rue du Capitaine Scott, 75015 Paris, France.
†E-mail: guy.pujolle@lip6.fr

Received 8 June 2005
Accepted 10 October 2005

Metric	Telecordia Statistics
Equipment MTTR	2 h
Cable-cut MTTR	12 h
Cable-cut rate	501142 FIT/1000 sheath miles
Tx failure rate	10867 FIT
Rx failure rate	4311 FIT

Table 1. Failure rates and repair times (Telecordia)[1]

Two main conclusions may be drawn based on these statistics:

- The frequency of failure occurrence in optical networks is not negligible.
- Cable cut is the dominant failure scenario compared to Tx and Rx failures, for lengths in the order of hundreds of kilometers, normally found in backbone optical networks.

With the frequent occurrence of fiber cuts and the tremendous loss that a failure may cause, fault management, together with its impact on network design, becomes a critical concern for operators who strive to keep up with the competition for broadband traffic transport. Moreover, as WDM networks migrate from ring to mesh topology, planning a survivable WDM mesh network has been the subject of extensive studies [3–5], leading to the definition of various resilience approaches. Mainly, there are two types of fault recovery mechanisms: *protection* [6] and *restoration* schemes [7]. In this paper we focus our study on protection schemes, dealing mainly with the impact these schemes have on customer-perceived service quality, which is an emerging topic and of special interest today. We believe that protection, a proactive procedure, is a key strategy to ensure fiber network survivability. To the best of our knowledge, what is still lacking in the existing literature is a systematic methodology to efficiently select a cost-effective protection scheme for each connection, while satisfying its quality of service (QoS) requirements. Usually, by means of service contracts called Service-Level Agreements (SLA), a client subscribes to optical network services from the optical operator with a certain guaranteed QoS level. Within the SLA, Service Level Specifications (SLS) [8] quantify the QoS provided to the customer. A certain number of SLSs indicate the reliability constraints needed by the subscribed service. The rationale behind this is as follows. The reliability requirements of the different subscribed services can be very different according to their diverse characteristics; for example, online trading, military applications, and banking services will require stringent reliability, while IP best-effort packet delivery service may be satisfied without a special constraint on reliability. Reliability parameters presented in the literature include mainly service availability and restoration time. Our interest will be directed to service availability since the problem of how connection availability is affected by network failures is currently attracting more research interest.

As a first main contribution in this paper, we propose an extension for the so-called shared protection scheme contributing to the design of a new quality of service-aware protection schemes. To date, the majority of the work concerning shared protection has considered the primary connections as equally important when contending for the use of the backup resources. As a result, when several connections fail successively, the first failed connection is recovered by the backup resources, regardless of the QoS requirements of the remaining failed connections. Hence, these latter connections are penalized and remain in an unprotected state until either their primary paths are repaired or until backup resources are released. From a service perspective, this scheme does not provide an optimal solution as it does not take into account the different QoS requirements (e.g., availabilities) of the primary connections during the recovery procedure.

To cope with such limitation, we envision through our proposal introducing a relative priority among the primary connections sharing backup resources. So, revisiting the previous scenario, if a low-priority connection fails first, its recovery would be possible. However, once a high-priority connection fails, it will use the backup resources, resulting in the preemption of the previously recovered lower-priority connection. In order to gauge the benefits of our proposal, the impact of such an approach on the customer-

DOI: 10.1002/nem

perceived service availability needs to be studied and compared with classical protection approaches. Moreover, to assess the efficiency of the proposed scheme in comparison to the classical protection schemes, we need to evaluate the cost in terms of resources (e.g., number of wavelengths needed) induced from the deployment of both the priority-aware scheme and the classical schemes in a real network. Therefore, we first present a mathematical model for both the classical shared-protection schemes and the proposed priority-aware scheme. We derive explicit analytic expressions for the average availability resulting from the deployment of such schemes. By solving these models we then evaluate numerically the benefits of the service differentiation feature introduced in our scheme. Finally, we exhibit the cost-effectiveness of our proposed approach regarding resource consumption (i.e., wavelengths) in a sample optical network topology using a simulation study. In this regard, a given set of randomly generated connection demands with predefined availability requirements are routed in the network using several provisioning schemes (i.e., using unprotected, dedicated, shared, and priority-aware shared protection schemes). The performances of these provisioning schemes are compared in terms of resources needed in the network, and in terms of the connections availability satisfaction rate. Our results show that the proposed protection approach achieves a high satisfaction rate while greatly economizing resource usage.

The paper is structured as follows: in the next section we propose and describe the priority-aware shared protection scheme; in the third section we introduce a mathematical model to evaluate the impact of the protection schemes analyzed in this paper on the connection availability; in the fourth section we present numerical results based on the mathematical study to evaluate the benefits of the service differentiation feature introduced in our scheme. In the fifth section the simulation study is developed with the corresponding results. The final section concludes this paper and proposes future issues.

2. PRIORITY-AWARE SHARED-PROTECTION SCHEME

This section introduces the proposed protection scheme that extends the existing shared-protection schemes through the introduction of relative priorities among different primary connections contending for the backup paths.

Let us consider N working paths (w_i, $i = 1, \ldots, N$) with the same source and destination sharing M backup paths (b_i, $i = 1, \ldots, M$); i.e., an M:N protections scheme, as depicted in Figure 1. Both working paths and backup paths can be in failure. When a failure occurs, the repair process is started.

In the classical shared-protection scheme, when several subsequent failures occur in the network, all connections are considered of equal importance when contending for backup resources. As such, the first failed connection gains access to the backup path.

On the other hand, in our proposed scheme these connections are divided into K sets of reliability classes, $C_1, \ldots, C_K$, with N_i connections belonging to class C_i for $i = 1$ to K, and $\sum_{i=1}^{K} N_i = N$. Connections belonging to class C_1 have the highest priority, while those belonging to C_K have the lowest priority.

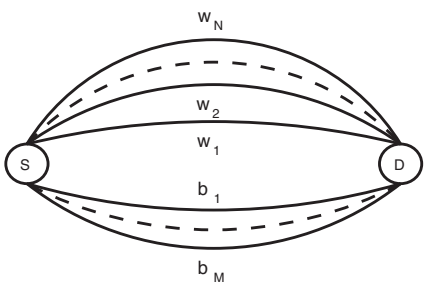

Figure 1. N working paths sharing M backup paths between a source node S and a destination node D

DOI: 10.1002/nem

When the working path of a connection t belonging to class C_i breaks down, the first available backup path, if any, is assigned to protect connection t and restoration is ensured by switching t to the backup path. Meanwhile, repair actions are performed on the primary path to restore it to be as good as new. Once repairing the primary path is achieved, the restored connection is switched back to its primary path.

On the contrary, if at the moment t fails all the backup paths are already occupied protecting other connections, a check is made to verify the existence of protected connections belonging to classes of lower priority than t, i.e. to classes comprised between $i + 1$ and K. If several such connections exist, the one having the lowest priority is immediately preempted by connection t. The preempted connection thus becomes unavailable, waiting for a backup path to be freed or for its working path to be repaired.

Finally, if neither of the two above situations is verified, connection t becomes unavailable.

3. THE MATHEMATICAL MODEL

In this section we present a mathematical model for both the classical $1:N$ shared protection scheme and the corresponding priority-aware extension discussed previously. Solving this model, we derive explicit expressions for the average availability of a connection resulting from deploying the aforementioned protection strategies. It is important to note that the dedicated protection case can be viewed as a special case of the shared protection scheme with $N = 1$. As we are interested in the *availability* of a connection, we need to define it first. The availability of a connection is defined as the probability that such connection is 'up' at any given time [9], and can be expressed as the proportion of time the connection is up during its entire service. If a connection is carried by a single unprotected path, its availability is equal to the path availability. The availability of a protected connection is determined by both the primary and the backup paths. In other words, a protected connection t is said to be *available* when either no failure affects its primary path or it is recovered by the backup path in case of failure along the primary path. Connection t becomes *unavailable* in the following two cases:

- one failure occurs on the primary path of t and a second failure occurs on its backup path;
- if t shares the backup path with connection t', then t will be unavailable if both t and t' fail but the shared backup path is taken by t'. In the priority-aware scheme, this occurs if t' has higher priority than t.

In this study we disregard the impact of the reconfiguration time for switching traffic from primary paths to backup paths on availability, since this time is negligible (usually on the order of milliseconds) compared to the failure repair time (usually on the order of hours) and to the connection's holding time (usually in the order of weeks or months).

3.1 Basic Assumptions

We base our mathematical study on the following classical assumptions [10]:

- a connection has only two states: it is either available or unavailable;
- different network components fail independently leading to repair actions;
- sufficient resources are available to repair simultaneously any number of failed connections, restoring them to be as good as new. This is known in the literature as *unlimited repair* [10];
- for any component the inter-failure time and the repair time are independent stationary Markovian processes with known mean values: Mean Time To Failure (MTTF) and Mean Time To Repair (MTTR), respectively.

A path holding a connection t fails when at least one of the components along the path is defective. The contribution of cable-cut rate to the overall path failure rate is predominant, compared to that of other components. Hence, for the sake of simplicity we assume that the failure rate λ of a path is equivalent to that of a single cable-link having the same length as the considered path. As a result, to compute the failure rate of each path we can multiply its length to the cable cut-rate per length unit (see Table 1).

DOI: 10.1002/nem

3.2 Model Definition and Resolution for the Classical Shared-Protection Scheme

Let us consider N working paths that share the same backup path, i.e. a $1{:}N$ shared-protection scheme. Let λ_i, $i = 1, \ldots, N+1$ be the mean failure rate of the ith path and μ_i be the mean recovery rate of the ith path; $1/\lambda_i$ and $1/\mu_i$ hence represent the Mean Time To Failure and Mean Time To Repair of the ith path, respectively. Based on the above assumptions, all the path failures are statistically independent and inter-failure and repair times are exponentially distributed. To gain insight into the behavior of the system and according to existing literature [10,11], we will consider a case of special interest in which all the paths (working as well as backup ones) have identical failure and recovery rates, i.e. $\lambda_i = \lambda$ and $\mu_i = \mu$, $\forall i = 1, \ldots, N+1$. Let us define $\rho = \lambda/\mu$. We have here a classical problem of reliability, with 1 redundant unit for N working units. Here a unit is an optical path. The steady-state availability A_i of a single path i, viz. the limiting ($\tau \to \infty$) probability of finding the path successfully operating at time τ, can be calculated as follows:

$$A_i = \frac{MTTF}{MTTF + MTTR} = \frac{1/\lambda}{1/\lambda + 1/\mu} = \frac{1}{1+\rho} \tag{1}$$

where $\overline{A_i} = 1 - A_i$ represents the unavailability of path i.

Let $F(\tau)$ be the number of failed paths at time τ. Because of the assumptions, $F(\tau); \tau \geq 0$ forms a continuous and stationary Markov process, with $F(0) = 0$. Let $p(n)$ be the steady-state probability that $F(\tau) = n$ in stationary regime. The transition diagram is given in Figure 2.

After some classical calculus we can express the steady-state probability $p(n)$ of the Markov chain as follows [10,12]:

$$p(n) = C_{N+1}^{n} \overline{A}^{n} A^{N+1-n} = \frac{(N+1)!}{n!(N+1-n)!} \frac{\rho^n}{(1+\rho)^{N+1}} \tag{2}$$

where C_{N+1}^{n} represents the number of all combinations of n failed paths out of $N + 1$, and A is given by equation (1). In other words, the number of failed paths follows a binomial distribution with parameters $N + 1$ and $\overline{A}$.

Note that $p(n)$ represents the proportion of time in which there are n failures in the network. When the total number of path failures n is greater than or equal to one, we can distinguish two cases:

(1) The backup path is among the failed paths and the remaining $n - 1$ connections cannot be restored.
(2) All the n failed paths are primary paths and, as such, only one connection is restored by the backup path while the remaining $n - 1$ connections are not.

Therefore, under such conditions there will always be exactly $n - 1$ unavailable connections. For $n \geq 2$ at least one connection will be unavailable, while when the number of failures n is equal to 1 there will be no unavailable connections. From this classical result, we are now interested in calculating the average unavailability of a specific connection t among the N shared-protected ones. The average unavailability of t is the proportion of time such connection is unavailable for all possible numbers of failures n, $2 \leq n \leq N + 1$. Let us define $Y(n)$ the event of t being unavailable under state n. The probability of having our reference connection t unavailable when there are n failed paths is equal to $p(n)P(Y(n))$. As $p(n)$ has already been calculated in equation (2), what remains is to calculate $P(Y(n))$. To do so, we have to consider all the events that may lead to the connection t becoming unavailable under state n. These events are the following:

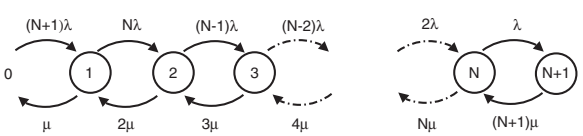

Figure 2. Transition diagram

DOI: 10.1002/nem

- $W(n)$: both the primary path of connection t and the backup path are failed;
- $Z(n)$: connection t's primary path is failed but the backup path is available.

Building on this information and according to the theorem of total probability, $P(Y(n))$ can be calculated as follows:

$$P(Y(n)) = P(Y(n)|W(n))P(W(n)) + P(Y(n)|Z(n))P(Z(n)) \tag{3}$$

where $P(Y(n)\,|\,W(n))$ and $P(Y(n)\,|\,Z(n))$ are, respectively, the conditional probabilities of having our reference connection t unavailable, given that events $W(n)$ and $Z(n)$ occurred. $P(Y(n)\,|\,W(n)) = 1$ as the backup path in this case is failed and restoration is possible; $P(Y(n)|Z(n)) = \dfrac{n-1}{n}$ as only one of the n primary paths under failure in this case can be restored.

The probability of the event $W(n)$ is

$$P(W(n)) = \frac{C_{N-1}^{n-2}}{C_{N+1}^{n}} = \frac{n(n-1)}{N(N+1)} \tag{4}$$

where the numerator indicates all possible combinations where the primary path of connection t and the backup path are among the failures. The denominator indicates all possible combinations of n failed paths out of $N + 1$.

The probability of the event $Z(n)$ is

$$P(Z(n)) = \frac{C_{N-1}^{n-1}}{C_{N+1}^{n}} = \frac{n(N+1-n)}{N(N+1)} \tag{5}$$

where the numerator indicates all possible combinations where the primary path of the connection t is among the failures while the backup is not.

Then, based on the above equations, the probability $P(Y(n))$ that the observed connection t is unavailable under state n is equal to

$$P(Y(n)) = \frac{n-1}{N}, 2 \le n \le N+1 \tag{6}$$

It can be seen that this equation is also valid for the case $n = 1$, for which $P(Y(n)) = 0$, since in this case all connections will be available, as stated before. Based on the theorem of total probability, the unavailability of a connection in the case of $1{:}N$ protection is given by the following formula:

$$U(N,\lambda,\mu) = \sum_{n=2}^{N+1} p(n) \cdot P(Y(n)) = \sum_{n=2}^{N+1} p(n) \cdot \frac{n-1}{N} \tag{7}$$

and, substituting the expression (2) for $p(n)$ we obtain

$$U(N,\lambda,\mu) = \frac{1}{N} \cdot \sum_{n=2}^{N+1} \frac{(n-1) \cdot C_{N+1}^{n} \cdot \rho^{n}}{(1+\rho)^{N+1}} \tag{8}$$

The average availability for a connection is simply equal to $1 - U(N,\lambda,\mu)$.

3.3 Model Definition and Resolution for the Priority-Aware Scheme

Let us consider the priority-aware shared-protection system proposed above, where N connections are divided into two sets of reliability classes, C_1 and C_2, with N_1 and N_2 connections belonging to class C_1 and C_2, respectively, and $N_1 + N_2 = N$. Connections of class C_1 have higher priority than connections belonging to C_2. In the following we derive the analytic expressions for the availability for each connection according to its priority class. We will begin by considering higher-priority connections. First of all,

DOI: 10.1002/nem

the N_1 connections having the highest priority can preempt instantaneously all the other connections belonging to the lower-priority class in the utilization of the backup path. Consequently, the analysis of the proposed scheme with regard to the high-priority connections is equivalent to the study of a classic $1:N_1$ shared-protection scheme. Therefore, we can derive straightforwardly the average unavailability U_1 of high-priority class connections based on equation (8) by simply substituting N with N_1.

$$U_1(N_1,\lambda,\mu)=\frac{1}{N_1}\cdot\sum_{n=2}^{N_1+1}\frac{(n-1)\cdot C_{N_1+1}^{n}\cdot\rho^{n}}{(1+\rho)^{N_1+1}} \tag{9}$$

When a low-priority connection fails, it becomes unavailable if any of the following mutually exclusive conditions is verified:

(1) The protection path has already failed.
(2) The protection path is up but there is at least one high-priority connection among the failures.
(3) The protection path is up, no high-priority connections are among failures, there is however another low-priority connection occupying the protection path.

Let E_i be the event of having condition i verified, $i = 1,2,3$. Therefore, to study the unavailability U_2 of a low-priority connection, we consider the process $Q(\tau)$ whose general state is a triplet (n_1,n_2,b), where n_1 and n_2 indicate, respectively, the number of failed high and low-priority connections at time τ, and b is a flag set to 1 if the backup path is down and to 0 if it is up.

$Q(\tau)$ is a continuous and stationary Markov process, with a limiting probability for each state given by

$$P(n_1,n_2,b)=P(n_1)P(n_2)P(b) \tag{10}$$

where $P(n_1)$, the probability of having n_1 failed high-priority connections and $P(n_2)$, the probability of having n_2 failed low-priority connections, are respectively equal to

$$P(n_1)=C_{N_1}^{n_1}\overline{A}^{n_1}A^{N_1-n_1} \tag{11}$$

$$P(n_2)=C_{N_2}^{n_2}\overline{A}^{n_2}A^{N_2-n_2} \tag{12}$$

and A is given by equation (1). $P(b)$ is the probability of having b backup path failures. In other words, when $b = 0$, there is no failure affecting the backup path, whereas if $b = 1$ the backup path is down. The expression of $P(b)$ is

$$P(b)=\overline{A}^{b}A^{1-b} \tag{13}$$

The events (E_i, $i = 1,2,3$), leading to the unavailability of a low-priority connection, are verified according to the values of n_1, n_2 and b. So, $b = 1$ leads to E_1, meaning that the protection path has failed; on the other hand, $b = 0$ and $n_1 \geq 1$ lead to event E_2; finally, $b = 0$, $n_1 = 0$ and $n_2 \geq 2$ produce event E_3. Under state (n_1,n_2,b), a specific low-priority connection t is unavailable when it fails *and* one of the events $E_1 - E_3$ is produced. Based on this observation, U_2 is given by

$$U_2=\sum_{\forall(n_1,n_2,b)}P(t\text{ fails in state }(n_1,n_2,b))\times P(n_1,n_2,b)\times P(E_1\cup E_2\cup E_3) \tag{14}$$

where

$$P(t\text{ fails in state }(n_1,n_2,b))=\frac{C_{N_2-1}^{n_2-1}}{C_{N_2}^{n_2}} \tag{15}$$

and $P(E_1 \cup E_2 \cup E_3)$ can be obtained with classical manipulations. It follows that U_2 is equal to

$$U_2=\sum_{i=2}^{N_2+1}C_{N_2-1}^{i-2}\overline{A}^{i}A^{N_2-i+1}+\sum_{i=1}^{N_2}C_{N_2-1}^{i-1}\overline{A}^{i}A^{N_2-i+1}\cdot(1-A^{N_1})+\sum_{i=2}^{N_2}C_{N_2-1}^{i-1}\overline{A}^{i}A^{N_2-i+1}\cdot A^{N_1}\cdot\frac{(i-1)}{i} \tag{16}$$

DOI: 10.1002/nem

4. NUMERICAL RESULTS

In this section we gauge the benefits of the proposed priority-aware protection scheme through numerical results induced from the previous mathematical study. For the sake of simplicity, we consider a scenario consisting of three primary connections sharing one backup path. We first consider a priority-aware protection scheme, with one high-priority and two low-priority primary connections. The availability of each class is calculated for different connections' lengths based on equations (9) and (14), and is reported in Figure 3. Then, a classical shared protection scheme is applied to this scenario, and the availability of a connection is evaluated using equation (8). The corresponding results are reported again in Figure 3 for comparison purposes. It is important to state that the Mean Time to Repair of all the paths is considered equal to 12 hours (see Table 1).

Based on Figure 3 we can observe that the high-priority connection protected using the priority-aware scheme is more available than the connections protected by the classical shared scheme. The observed availability results can be interpreted from a Quality of Service level perspective using the following reasoning. According to reference 8 a Platinum client requests an availability of 99.999% (i.e., at most 5 minutes of unavailability per year), whereas a Gold client requires an availability of 99.99% per year. With regard to this QoS terminology, the high- and low-priority classes can be mapped into Platinum and Gold QoS levels [8] or to lower QoS classes according to the connection's length. In fact, as shown in Figure 3, the availability of the high-priority connection drops below 99.999% when the connection length exceeds 850 km, while in the classical scheme this target availability is never achieved. This proves that by deploying the proposed scheme Platinum connections provisioning becomes possible in the network even for long communications which are encountered typically in backbone optical networks. Moreover, the QoS level of the Gold connections is still maintained.

To further underline the interest behind the proposed approach, we investigate a second scenario where we consider an invariant length of optical connections (800 km). However, the number of primary paths N sharing the backup path varies from 2 to 10. Following a similar approach as before, we first apply a priority-aware scheme where only one connection has high priority and the remaining ones have low priority. Then we consider a classical $1{:}N$ protection scheme. Figure 4 shows the average availability achieved in the two schemes. In the classical scheme, when the number of sharing primary connections increases, all such connections are penalized as they become less available. On the other hand, when using the priority-aware scheme, the high-priority connection is not impacted, maintaining the same availability level as shown in Figure 4. It is true that low-priority connections are less available than in the classical case, but the target availability level of Gold class connections is still achieved.

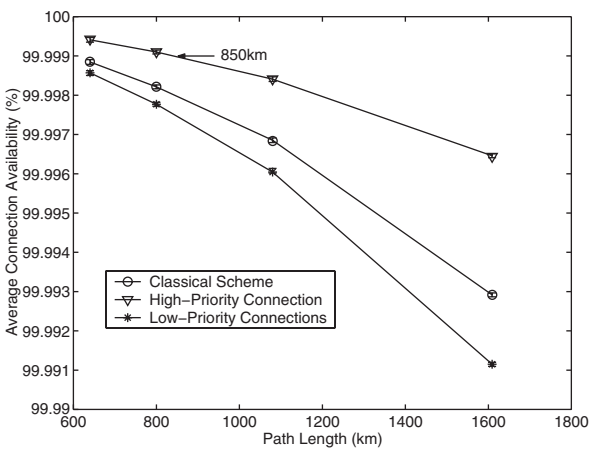

Figure 3. Average availability for the classical and the priority-aware 1:3 shared-protection scheme

DOI: 10.1002/nem

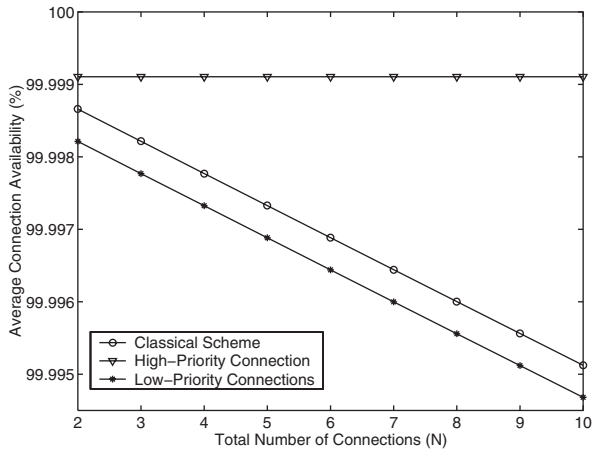

Figure 4. Average availability for the classical and the priority-aware 1:N shared-protection scheme, with 1 high-priority connection and $N - 1$ low-priority ones

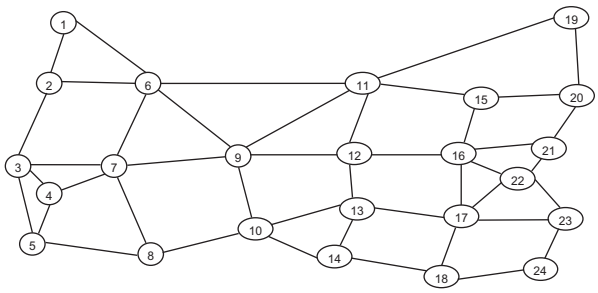

Figure 5. A sample network topology

5. SIMULATION STUDY

It is important to note first that, in our simulation, we relax some of the assumptions already considered in the mathematical study. In other words, when developing the mathematical model, we considered, for instance, backup sharing among primary connections having the same failure rates. These assumptions were made in an attempt to simplify the study, to gain insight into the model, and to concentrate mainly on the objective of comparing the protection schemes. However, in the simulation study we make no such assumptions; instead, backup sharing is considered in its most general form. As a result, to compute the availability of a protected connection a combinatorial approach is used, as will be explained when the different provisioning schemes are presented.

5.1 Description

For illustration purposes and following the guidelines presented by Zhang *et al.* [13], in our simulation we consider the network topology of Figure 5; availability of fibers is a pre-assigned value which can be 99.8%, 99.9%, 99.95%, or 99.995% according to their length. A traffic matrix of connection requests among all node pairs (i.e., total number of connections = 24×23 connections) is randomly generated. The availability requirements of the connection requests are uniformly distributed between two classes—99.9% or 99.99%—which are referred to as Silver and Gold classes, respectively. The traffic matrix is routed in the network according to different provisioning schemes which adopt distinct protection strategies. The

DOI: 10.1002/nem

Scheme	ASR_G	ASR_S	W	W_{Total}
Scheme I	5%	20%	94	3352
Scheme II	100%	100%	180	7961
Scheme III	94%	100%	150	6182
Scheme IV	100%	100%	150	6182

Table 2. Results from four provisioning schemes

availability for each provisioned connection is then calculated and compared to its required availability. Based on this, the Availability Satisfaction Rate resulting from each provisioning scheme for both Gold (ASR_G) and Silver (ASR_S) connections is computed and reported in Table 2. Moreover, in Table 2, the performance of the different provisioning schemes is stipulated in terms of the number of wavelength channels needed (W), and the total number of wavelength links (W_{Total}). W denotes the number of wavelength channels on the most congested fiber. On the other hand, W_{Total} denotes the total number of consumed wavelengths in the whole network. We compare the performance of four different provisioning schemes below.

Scheme I (without protection)
In Scheme I, all connections are routed using a simple Dijkstra algorithm applied to the hop number without any protection, and without any connection-availability consideration. In this case, a connection is available only when all the network components along its route are available. In other words, if a_j denotes the availability of a network component j, and S_i denotes the set of components used by path i, the availability of path i, A_i, can be computed as

$$A_i = \prod_{j \in s_i} a_j \tag{17}$$

Scheme II (dedicated protection)
In Scheme II, all connections are provisioned with dedicated-path protection (i.e., 1:1 protection). Under such a condition, a connection t is carried by one primary path p and protected by one backup path b which is link disjoint with p. As a result, t is up only when p is up, or b is up when p fails. A_t can thus be computed as follows:

$$A_t = A_p + (1 - A_p) \times A_b \tag{18}$$

Scheme III (classical shared-path protection)
In Scheme III, all connections are provisioned with the classical shared-path protection. Therefore, a connection t is carried by one primary path p and protected by one backup path b which is link disjoint with p. In this scheme, if t_i is a connection whose primary path p_i is link disjoint with p, then its backup path b_i can share backup resources with b when possible. Let us denote S_p as the set of all primary paths (except p) whose backup paths are sharing some resources with b. S_p can be seen as the set of connections sharing backup resources with t. t will thus be available if

(1) p is available; or
(2) p is unavailable, b is available, and the failure on p occurs before failure to other primary paths in S_p.

Therefore, A_t can be computed as follows:

$$A_t = A_p + (1 - A_p) \times A_b \times \sum_{i=0}^{n} \frac{1}{i+1} \times p_i \tag{19}$$

DOI: 10.1002/nem

where A_p and A_b are the availability of p and b, respectively; n is the size of S_p; and p_i is the probability that exactly i primary paths in S_p are unavailable. p_i can be easily calculated by enumerating all the possible i unavailabilities among the n sharing primary paths. The correctness of the above equation is already verified in Zhang *et al.* [13].

Scheme IV (priority-aware shared protection)

In Scheme IV, all connections are provisioned according to the proposed priority-aware shared-path protection. Unlike Scheme III, the availability of a connection will depend in this scheme on the class of service of the connection. So, if t_G is a Gold connection carried by one primary path p_G and protected by one backup path b_G which is link disjoint with p_G, then, even if S_{p_G}, which is the set of connections sharing backup resources with t_G, will contain primary paths of both Silver and Gold connections, the availability of t_G will be influenced only by the Gold ones (as already proved in the mathematical section). In other words, t_G will be available if

(1) p_G is available; or
(2) p_G is unavailable, b_G is available, and the failure on p_G occurs before failure to other Gold primary paths in S_{p_G}.

Therefore, A_{t_G} can be computed as follows:

$$A_{t_G} = A_{p_G} + (1 - A_{p_G}) \times A_{b_G} \times \sum_{i=0}^{n_G} \frac{1}{i+1} \times p_{G_i} \tag{20}$$

where n_G is the number of Gold primary paths in S_{p_G}, and p_{G_i} is the probability that exactly i Gold primary paths in S_{p_G} are unavailable. On the other hand, if t_S is a Silver connection whose primary path p_S is link disjoint with the backup path b_S, then the availability of t_S will be influenced by both the Gold and Silver connection primary paths present in S_{p_S} (as already proved in 'The Mathematical Model' section). In other words, t_S will be available if

(1) p_S is available; or
(2) p_S is unavailable, b_S is available, no Gold primary paths in S_{p_S} fail, and the failure on p_S occurs before failure to other Silver primary paths in S_{p_S}.

Therefore A_{t_S} can be computed as follows:

$$A_{t_S} = A_{p_S} + (1 - A_{p_S}) \times A_{b_S} \times \sum_{i=0}^{n_S} \frac{1}{i+1} \times p_{s_i} \times p_{G_0} \tag{21}$$

where n_S is the number of Silver primary paths in S_{p_S}; p_{G_0} is the probability no Gold primary paths in S_{p_S} are unavailable; and p_{S_i} is the probability that exactly i Silver primary paths in S_{p_S} are unavailable.

5.2 Numerical Results Analysis

From Table 2, one can observe that Scheme I consumes the least amount of resources compared with the other schemes. But in Scheme I only 5% of Gold and 20% of Silver connections can meet their required availabilities. This is because the primary path in Scheme I is calculated according to the minimum number of hops but it may not be reliable enough. By deploying a dedicated protection as in Scheme II, the Gold and Silver connection Availability Satisfaction rates (ASR_G, ASR_S) reach 100%; however, a large amount of resources is consumed. By providing a classical shared protection scheme as in Scheme III, an optimization of resource usage is achieved while realizing high *ASR*s but the Availability Satisfaction Rate of Gold connections drops below 100%. Finally, when deploying the priority-aware protection scheme proposed in this paper (Scheme IV), the Availability Satisfaction Rates for both Gold and Silver connections (ASR_G, ASR_S) attain 100% while optimizing resource usage.

DOI: 10.1002/nem

6. CONCLUSIONS AND FUTURE ISSUES

In this paper we have proposed an improvement of the existing shared protection schemes through the introduction of relative priorities among the different primary connections contending for the access to the protection path. We presented a detailed mathematical model for both the classical shared-protection schemes and for the proposed priority-aware scheme. We derived explicit analytic expressions for the average availability resulting from the deployment of such schemes. Through this study, it has been proven that service differentiation is better achieved through the use of our proposed protection scheme. Finally, we developed a simulation study where it has been shown that the proposed scheme achieves high Availability Satisfaction Rates while realizing cost-effectiveness in terms of resource usage in the network. To conclude, the introduction of the priority-aware protection scheme and of the models studied in this paper has a generic fundamental significance, beyond the specific context of path protection in WDM networks. Indeed, they can be applied to general systems. Due to this generality, any further results that can be derived have a potential significance for other fields.

REFERENCES

1. Ramamurthy S, Mukherjee B. A review of fault management in WDM mesh networks: basic concepts and research challenges. *IEEE Network* 2004; **18**(2): 41–48.
2. Ramaswami R. Optical fiber communication: from transmission to networking. *IEEE Communications Magazine* 2002; **40**(5): 138–147.
3. Ramamurthy S, Sahasrabuddhe L, Mukherjee B. Survivable WDM mesh networks. *Journal of Lightwave Technology* 2003; **21**(4): 870–883.
4. Mohan G, Murthy SR, Somani AK. Efficient algorithms for routing dependable connections in WDM optical networks. *IEEE/ACM Transactions on Networking* 2001; **9**(5): 553–566.
5. Ellinas G, Hailemariam A, Stern TE. Protection cycles in mesh WDM networks. *IEEE Journal on Selected Areas in Communication* 2000; **18**(10): 1924–1937.
6. Ramamurthy S, Mukherjee B. Survivable WDM mesh networks. Part I: Protection. In *Proceedings of INFOCOM 1999*, New York, March 1999; 744–751.
7. Ramamurthy S, Mukherjee B. Survivable WDM mesh networks. Part II: Restoration. In *Proceedings of ICC 1999*, Vancouver, June 1999; 2023–2030.
8. Fawaz W, Daheb B, Audouin O, Berde B, Vigoureux M, Du-Pond M, Pujolle G. Service level agreement and provisioning in optical networks. *IEEE Communications Magazine* 2004; **42**(1): 36–43.
9. To M, Neusy P. Unavailability analysis of long-haul networks. *IEEE Journal on Selected Areas in Communications* 1994; **12**(1): 100–109.
10. Angus JE. On computing MTBF for a k-out-of-n:G repairable system. *IEEE Transactions on Reliability* 1988;**37**(3):312–313.
11. Lee D, Libman L, Orda A. Path protection and blocking probability minimization in optical networks. In *Proceedings of INFOCOM 2004*, Hong Kong, March 2004.
12. Mitra D. Stochastic theory of a fluid model of producers and consumers coupled by a buffer. *Advances in Applied Probability* 1988; **20**: 646–676.
13. Zhang J, Zhu K, Zang H, Mukherjee B. A new provisioning framework to provide availability-guaranteed service in WDM mesh networks. In *Proceedings of ICC 2003*, Anchorage, Alaska, May 2003; 1484–1488.

AUTHOR'S BIOGRAPHIES

Wissam Fawaz got his Ph.D. from the L2TI Laboratory of the University of Paris 13. His research concerns reliability-constrained optical fault management, and the more general scope of quality of service management in next generation optical networks.

DOI: 10.1002/nem

Fabio Martignon works as an associate professor at the University of Bergamo, Italy. His research interest concerns Quality of Service in optical networks, and the design of enhanced TCP congestion control schemes.

Ken Chen works as a professor at the University of Paris 13, and director of the L2TI laboratory. His research concerns optical networks performance evaluations and real time communications.

Guy Pujolle works as a professor at the University Pierre et Marie Curie (Paris 6), and is in charge of the Phare group within the LIP6 Laboratory. His research concerns several network fields such as management, wireless networks, ad hoc and sensor networks.

DOI: 10.1002/nem