Proposal and Analysis of Novel Availability Aware Protection Schemes in WDM Optical Networks

Timothy I. Sawwah

This Thesis is presented in partial fulfillment of the requirements for the degree of

Masters of Science in Computer & Communications Engineering

Lebanese American University

Spring 2009

Plagiarism Policy Compliance Statement

I certify that I have read and understood LAU's Plagiarism Policy. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.

This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Timothy Sawwah

Signature: Date: June 29, 2009

I grant to the LEBANESE AMERCIAN UNIVERSITY the right to use this work, irrespective of any copyright, for the University's own purpose without cost to the University or its students and employees. I further agree that the University may reproduce and provide single copies of the work to the public for the cost of reproduction.

Acknowledgment

I would like to thank my advisor Dr. Wissam Fawaz for his guidance throughout my thesis work and the thesis committee members Dr. Zahi Nakad and Dr. Raymond Ghajar. I would like to also thank my family and friends for their continuous support.

To my parents

& the one I love

Abstract

With the frequent occurrence of fiber cuts in optical core networks and the tremendous loss that a failure may cause, the design of survivable optical networks is becoming of extreme importance to optical network operators. One of the major concerns in this regard is related to improving the availability of the services that the optical operators offer to their clients. This work addresses this issue by presenting three novel availability-aware protection schemes that achieve high level of availability for optical connections. As a distinguishing feature from existing protection schemes, the proposed schemes introduce relative priorities among the different primary connections contending for the use of the backup resources. In an attempt to gauge the benefit of the proposed protection schemes relative to the ones studied in the open literature, mathematical models are provided for evaluating the average connection availability resulting from the deployment of such schemes. The numerical results obtained from the mathematical models prove that higher availability levels can be realized through the use of the availability-aware protection schemes defined in this work.

Table of Contents

List of Figures:

List of Tables:

Abbreviations:

WDM: Wavelength Division Multiplexing

FIT : Failure in Time

MTTR : Mean Time to Repair

MTTF : Mean Time to Repair

QoS : Quality of Service

SLA : Service Level Agreement

Chapter 1

Background Information

1.1 Introduction

The revolutionary Wavelength-Division multiplexing (WDM) technology increases the transmission capacity of fiber links by several orders of magnitude. It divides the tremendous bandwidth of a fiber into many non-overlapping wavelengths (WDM channels), which can be operated at the peak electronic speed of several gigabits per second [RAM 02]. 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 along a path that may span multiple fiber links. As WDM keeps on evolving, fibers are witnessing a huge increase regarding their carriage capacity, which has already reached the order of terabits per second and will continue to grow for years to come.

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. Indeed, a single outage can disrupt millions of users and result in millions of dollars of lost to users and operators of the network. The Gartner research group attributes for instance up to $500 million in business losses due to network failures by the year 2004 [GRO 04]. Providing resilience against failures is thus an important requirement for WDM optical networks.

Building on this, *network survivability*, together with its impact on network design, becomes a critical concern for optical operators. Quoting from [MAN 06], network survivability refers to “the set of capabilities that allow a network to restore affected traffic in the event of a failure”. There are several mechanisms to ensure fiber network survivability. These mechanisms are referred to as *fault recovery Techniques*, and involve providing some redundant (backup) capacity within the network and rerouting traffic around the failure using this redundant capacity.

Mainly, fault recovery techniques can be classified into two general categories: pre-designed *protection* [RAM 99] and dynamic *restoration* [MUK 99]. The distinction between protection and restoration is centered on both the different time scales in which they operate, and the resource allocation done during the recovery period [BAN 01]. Protection requires pre-allocated backup resources and is designed to react to failures rapidly (less than a couple of hundred milliseconds). Restoration, on the other hand, relies on dynamic backup resource establishment in case of failure, and it may take up to an order of magnitude longer to restore the connection compared with protection.

1.2 Optical Transport Network Failures:

An end to end optical connection (lightpath) is routed through many optical components (fiber cables, nodes, etc.) in the network between its source and its destination. As such, the fraction of time during which the lightpath will be in the operating state (availability of lightpath) depends on the failure characteristics of the elements along its path. For example, Figure 1.1 shows a sample wavelength routed network with a lightpath on wavelength λ_1 connecting nodes A and D. The considered lightpath becomes unavailable if any of the nodes (A, B, C, or D) or of the links (A-B, B-C, or C-D) along its path fails.

Optical network survivability techniques (protection, restoration) contribute to the improvement of lightpaths' availabilities, since they allow unavailable connections to be recovered by backup resources. The amount of time during which the connection will be operational increases and thus the connection's availability is improved. However, this improvement is realized at the expense of a certain additional cost (due to resource redundancy) that results from to the deployment of the survivability techniques in the optical network. This additional cost can be justified by the frequent occurrence of fiber cuts as will be illustrated in the following subsection.

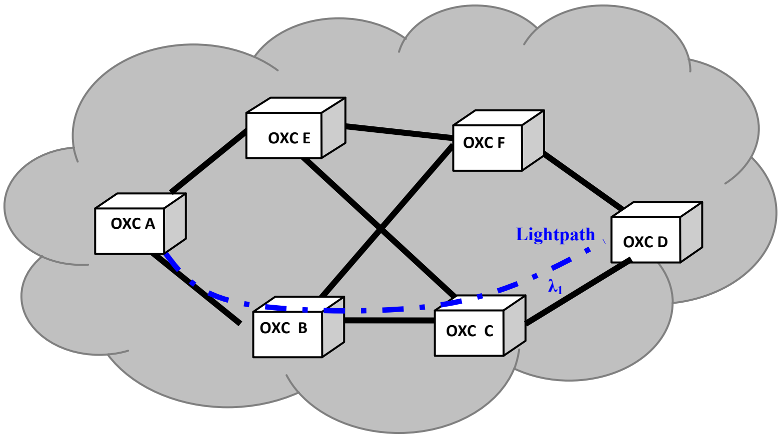


Figure 1. 1 Sample wavelength-routed optical network

1.2.1 Failure Statistics

To get an estimate of the different optical components failure characteristics, Table 1.1 presents the mean failure rates and failure repair times of various optical network components according to Bellcore (now Telecordia) [ZAN 04], 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.

Table 1- 1 Failure *rates and repair times (Telecordia [ZAN 04])*

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

Two main conclusions may be drawn based on these statistics:

- The frequency of failure occurrence in optical networks is not negligible. In fact, according to Table 1.1, any given mile of cable will operate about 228 years before it is damaged (cable cut rate = 4.39 cuts/year/1000 sheath miles). At first that sounds reassuring. But on 100000 installed route miles (in backbone optical networks), it implies more than one cut *per day* on average;
- 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 networks. This helps explain why optical network survivability design is primarily focused on recovery from failures arising mainly from cable cuts.

It is reasonable to ask why fiber optic cables get cut at all, given the prominent understanding of how important it is to physically protect such cables. Isn't it enough to just bury the cables suitably deep or put them in conduits and stress that everyone should be careful when digging?

Unfortunately what seems so simple is actually not. Despite best-efforts at physical protection, it seems that a fairly high rate of cable cuts is inevitable. Next, we discuss the main causes of failures.

1.2.2 Causes of Cable-cut Failures

After several serious cable-related network outages in the 1990s, a comprehensive survey on the causes of fiber optic failures was commissioned by regulatory bodies in the United States [CRA 92].

Figure 1.2 presents data from that report on the causes of fiber failures. As shown in Figure 1.2, dig-ups are the largest cause of fiber optic damage accounting for almost 60% of the reported failures. Two-thirds of those occurred even though the contractor had notified the facility owner before digging. Following dig-ups, vehicle induced damage due to the improper depth of installed cable is responsible for 7.5% of the reported failures. In this case, vehicle damage was often suffered by aerial cables from collision with poles. Human error comprises

7.0% of the reports. It is typified by a craftsperson cutting wrong cables during maintenance or during cable salvage activities ("copper mining") in a manhole.

As a wrap up, dig-ups, vehicle, and human error induced failures constitute the dominant failure contributing factors in optical networks. The relative magnitudes of these three main failure causes, along with most of the remaining failure causes, correlate well with data presented in Bellcore's Field Tracking Study [RAM 01]. Moreover, these failure percentages present a close matching to another set of statistics presented in [RAD 02]. The authors of this paper show that digging participates in 62.97% of failure cases, while vehicles cause 5.7% of the failures.

As for the remaining failure contributing factors presented in Figure 1.2, they contribute at a lower degree in optic cable cut. Power line refers to metallic contact of the strain-bearing “messenger cable” in aerial installations with power lines. Sabotage failures were typically the result of deliberate actions by disgruntled employees. Tree-falls were not a large contributor in this U.S. survey but in some areas where ice storms are more seasonal, tree falls and ice loads can be a major hazard to aerial cables.

In fact, Conduits are expensive to install, and in some countries cable burial can be a major capital expense. For example, in parts of Canada, trenching can be almost infeasible as bedrock lies right at the surface. Consequently, much fiber cable mileage remains on aerial pole-lines and is subject to weather-related hazards, such as ice, tree falls, and lightening strikes.

It is clear at this stage that network survivability design is a major concern for optical operators, who strive to keep up with the competition for broadband traffic transport. Hence, failure recovery techniques need to be deployed to improve the reliability of WDM optical networks. This issue is the key driver for the following section in which we delve into a detailed analysis of the existing survivability mechanisms.

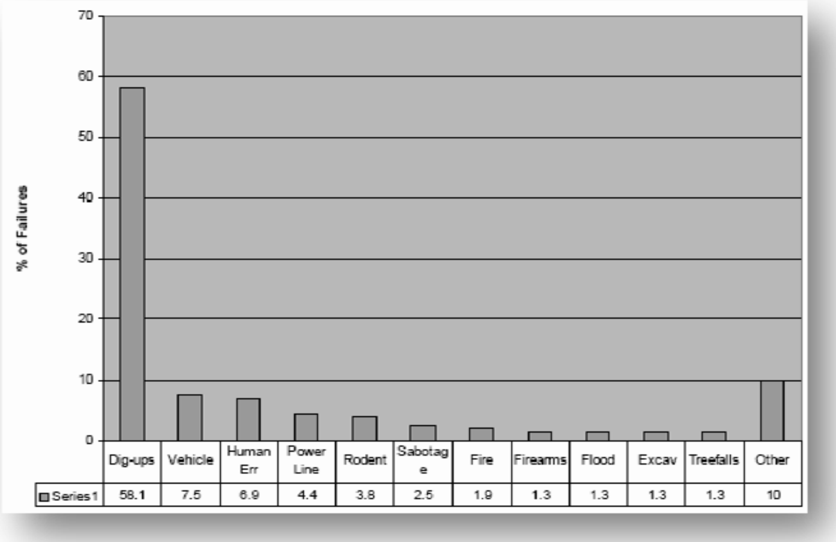


Figure 1. 2 Immediate cause of breakdown for 160 fiber optic cable cuts [CRA 92]

1.3 Survivability Mechanisms in WDM optical Networks:

There are two types of fault recovery mechanisms:

- If backup resources are pre-computed and reserved in advance, we call it a *protection* scheme;
- Otherwise, if backup resources have to be discovered dynamically for each interrupted connection, we call it a *restoration* scheme.

Protection and restoration schemes have traditionally been addressed using two concepts:

- Path switching, and
- Line switching.

In path switching, the failure is addressed at the path endpoints (i.e., the path initiating and terminating nodes), whereas in line switching the failure is addressed at the transit node where the failure is detected.

Path switching can be further subdivided into *path protection*, and *path restoration* (as illustrated in Figure 1.3).

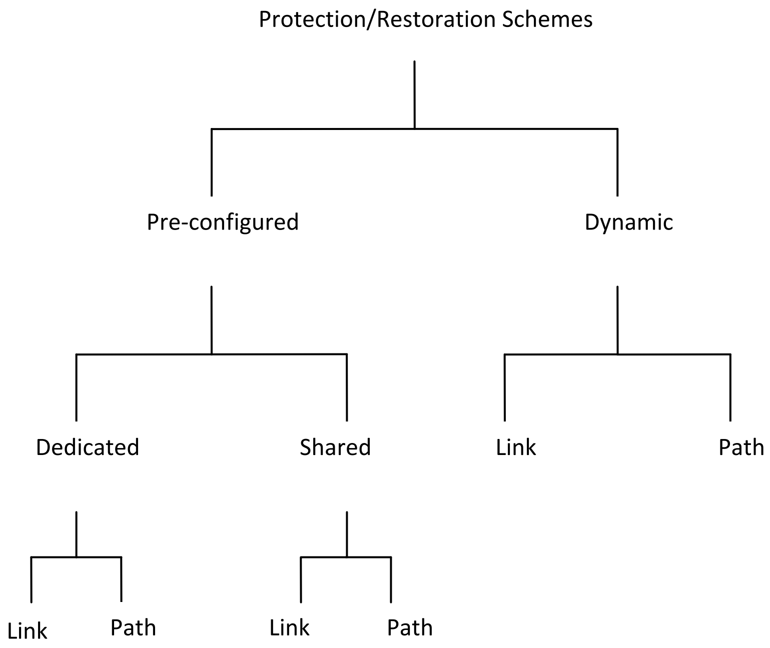


Figure 1. 3 Different Protection/Restoration schemes

1.3.1 Path Protection

In path protection, the source and destination nodes of each connection statically reserves backup paths on an end-to-end basis during call setup.

When the primary path of the connection fails (1-4-5-6 in Figure 1.4), the same connection is rerouted end to end from its source to its destination along the pre-reserved backup path (1-2-3-6). The backup and the primary paths must not share the same risk; and as such they are link disjoint, which is the case of the primary and backup paths presented in Figure 1.4.

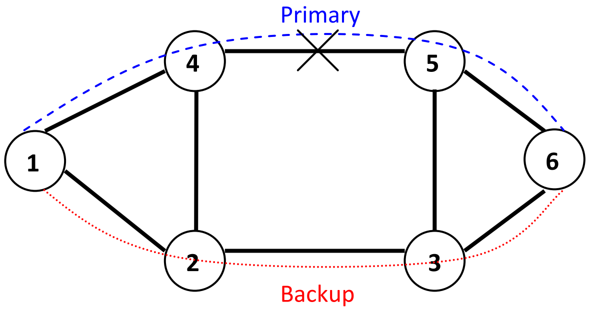


Figure 1. 4 *Path protection*

The nomenclature for path protection is as follows [MAN 06, PAP 06]:

1+1 protection: when using this type of protection, the connection is duplicated at the source node (Node 1 in Figure 1.4) on both the primary and backup paths, and a selector is used at the receiving node (Node 6) to choose the best signal. If the primary path fails, the destination simply switches over to the backup path and continues to receive data. This form of protection is very fast and requires no signaling protocol between the two ends. However, the disadvantage of the 1+1 protection is the waste of bandwidth.

1:1 dedicated protection: In 1:1 protection, there will always be two disjoint paths from source to destination. However, traffic is transmitted only along the primary path. In case of primary path failure, the source and destination both switch over to the dedicated backup path. Signaling is thus required between source and destination. For this reason, 1:1 protection is not as quick as 1+1 protection in restoring traffic. More valid is its advantage. In normal operation, the unused protection path can be used for transmitting low-priority traffic (Extra traffic), and a better network utilization can be achieved. In case of failure of the primary path, the traffic is switched over to the protection path, and the extra traffic is dropped.

M:N shared protection: M pre-allocated backup paths are shared under this scheme between N primary paths; however, data is not replicated onto a backup path, but is assigned and transmitted along the backup path only on the failure of the primary path. This scheme is thus more capacity efficient when compared with 1+1, and 1:1 protection schemes.

1:N shared protection: 1 pre-allocated backup path is shared among N primary paths.

1.3.2 Path Restoration

Restoration implies the discovery of backup resources dynamically in the network to restore affected connections; that is, the resources used for recovery are not reserved at the time of connection establishment, but are chosen from available resources when the failure occurs.

In the particular case of path restoration, traffic is switched to an alternate route after failure occurrence on an end to end basis. In other words, the source node of a connection traversing a failed link participates in discovering a backup route to recover the broken connection. If no backup route is discovered, that connection is blocked.

1.3.3 Link Protection

In link protection (as illustrated in Figure 1.5), all the connections that traverse the failed link are routed around that link. The source and destination nodes of the connections traversing the failed link are oblivious to the link failure. In link protection, during connection setup, backup resources are reserved around each link of the primary path. Upon failure occurrence, recovery is performed around the failed link. For example in Figure 1.5, when fiber 4-5 fails, the connection is restored by node 4 along 4-2-3-5.

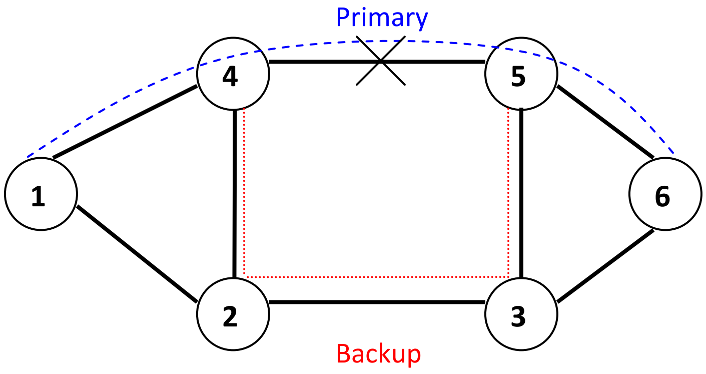


Figure 1. 5 ***Link protection***

The following taxonomy for link protection exists in the literature [LIU 02]:

- Dedicated link protection: At the time of call setup, for each link of the primary path, backup resources are reserved around that link, and are dedicated to that call.
- Shared link protection: In shared link protection, for each link of the primary path, backup resources are always reserved around that link. However, these backup resources may be shared with other backup paths. As a result, backup resources are multiplexed among different failure scenarios (which are not expected to occur simultaneously), and therefore share-link protection is more capacity efficient than dedicated-link protection.

1.3.4 Link Restoration

In link restoration, the node which is adjacent to the failed link discovers dynamically a route around the link in order to restore the affected connection. If no such route is found, the connection is blocked.

Considering the scenario presented in Figure 1.5, if node 4 will be unable to reserve backup resources (due to lack of capacity) upon the failure of the 4-5 link, the connection routed initially along the primary path 1-4-5-6 will not be recovered.

Chapter 2

Priority Aware Protection Scheme

The following conclusions can be drawn from Chapter 1:

- With regard to network resource utilization, restoration schemes are more resource efficient than protection schemes. However, protection schemes prove to have faster recovery time compared to restoration schemes.

- While path protection leads to efficient utilization of backup resources, link protection provides shorter recovery time. Therefore, in this study we focus our attention on path protection schemes. In addition, since shared path protection is more efficient in terms of capacity usage than dedicated path protection, we deal in this document mainly with the impact that shared path protection has on the availability of optical connections.

To the best of our knowledge what still lacks in existing literature is a systematic methodology to efficiently select a cost-effective protection scheme for each connection, while satisfying its availability requirements. The problem of how connection availability is affected by network failures is currently capturing the attention of the optical research community. Contributing to the design of new availability-aware protection schemes we propose in this chapter a first extension to the existing shared path protection scheme (described in section 1.3). The proposed extension is based on the following observation. To date, the majority of the work on shared protection 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 availability requirements of the remaining failed connections. Hence, the unrecovered connections are penalized and remain in an unprotected state until either their primary paths are repaired or until backup resources are released.

From a quality of service perspective, the existing scheme is not optimal since it does not account for the different availability requirements of the primary connections during recovery.

To cope with such a limitation, this chapter proposes to introduce a relative priority among the failed primary connections sharing the same backup resources. The priority of a failed connection is determined by its availability requirement; the higher the requirement is the higher the priority of the connection would be. In this way, if a low priority connection fails before a high priority one breaks down, the low priority connection will be granted access to the backup resources. But, once a high priority connection fails, it will be given the privilege of using the backup resources irrespective of the recovered low priority connections. In other words, a failing high priority connection is allowed to preempt the previously recovered lower priority connections if there are any. In order to gauge the benefits of the proposed priority-aware shared protection scheme, its impact on the availability of an optical connection needs to be studied and to be contrasted to that of the existing shared protection schemes.

Therefore, this chapter presents a mathematical model for both the classical and priority-aware shared protection schemes. Analytic expressions for the average availability resulting from the deployment of such schemes are derived. By solving these models, the service differentiation feature introduced by the proposed scheme is numerically evaluated.

2.1 Proposal

The priority-aware protection scheme is an extension to the existing shared M:N protection schemes. This novel scheme introduces relative priorities to different primary connections that share common backup paths.

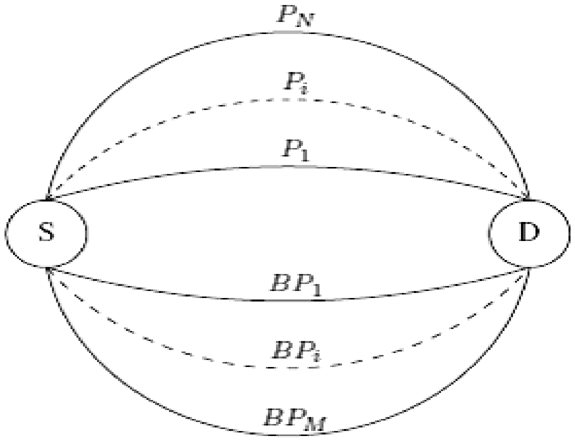


Figure 2. 1 N *primary Paths Sharing M Backup paths*

Consider N primary paths sharing M backup paths having same source and destination nodes. Each primary and backup path has a probability of failure. In the existing classical models, all connections are considered to have equal probability to be restored by backup paths.

In our proposed model, we divide the N primary connections into K sets of priority classes $C_1..C_k$, Let N_i primary connections belong to class C_i . Let the connections with class C_1 have the highest priority and those of class C_k with lowest priority.

First, we consider the case when primary path holding connection t, which belongs to Ci, fails & backup path is available. This will result in having connection t occupy the backup path.

Second, when primary path holding connection t fails and the backup is in use. Then a check will be made: if the backup is occupied by a lower class connection, then t will preempt that connection and occupy the backup path. However, if the backup path is occupied by similar or higher class connection then connection t will be blocked.

Third, when both the primary path holding connection t and the backup path are down, then connection t will be blocked.

2.2 Mathematical Model

In this section, we present a mathematical model for the availability of 1:N priority aware shared protection scheme. Then we will develop a mathematical model considering multiple backup paths to derive the analytical expression describing the M:N priority-aware shared protection scheme.

2.2.1 Basic Assumptions

We base our mathematical study on the following assumptions:

- A connection has 2 states : available or unavailable
- A path, whether primary or backup, is either up state (operational) or down state (failed).
- Failures of network components are independent of each other
- Sufficient resources are available to repair simultaneously any number of failed connections. This is referred to in literature as *unlimited repair*.
- A path fails when at least one of its components fail or is defective.

2.2.2 Analytical Model

Cable cut is proven, in the introduction, to be the main cause of primary paths failures. For simplicity we will set λ to be the failure cut rate where:

$$\lambda = \text{path length x cable cut rate/ unit length.}$$

2.2.2.1 Modeling Classical Shared Protection Scheme 1:N

Consider a system where we have 1 backup path shared among N primary paths.

Let λ_i , $i=1,\ldots N+1$ be the mean failure rate of the i-th path.

Let μ_i , i=1,…N+1 be the mean repair rate of the i-th path.

Thus the Mean Time to Failure (MTTF) = $1/\lambda_i$ and

the Mean Time to Repair (MTTR) = $1/\mu_i$

MTTF and MTTR are exponentially distributed.

We also consider that all paths including backup have identical λ and μ.

Let $\rho = \lambda/\mu$, therefore the probability of having path i available at t→ ∞ (steady state):

$$A_i = p = \frac{MTTF}{MTTF+MTTR} = \frac{1/\lambda}{\frac{1}{\lambda}+\frac{1}{\mu}} = \frac{1}{1+\rho} \text{ = Availability of path i} \qquad \textbf{(2.1)}$$

Where the Unavailability = $1 - A_i = \overline{A}_i = q$

Let p(n) be the probability of having n failed paths at time t. Using the transition diagram in Figure 3.2 we can conclude the following expression from the Markovian chain :

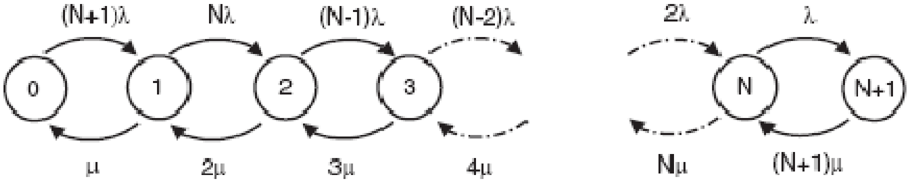


Figure 2. 2 Transition diagram for number of failed paths

$$p(n) = \binom{N+1}{n} q \cdot p^{(N+1-n)} \qquad \textbf{(2.2)}$$

$$= \frac{(N+1)!}{n!(N+1-n)!} \frac{\rho}{(1+\rho)^{N+1}}$$

Where $\binom{N+1}{n}$ is the number of all combinations of n out of N+1 paths.

When n ≥ 1, we consider 2 cases

1- Backup failed and thus the remaining n-1 failed connections will be blocked since no backup path available
2- Backup is operational and 1 connection is restored, keeping n-1 connections blocked.

We clearly note that in both cases n-1 connections will be blocked. Therefore only when n=1 there will be no unavailable connection, otherwise at least 1 connection will be unavailable.

We define the following events:

Y(n) = event that connection t is unavailable, given that we have n failed primary paths

W(n) = the event that the backup path and the path holding connection t are failed

Z(n) = the event that the backup path is operational while path holding connection t is failed.

p(n) P(Y(n)) = probability of having connection t unavailable given that we have n failed primary paths.

⇨ $$P(Y(n)) = P(Y(n)/ W(n))\, P(W(n)) + P(Y(n)/ Z(n))\, P(Z(n)) \qquad (2.3)$$

In event **W(n),** connection t is unavailable since there are no backups to restore it when its primary path is failed. Thus **P(Y(n)/ W(n)) =1.**

On the other hand, when the backup path is operational and primary path holding t failed, then only 1 connection out of n failed will be restored by the backup. Thus we can conclude that $P(Y(n)/ Z(n)) = \frac{n-1}{n}$ **.**

The probability of having both primary path holding t and backup path are down, can be calculated by dividing the all possible combinations that covers cases when primary path holding t and back up are failed, over the combinations of having n failed paths out of the N+1 paths in the system.

⇨ $$P(W(n)) = \frac{C_{N-1}^{n-2}}{C_{N+1}^{n}} = \frac{n(n-1)}{N(N+1)} \qquad (2.4)$$

To get the P(Z(n)), we divide all possible combinations of having t belong to the failed connections while the backup is operational, over the possible combinations of having n failed paths out of the N+1 paths in the system.

$$\Rightarrow \quad \mathbf{P(Z(n))} = \frac{C_{N-1}^{n-1}}{C_{N+1}^{n}} = \frac{n(N+1-n)}{N(N+1)} \qquad \textbf{(2.5)}$$

Using the above equations we can

$$\Rightarrow \quad \mathbf{P(Y(n))} = \frac{n-1}{N} \qquad 2 \leq n \leq N+1 \qquad \textbf{(2.6)}$$

Noting that when n=1, **P(Y(n))=** 0 which is true since all connections will be available.

We conclude from the above calculations that the unavailability of a connection t in 1: N classical shared scheme is:

$$U = \sum_{n=2}^{N+1} p(n)P(Y(n)) \qquad \textbf{(2.7)}$$

By substituting the above equations we get:

$$U = \frac{1}{N} \sum_{n=2}^{N+1} \frac{(n-1).C_{N+1}^{n} .\rho^{n}}{(1+\rho)^{N+1}} \qquad \textbf{(2.8)}$$

Where Availability = 1- U

2.2.2.2 Modeling Priority Aware Shared Protection Scheme

In our proposed model, we will divide the primary connections in to 2 sets of priority classes. Let the high priority class be the “Gold” class while the low priority class be the “Silver” class.

N_1 = # of Gold connections N_2 = # of silver connections.

Since Gold connections can preempt any silver connection occupying the backup then the same analytical expression derived for classical shared protection scheme can be applied with N_1

instead of N. Thus the expression for the unavailability of the high priority class connections can be written as follows:

$$U_{\text{gold}} = \frac{1}{N1} \sum_{n=2}^{N1+1} \frac{(n-1).\mathrm{C}^{\mathrm{n}}_{\mathrm{N1+1}} .\rho^{n}}{(1+\rho)^{N1+1}} \qquad \textbf{(2.10)}$$

On the other hand, the Silver connections are unavailable if any of the following conditions apply:

1- E1= Primary path holding connection t failed & Backup path is down
2- E2= Primary path holding connection t failed & Backup path is operational but at least 1 Gold connection is among the n failed connections.
3- E3= Primary path holding connection t failed & Backup path is operational but another Silver connection occupies the backup path.

Let n1= # of failed Gold connections and n2 = # of failed silver connections

Let b= 1 when backup path is down otherwise its 0.

Since the probabilities of having n_1 & n_2 failed connections are independent, as well as independent to the state of the backup, we can write the following statement:

$$P(n_1,n_2,b) = P(n_1)P(n_2)P(b) \qquad \textbf{(2.11)}$$

The probabilities $P(n_1)$ & $P(n_2)$ can be defined by :

$$P(n_1) = \binom{N1}{n1} \bar{A}^{n1} A^{N1-n1} \qquad \textbf{(2.12)}$$

$$P(n_2) = \binom{N2}{n2} \bar{A}^{n2} A^{N2-n2} \qquad \textbf{(2.13)}$$

Whereas the probability of having P(b) can be defined by :

$$P(b) = \bar{A}^{b} A^{1-b} \qquad \textbf{(2.14)}$$

To achieve the 3 conditions mentioned above, the following inequalities should be satisfied.

E1 satisfied when b=1

E2 satisfied when b=0 and n1≥ 1

E3 satisfied when b=0, n_1=0 and n_2≥2

The probability that connection t, belonging to Silver class, fails under state n_1,n_2, b is :

$$\text{P(t fails in state } (n_1,n_2, b)) = \frac{\binom{N2-1}{n2-1}}{\binom{N2}{n2}}$$

Therefore the unavailability of silver connection can be calculated by evaluating equation 3.15 by summing over all the values of $\mathrm{n1, n2, b}$

$$\mathrm{U_{silver}} = \sum \mathrm{P\big(t\ fails\ in\ state\ (n1, n2, b)\big)}\ P(\mathrm{n1, n2, b})\ P(\ E1\ U\ E2\ U\ E3) \qquad \textbf{(2.15)}$$

$$\mathrm{U_{silver}}= \sum_{i=2}^{N_2+1} \binom{N_2-1}{i-2} q^i p^{N_2-i+1} \ + \sum_{i=1}^{N_2} \binom{N_2-1}{i-1} q^i p^{N_2-i+1}.\ (1-\mathrm{p}^{\mathrm{N}_1})$$

$$+\sum_{i=2}^{N_2} \binom{N_2-1}{i-1} q^i p^{N_2-i+1}.\ \mathrm{p}^{\mathrm{N}_1}\, \frac{\mathrm{(i-1)}}{\mathrm{i}} \qquad \textbf{(2.16)}$$

2.2.2.3 Modeling Multiple backups- Priority Aware Shared Protection Scheme

In this section we develop an analytical model for N primary paths sharing M backup paths. We will keep the same assumptions as the previous section, by considering 2 priority classes, Gold and Silver. We consider the stochastic process X(t) having a state denoted by the triplet n_1,n_2,m, where n_1 and n_2 represent the number of failed Gold and Silver connections respectively, whereas m represents the number of *operational* backups.

N1= # of Gold connections

N2= # of Silver connections

M= # of backups

n_1= # of failed gold connections

n_2= # of failed silver connections

m= # of operational backups

Since failure of any path is independent of the other then we can have:

$$p(n_1, n_2, m) = p_1(n_1)\, p_2(n_2)\, p(m) \qquad \textbf{(2.17)}$$

Let the availability $A_i = \frac{MTTF}{MTTF+MTTR}$ be denoted by "p",

whereas the Unavailability = 1- A_i =$\overline{A}_i$ be denoted by "q".

Then as proven in the section 3.2.2.2,

$$P(n_1) = \binom{N1}{n1} q^{n1}\, p^{N1-n1} \qquad \textbf{(2.18)}$$

$$P(n_2) = \binom{N2}{n2} q^{n2}\, p^{N2-n2} \qquad \textbf{(2.19)}$$

Whereas the probability of having P(b) differs from the previous section since multiple backups are considered and the probability of having m operational backups can be defined by :

$$P(m) = \binom{N2}{n2} p^{m}\, q^{M-m} \qquad \textbf{(2.20)}$$

Calculating the Unavailability for Gold connections

Connection t, belonging to Gold class, is unavailable when both of the following conditions are satisfied:

1- A : primary path holding connection t is down
2- B: connection t is not restored by any of the backup paths.

⇨ $U_{gold} = P\ \{A,B\}$

$$= \sum_{n1=1}^{N1} \sum_{n2=0}^{N2} \sum_{m=0}^{M} P\{B/\ A\ , X\ =\ (n1, n2, m)\}\ \ P\{A\ /X\ \ =\ (n1, n2, m)\}\, p(n1, n2, m)$$

(2.21)

The probability of having condition A satisfied given state X, is equal to the number of failed gold connections, divided by the total number of gold connections.

⇨ $P\{A\ /X\ = (n1, n2, m)\} = \frac{n1}{N1}$

The probability of having condition B satisfied while given condition A and state X, is always equal to zero except in the following case:

$P\{B/\ A\ , X = (n1, n2, m)\}\ \neq 0$ When:

m < n₁ , in this case only m out of the n_1 failed gold will be restored and thus the probability of having connection t not restored is : 1 - $\frac{m}{n1}$

⇨ U_{gold}=

$$\frac{1}{N1} \sum_{n1=m+1}^{N1} \sum_{m=0}^{n1-1} (n1 - m)\ \mathrm{p}(n1) p(m)$$

(2.22)

<u>Calculating the Unavailability for Silver connections</u>

Similarly, we consider connection t , belonging to the Silver class of service.

1- A : primary path holding connection t is down
2- B: connection t is not restored by any of the backup paths.

⇨ U_{silver} = P {A,B }

=

$$\sum_{n1=0}^{N1} \sum_{n2=1}^{N2} \sum_{m=0}^{M} P\{B/\ A\ , X = (n1, n2, m)\}\ X\ P\{A\ /X\ = (n1, n2, m)\}\ \mathrm{p}(n1, n2, m)$$

The probability of having condition A satisfied, given state X, is equal to the number of failed silver connections divided by the total number of Silver connections.

⇨ $P\{A\,/X\ =(n1,n2,m)\}=\frac{n2}{N2}$ **(2.23)**

The probability of having condition B satisfied, given condition A and state X, is always equal to zero except in the following cases:

⇨ $P\{B/\,A\,,X=(n1,n2,m)\}\ \neq 0$ When:

1- **$m < n_1$** , in this case the number of failed Gold connections exceed the available backups, and that will result in having Gold connections occupying all the operational backups leaving no place for restoring connection t since it belongs to lower class. Thus the probability of having connection t blocked is equal to **1**.

2- **$n_1 \leq m$ and $n_1+n_2 > m$** , in this case n_1 gold connections will occupy n_1 operational backups while the remaining operational backups will restore $(m–n_1)$ out of the n_2 failed silver connections. Thus the probability of having connection t among the blocked connections is : **1-** $\boldsymbol{\frac{m-n1}{n2}}$

Therefore, the Unavailability of Silver connection can be expressed by:

$U_{silver} =$

$$\frac{1}{N2}\Big[\sum_{m=0}^{M}\ \sum_{n1=m+1}^{N1}\ \sum_{n2=0}^{N2} n2\ \ \mathrm{p}(n1,n2,m)$$

$$+\sum_{m=0}^{M}\ \sum_{n1=0}^{m}\ \sum_{n2=m-n1}^{N2}\ (n1-n2-m)\ \ \mathrm{p}(n1,n2,m)\ \Big]$$

(2.24)

2.3 Analysis

In our data analysis we will evaluate the benefits of the proposed scheme. We will compare priority-aware protection scheme with the classical protection scheme in order to pin point the improvements introduced. We will also study the effect of several factors, such as distance, multi backup paths, cut rate, mean time to repair and variation in number of gold connections, in order to understand the pros and cons of the proposed scheme.

2.3.1 Effect of distance variations & multi backup paths

We start our analysis by comparing the priority-aware scheme with the classical share protection scheme. In this section, we will base our comparisons on the results achieved from varying the cable distance as well as adding multiple backup paths.

In the first example, we base our calculation on equations 2.8 and 2.16 .We vary the distance between 600 and 1400 Km, and compare priority aware protection scheme with Classical protection scheme for a system having 10 primary connections and 1 backup path. We consider 4 gold connections and 6 silver, while we set the MTTR to be 12hrs and the cut rate to be 4.39 cuts/yr / 1000miles.

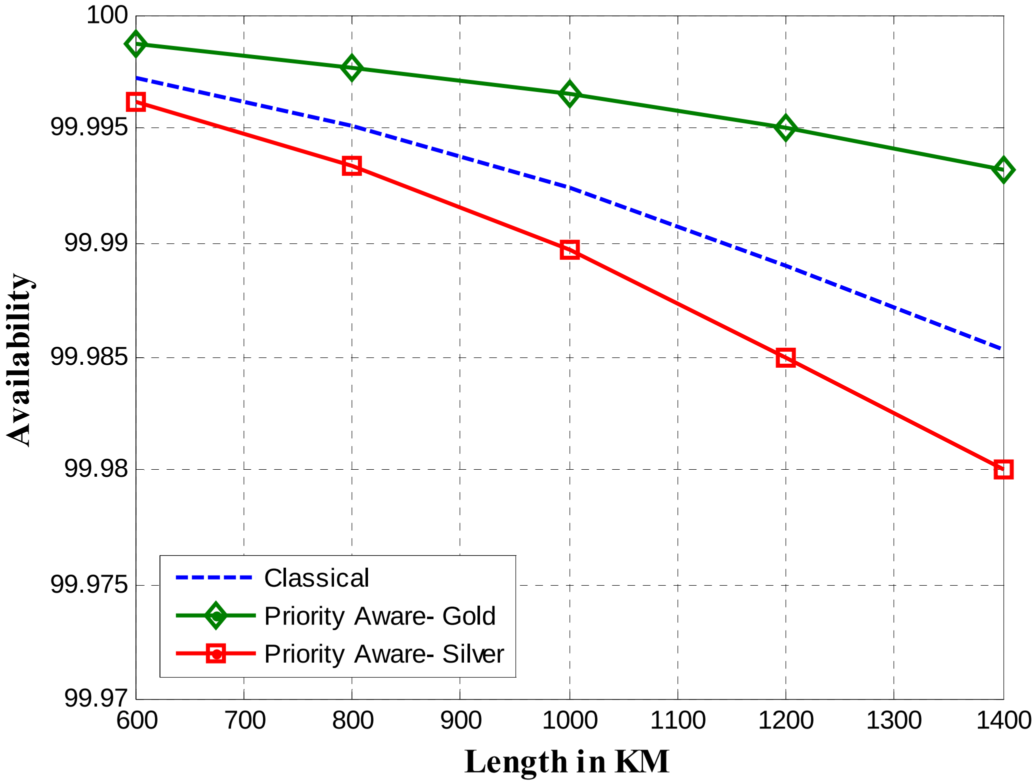


Figure 2. 3 Availability for classical and priority aware 10:1 protection schemes

We observe from figure 2.3 that our proposed scheme resulted in a higher availability for the Gold class connections compared to classical shared scheme. From quality of service point of view, 99.99% is required for Gold clients, whereas 99.9% required for silver clients. SLA requirements for both service classes are satisfied over a fiber length of 1400 Km while using the priority-aware protection scheme. On the other hand, the availability dropped below 99.99% while using the classical shared protection, which does not satisfy the requirement of the High class connection. Achieving the desired availability levels for both classes over a distance of 1400 km encourages operators to use the proposed scheme in the backbone networks.

For a better understanding of the effect of increasing cable length, we will increase the distance beyond 3000Km. We will consider the same assumptions as the previous example while varying the distance between 3200 and 4000 Km as an extreme case, to have a more precise idea about the availability of optical connections connecting continents under sea.

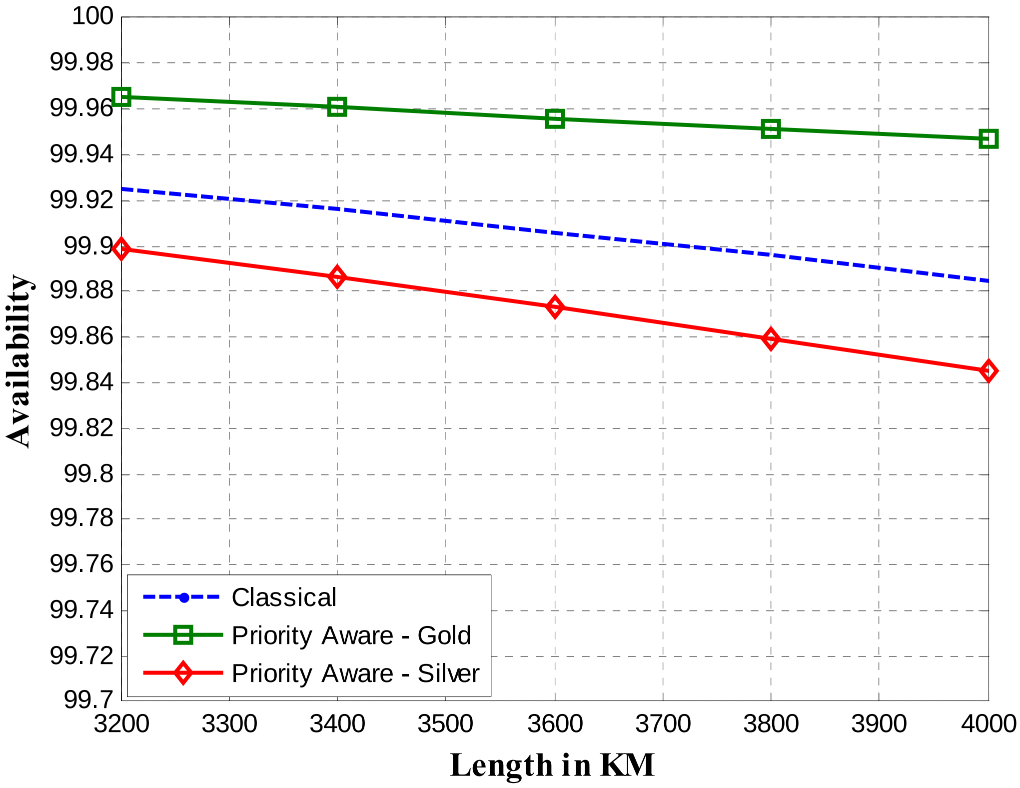


Figure 2. 4 Availability for classical and priority aware protection schemes on long distances

Figure 2.4 shows the decrease in the availability of both gold and silver class connections, due to the increase in distance. The increase in distance led to a drop in availability beyond the required levels. Although the drop wasn't critical, since the Gold clients still achieve availability almost equal to 99.95% over a distance of 4000Km, while the silver connections retained an availability level above 99.84%.

As a solution for the drop in availability, in the following scenario we will add another backup path to the system. This addition, as shown in Figure 2.5, resulted in a remarkable increase in the availability of both Gold and Silver connections. The availability levels reached 99.998% for Gold clients and 99.99% for silver clients over a distance of 4000Km, thus satisfying the requirements of both service classes.

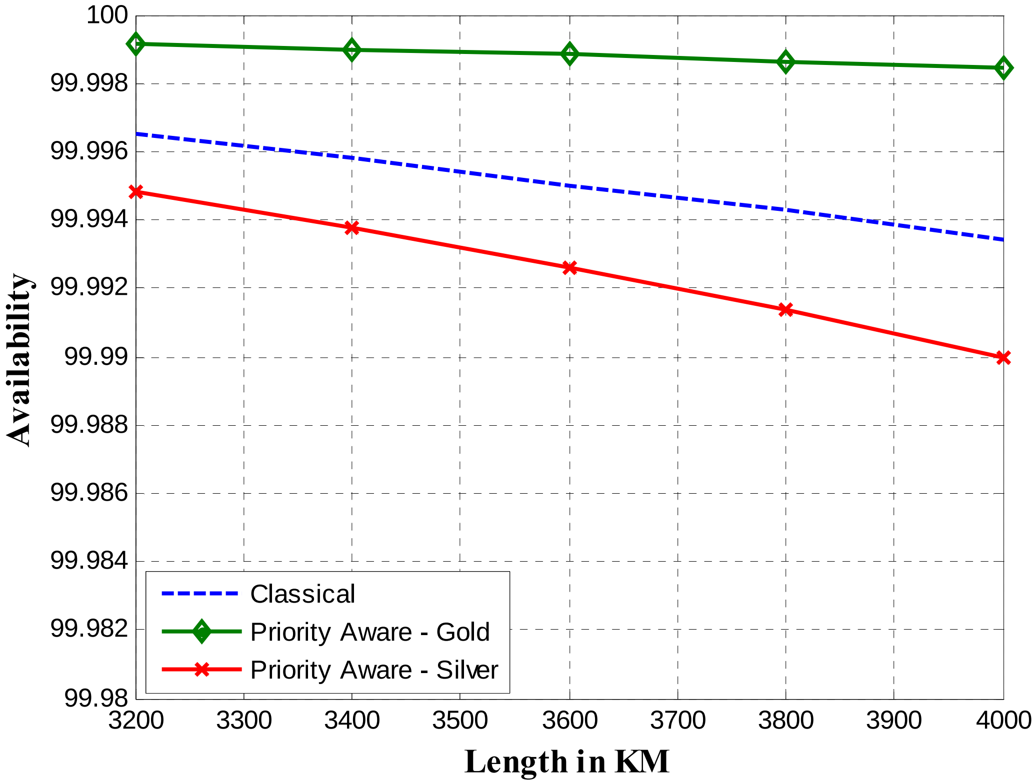


Figure 2. 5 Availability for classical and priority aware protection schemes with 2 backup paths

2.3.2 Effect of cut rate

As mentioned in Chapter 1, fiber cut is the main reason for connection failures. Several causes of fiber cuts have been reported such as dig ups, vehicle induced damage and human error in cases where a craftsman cuts the wrong cable during maintenance process or during cable salvage activities. Having all those factors involved in the average cut rate, makes it a critical parameter to study. In this section, we will vary the cut rate between 4 cuts/year/1000miles and 12 cuts/year/1000miles.We consider 4 gold connections and 6 silver, while we set the MTTR to be 12hrs and the cable length to be 2000Km.

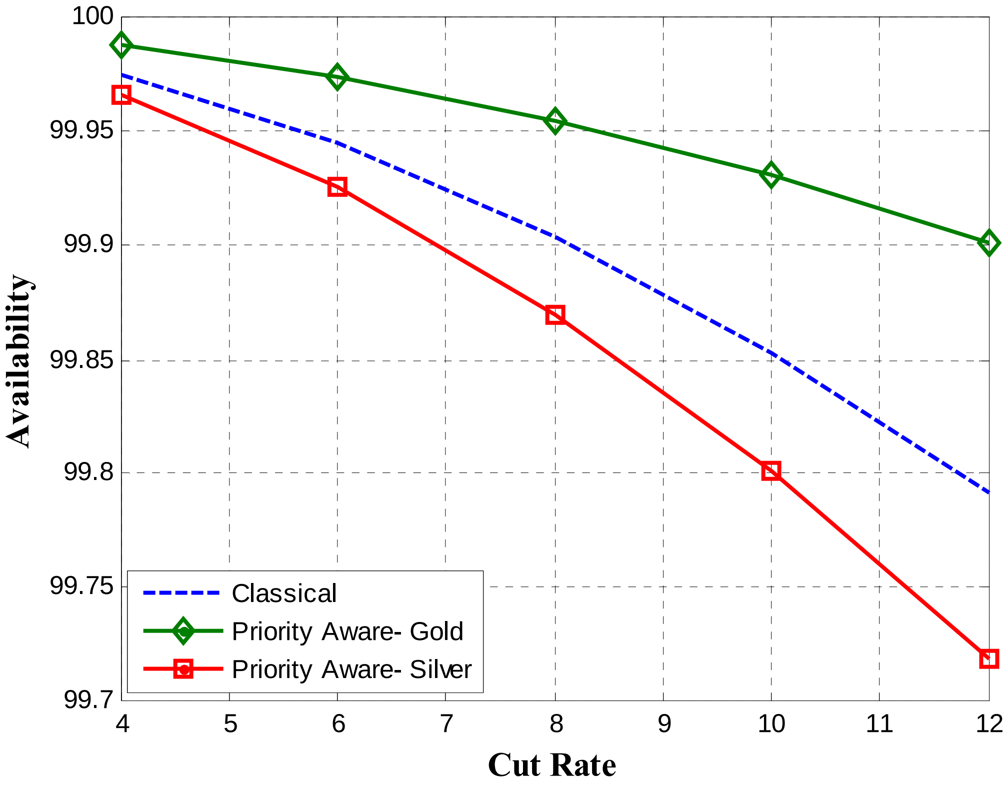


Figure 2. 6 Cut Rate effect on availability for classical and priority aware protection schemes

Based on Figure 2.6, we notice that a minor increase in cut rate can result in a drastic decrease in the availability of the connections under study. Increasing the cut rate from 4 to10 has decreased the availability of Gold clients from the order of 99.99% to 99.9%, whereas the silver connections were severely penalized and their availability decreased from the order of 99.96% to values around 99.72%.

The introduction of the priority-aware protection scheme provided a better reliability for Gold clients as compared to the classical approach. Based on Figure 2.6, we can clearly note that for Gold class connections, 99.9% availability was achieved with cut rate equal to 12 cuts/year/1000miles, while the same availability was reached only at 8 cuts/year/1000miles using the classical shared protection scheme.

Availability of gold and silver class connections dropped beyond 99.99% and 99.9% respectively, when exceeding an average cut rate of 5 cuts/year/1000miles. Thus maintaining a low cut rate is essential for reliable network.

2.3.3 Effect of Mean Time to Repair

Another significant parameter to consider is the mean time to repair (MTTR). Several improvements are being implemented in the field of fiber cabling, and new techniques are being used to repair fiber cuts with minimum downtime. Most of the recent serious fiber cuts where located in remote, difficult to reach places, such as ocean grounds where the time to repair can exceed 24hrs. In short, repair time vary widely between different fiber networks depending on their geographic locations, which makes MTTR a parameter worth considering while studying the availability. To study the effect of MTTR on the availability of connections, we vary this parameter between 6 and 16 hours, while keeping other parameters, as in previous examples, to have 4 gold and 6 silver connections and 1 backup path. We also stick to a cut rate of 4.39 cuts/yr/1000 miles and a fiber cable with length equals to 2000Km.

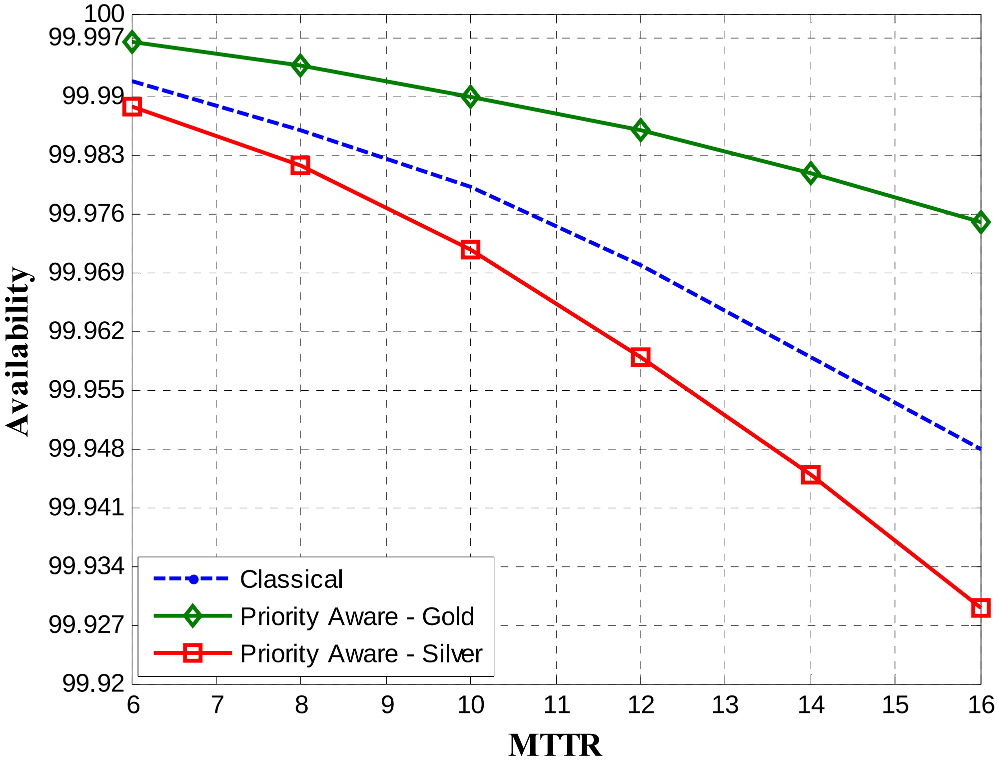


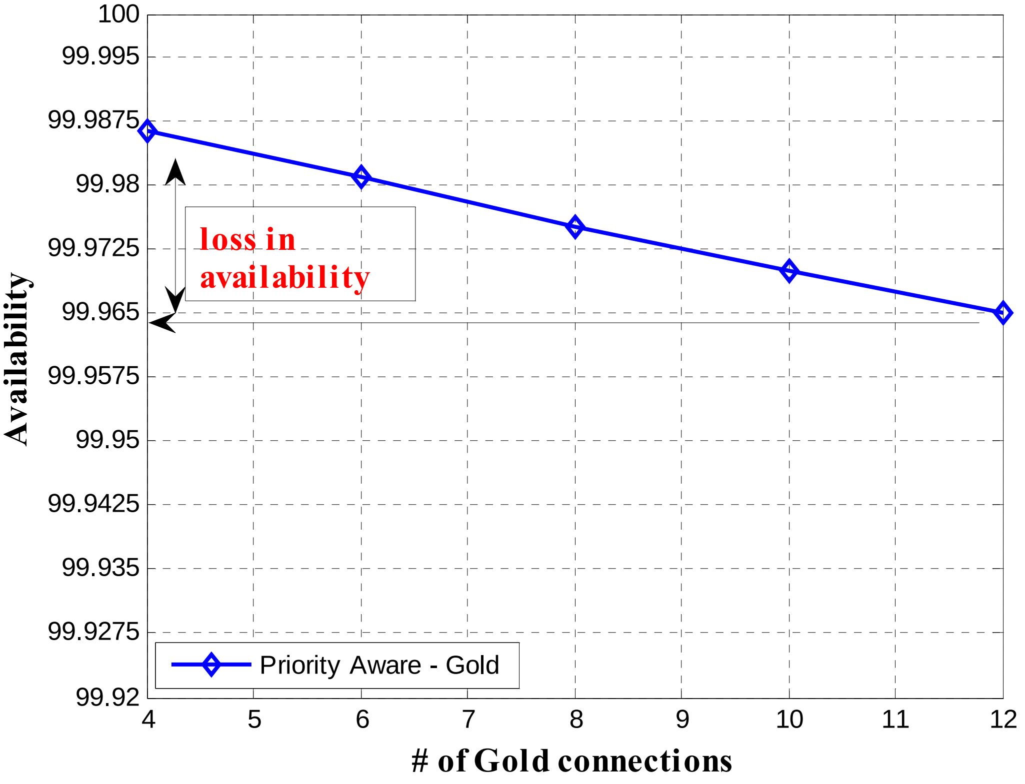
Figure 2. 7 MTTR effect on availability for classical and priority aware protection schemes

Based on figure 2.7, we can deduce that as MTTR increases to values around 16 hrs, the availability of the classical protection scheme drops beyond 99.95% while priority aware scheme preserved availability not less than 99.98% for Gold connections. Thus introducing class differentiation adds to the Quality of service provided, even when the mean time to repair increases due to technical or geographical reasons.

2.3.4 Effect of Increasing # of Gold Connections

Variation in the number of Gold and silver connections is another variable to be considered specifically by operators who desire to have high levels of availability specially with increasing number of clients. Adding the number of silver connections in a network, while following priority-aware scheme, would have very minor effect on the availability of both silver and gold connections. This minor effect is due to the preemption process during Gold connection failures. On the other hand, increasing the number of Gold connections would result in decreasing the availability of Gold connections, since failing gold connections will be competing to occupy the operating backup paths.

To study the effect of increasing the number of Gold connections, we vary the number of Gold connections between 4 and 12. We fix the distance to 2000 Km, as well as we set the number of silver connections to 6, MTTR to 12 hrs and the cut rate to 4.39 cuts/yr / 1000miles.



.

Figure 2. 8 Decrease in availability due to the introduction of Gold connections

As shown in Figure 2.8, tripling the number of Gold connections dropped the availability from 99.986% to 99.965%. This loss in availability is not critical, but should always be considered by operators to set an upper limit to the number of gold subscribers in order to ensure reliability based on the service level agreement.

2.4 Conclusion

The proposal of priority-aware shared protection scheme added major improvements to the existing shared protection schemes through introduction of relative priorities among the different primary connections sharing the same backup paths.

While increasing the length of a fiber cable, high priority connections provided an improved level of availability compared to classical shared protection scheme. Also it was noted that the priority-aware protection scheme offered better reliability when the mean time to repair increased. Thus, the priority aware scheme succeeded to preserve high levels of availability for the high class connections with different parameter variation in the network.

During result analysis, several drawbacks can be highlighted for the newly proposed scheme. It was shown evidently that the low class connections were penalized. On the other hand, the availability of high class connections dropped dramatically during the increase of the cut rate. Finally, it was noted that when the number of high class connections increase, during simultaneous failures, these connections will be competing over the backup paths and thus dropping the availability of high class connections. Overcoming those drawbacks using the proposed or the classical scheme can only be achieved by increasing the number of backup paths, which implies increasing the cost of installation, maintenance and operation. In the following chapter, we will propose a novel improvement to the priority-aware shared protection scheme that will provide a cost effective solution to the above mentioned drawbacks.

Chapter 3

Hard Preemption Protection Scheme

The analysis of the newly introduced priority-aware shared protection scheme showed that the connection availability was severely penalized at high cut rates. It was also noted that an increase in the mean time to repair might result in a decrease in the availability of Gold class connections beyond the acceptable limits agreed on between operators and clients as stated in the Service Level agreement (SLA). In many real life circumstances, the time to repair a fiber cut can be days and sometimes weeks due to difficulties encountered during the maintenance processes. Based on the results achieved in the prior section, adding extra backup paths will retain the availability of connections above the recommended levels.

Backup paths are the longest disjoint paths between a source and a destination. Increasing the number of backup paths is expensive and resource inefficient. Adding redundant resources to improve network survivability is not always the preferred technique that operators would like to pursue to achieve a highly reliable and available network.

3.1 Proposal

Hard Preemption Protection scheme is a novel improvement based on the proposed Priority-aware protection scheme. This extension's main purpose is to improve the availability of higher class connections in a cost effective manner. In hard preemption, a higher class connection, when blocked due to a failure in its primary path and the lack of any backup path, can preempt a connection from a lower class and occupy its *primary path*. The lower class connection will stay blocked until a backup path is available or until the primary path of the higher class connection is repaired. Thus the higher class connections will be using both, backup paths and lower class primary paths, as backup resources.

Consider N primary paths sharing M backup paths having same source and destination Nodes. Each primary and backup path has a probability of failure. In the priority shared protection scheme, connections are considered to have different probabilities, according to their class of service, when restored by backup paths.

In our proposed model, we divide the N primary connections into K sets of priority classes $C_1..C_k$, Let N_i primary connections belong to class C_i . Let the connection with class C_1 have the highest priority and those of class C_k with lowest priority.

First, when the primary path holding connection t, belonging to Ci, fails and backup path is available, then connection t will occupy the backup path.

Second, when the primary path holding connection t fails and the backup is occupied, then a check will be made: if any of the backup paths is occupied by a lower class, then t will preempt that connection and occupy the backup (regular preemption). However, if all the backup paths are occupied by similar or higher class connections then connection t will preempt a lower class connection and occupy its primary path (Hard Preemption).

Third, when the primary path holding connection t fails and all backup paths are down, then connection t will preempt a lower class connection and occupy its primary path (Hard Preemption).

Forth, when connection t belongs to the lowest class of service, if the primary path holding connection t fails and a backup path is available then connection t will be restored, otherwise if no backup is available then connection will be blocked.

Fifth, when primary path holding connection t fails and backups are either occupied by similar or higher class connections, or all backups are down and all the primary paths of lower class connections are either down or occupied by similar or higher class connections, then connection t will be blocked.

Finally, when the primary path holding connection t is up, and a higher class connection fails with no backup paths to restore it, then connection t may be hard preempted and will be blocked with a certain probability, discussed in the analytical model.

Hard preemption scheme provides higher class connections with additional backup paths on the expense of lower class connections. In an attempt to control this penalty, we propose another variable to our model, the preemption quota. The number of acceptable preemptions in the network should never exceed the quota set by the operators and network designers to ensure fewer penalties on low class connections when using the hard preemption scheme. Deciding on an optimal quota depends on several network parameters such as mean time to repair, cut rate, and the number of high and low class connections available.

3.2 Mathematical Model

We present the mathematical model for the availability of M:N Hard preemption protection scheme. The analytical model will consider preemption quota .We will develop the analytical model for 2 classes of service.

3.2.1Basic Assumptions

We base our mathematical study on the following assumptions:

- A connection has 2 states : available or unavailable
- A path, whether primary or backup, is either up state (operational) or down state (failed).
- Failures of network components are independent of each other
- Sufficient resources are available to repair simultaneously any number of failed connections. This is referred to in literature as *unlimited repair*.
- A path fails when at least one of its components fail or is defective.

3.2.2 Analytical Model

In this section we derive the analytical expression for the availability of connections using the hard preemption technique. We will start first by deriving the expression for 1:N hard preemption scheme. Afterwards we will develop the complete analytical expression for M:N Hard preemption scheme for two classes of service, gold and silver. The M:N expression will consider a quota M1 on number of Preemptions allowed for Gold class connections.

3.2.2.1 Modeling 1:N Hard Preemption Scheme

Consider a system where 1 backup path is shared among N primary paths.

Let C_i be class of connection i , where C_1 has the highest connection class

Let N_i be the number of primary paths holding connections belonging to class i, where

$\sum_i Ni$ = N = total number of primary connections

Let λ_i , i=1,…N+1 be the mean failure rate of the i-th path.

Let μ_i , i=1,…N+1 be the mean repair rate of the i-th path.

Thus Mean Time to Failure (MTTF) = $1/\lambda_i$ & Mean Time to Repair (MTTR) = $1/\mu_i$

MTTF and MTTR are exponentially distributed.

We also consider that all paths including backup have identical λ and μ.

The availability of path i is denoted by p_i and unavailability be q_i where:

$$p_i = \frac{\mu}{\lambda+\mu} \quad \text{and } q_i = 1 - p_i \qquad \textbf{(3.1)}$$

Let us denote by {pp(t) =0} the event that the primary path holding connection t is down.

P{t is unavailable} = 1 – P { t is available}

P{t is unavailable} = 1- (P{t is available, pp(t) =0}+ P{t is available, pp(t) =1})

For connection to be available while its primary path is down, then it has to be occupying a backup path. On the other hand, a connection whose primary path is up can only be available if it is not hard preempted by a higher class connection.

$$P\{t \text{ is available, } pp(t) = 0\} = \frac{P\{a\ connection\ Ci\ is\ restored\ by\ backup\}}{Ni}$$

$$P\{t \text{ is available, } pp(t) = 1\} = \frac{P\{a\ connection\ Ci\ is\ not\ preempted\}}{Ni}$$

⇨

P {t is available} = 1 - $^{1}/_{Ni}$ (P{ a C_i connection is restored by backup, pp(t) =0}

+ P{ a C_i connection is not preempted, pp(t) =1})

(3.2)

a) **P{ a C_i connection is restored by backup, pp(t) =0}**

Condition A_1 = backup is up

Condition B_1 = at least one C_i connection is down

Condition C_1= all the primary paths of C_j connections are up, where j < i

- ⇨ P{ a C_i connection is restored by backup, pp(t) =0} = $P(A_1)\, P(B_1)\, P(C_1)$

$P(A_1) = P$

$P(B_1) = (1- P_i^{Ni})$

$P(C_1) = \prod_{j=1}^{i-1} P_j^{N_j}$

- ⇨ P{ a C_i connection is restored by backup, pp(t) =0} =

$$= P \,.\, (1- P_i^{Ni}) \,.\, \prod_{j=1}^{i-1} P_j^{N_j} \qquad \textbf{(3.3)}$$

b) **P{ a C_i connection is not preempted, pp(t) =1}**

Condition A_2 = at least one C_i connection is up

Condition B_2 = all the primary paths of C_j connections are up , where j < i

OR

Condition A_2 = at least one C_i connection is up

Condition C_2= Only 1 C_j connection is down and is restored by backup path, where j < i

⇨ P{ a C_i connection is not preempted} = $P(A_2)$ ($P(B_2)$ +$P(C_2)$)

$P(A_2) = 1 - (1 - P_i)^{N_i} = (1 - q_i^{N_i})$

$P(B_2) = \prod_{j=1}^{i-1} P_j^{N_j}$

$P(C_2) = \sum_{j=1}^{i-1} P(\text{Only 1 Cj connection is down and is restored by backup path})$

$$= \sum_{j=1}^{i-1} \left[P\, N_j q_j\, P^{N_j - 1} \prod_{k=1}^{j-1} P_k^{N_k} \right] \qquad \textbf{(3.4)}$$

⇨ P{ a C_i connection is not preempted, pp(t) =1} =

$$= (1 - q_i^{N_i}) \left[\prod_{j=1}^{i-1} P_j^{N_j} + \sum_{j=1}^{i-1} \left[P\, N_j q_j\, P^{N_j - 1} \prod_{k=1}^{j-1} P_k^{N_k} \right] \right] \qquad \textbf{(3.5)}$$

Therefore based on equation 4.2 , Unavailability U_i = P{ t is unavailable} =

$$\mathbf{= 1 - {}^{1}/_{Ni} \left(P.\left(1 - P_i^{N_i}. \prod_{j=1}^{i-1} P_j^{N_j} \right.\right.}$$

$$\mathbf{+ (1 - q_i^{N_i}) \left[\prod_{j=1}^{i-1} P_j^{N_j} + \sum_{j=1}^{i-1} \left[P\, N_j q_j\, P^{N_j - 1} \prod_{k=1}^{j-1} P_k^{N_k} \right] \right] \Big)}$$

(3.6)

3.2.2.2 Modeling M:N Hard Preemption Scheme

Consider a system having M backup paths and N primary paths. For simplicity we consider 2 classes of service gold and silver which denote classes C_1 and C_2 respectively.

We also consider that all paths including backup have identical λ and μ.

The availability of path is denoted by p and unavailability is q where:

$$p = \frac{\mu}{\lambda + \mu} \quad \text{and } q = 1 - p \qquad \textbf{(3.7)}$$

Let N_1 be the number of Gold connections

Let N_2 be the number of Silver connections

$N_1 + N_2 = N$

Let M be the number of Backup paths

Let M1 be the quota on preemptions allowed.

Define the state descriptors as follows:

n_1= # of failed gold connections

n_2= # of failed silver connections

m= # of operational backups

Since failure of any path is independent of the other then we can have:

$p(n_1, n_2, m) = p_1(n_1)\, p_2(n_2)\, p(m)$

Then as proven in the section 3.2.2.3,

$$P(n_1) = \binom{N1}{n1} q^{n1}\, p^{N1-n1} \qquad \textbf{(3.8)}$$

$$P(n_2) = \binom{N2}{n2} q^{n2}\ \ p^{N2-n2} \qquad \textbf{(3.9)}$$

Whereas the probability of m *operating* backups can be defined by:

$$P(m) = \binom{N2}{n2} p^{m}\ \ q^{M-m} \qquad \textbf{(3.10)}$$

Let P(X) be the probability of having state X ={n_1,n_2,m}

<u>Calculating Unavailability for Gold connections</u>

A connection t belonging to Gold class is unavailable in a system with state X , if both conditions are satisfied :

1) A = Primary path ,holding connection t , is down
2) B = t is not restored by neither the backup path nor a primary path of silver connections.

⇨ Unavailability of Gold $U_{gold} = \sum_{x=(n1,n2,m)} P(A, B, X)$

⇨ $U_{gold} = P\{B/A, X). P\{A/X\} .P\{X\}$ **(3.11)**

Since n_1, n_2 &m are independent , then:

$$\mathbf{P(X) = P(n_1)\, P(n_2)\, P(m)} \qquad \textbf{(3.12)}$$

The probability of having primary path holding connection t down, given state X is :

$$\mathbf{P\,(A/X) = \frac{n1}{N1}} \qquad \textbf{(3.13)}$$

The probability of having condition B applied, given condition A and state X, is always equal to zero except in the following conditions:

P (B/A,X) ≠ 0 when :

a) $\underline{(m + N_2 - n_2) \leq M1 \text{ and } (m+N_2-n_2) \leq n_1 \,\&\, n_1 \neq 0}$

In this case, the number of available backups (silver + backups) is less than the quota and less than the number of failed Gold. Therefore, only the number of available backups (silver + backups) will be restored out of n_1 failed Gold connections.

⇨ Unavailable =

$$P(B/A,X) = 1 - \frac{m + N2 - n2}{n1} \qquad \textbf{(3.14)}$$

b) $\underline{(m + N_2 - n_2) > M1 \text{ and } (m + N_2 - n_2) \leq n1 \,\&\, n_1 \neq 0}$

In this case, the number of available backups (silver + backups) is greater than the quota and less than or equal to the number failed Gold connections.

b.1) $\underline{(n_1 + n_2) > m \text{ and } m > M1}$

The number of failed gold and silver exceeds the number of available backups. And the number of operating backups exceeds the quota given the condition in "b". Thus the restored connections will be M1 out of n_1 failed & m-M1 out of all failed connection minus quota.

$$P(B/A,X) = \left(1- \frac{M1}{n1}\right) \left(1- \frac{m- M1}{n1+n2-M1}\right) \quad \textbf{(3.15)}$$

b.2) m < M1

On the other hand, given condition “b”, when the number of operating backups is less than the quota, then the only restored connections will be M1 out of n_1 failed.

$$P(B/A,X) = \left(1- \frac{M1}{n1}\right) \quad \textbf{(3.16)}$$

c) $(m + N_2 - n_2) > M1$ and $n_1 < (m + N_2 - n_2)$ & $n_1 \geq M1$

In this case, the number of available backups (silver + backups) is greater than the quota and less than or equal to the number of failed Gold connections.

c.1) $n_1 > m$

The number of failed Gold exceeds the number of operating backups, while given in “c” that the number of backups (silver + backups) exceeds the quota but still less than the number of failed Gold. Thus this will lead to hard preemption and the probability of blocking a connection can be expressed by the following equation:

$$P(B/A,X) = \left(\frac{(n1-M1)(n1+n2-m)}{n1(n1+n2-M1)}\right) \quad \textbf{(3.17)}$$

c.2) $n_1 < m < n_1 + n_2$

In this case, what differs from the prior case is that the number of failed gold doesn’t exceed the number operating backups, thus no hard preemption and only M1 connections will be restored out of the n_1 failed.

$$P(B/A,X) = \left(1- \frac{M1}{n1}\right) \quad \textbf{(3.18)}$$

Calculating Unavailability for Silver connections

A connection t belonging to Silver class is unavailable in a system with state X, if the following conditions are satisfied:

1) A = Primary path ,holding connection t , is down
2) B = t is not restored by the backup path
3) C = Primary path ,holding connection t , is up
4) D = t is hard preempted on its primary path.

⇨ Unavailability of Silver U_{silver}

$$U_{silver} = \sum_{x} P(A,B,X) + \sum_{x} P(C,D,X)$$

$$U_{silver} = \sum_{x} P(B/A,X)\, P(A/X)\, P(X) + \sum_{x} P(D/C,X)\, P(C/X)\, P(X) \quad \textbf{(3.19)}$$

Since n_1, n2 &m are independent, then:

$P(X) = P(n_1)\, P(n_2)\, P(m)$ as stated in equation 4.12

The probability of having primary path holding connection t down, given state X is:

$$\mathbf{P\ (A/X)} = \frac{n2}{N2} \quad \textbf{(3.20)}$$

While the probability of having primary path holding connection t up, given state X is simply 1- P (A/X), therefore:

$$\mathbf{P\ (C/X)} = 1 - \frac{n2}{N2} \quad \textbf{(3.21)}$$

The conditional probability of having condition B given condition A and state X , as well as the conditional probability of having condition D given A and X , are always equal to zero except in the following conditions:

$P(B/A,X) \neq 0$ when :

a) **$n_1 \geq m$ and $n_1 < M1$:**

In this case all the backups are occupied by Gold connections, therefore a failure in primary path holding a silver connection will result in definite unavailability of this connection.

$$P(B/A,X) = 1 \quad \mathbf{(3.22)}$$

b) $n_1 < m$ and $n_1 < M1$ and $n_2 \geq (m-n_1)$:

In this case not all backups are occupied by failed Gold connections, thus a failed silver connection will be restored by one of the ($m - n_1$) remaining backups.

$$P(B/A,X) = (1- \frac{m-n1}{n2}) \quad \mathbf{(3.23)}$$

c) $n_1 < m$ and $n_1 \geq M1$ and $n_1 + n_2 > m$:

In this case, the quota is exceeded, so the remaining failed Silver and Gold will have equal probability to occupy the remaining backup paths. And all the remaining failed primary connections exceeding m, will not be restored with the following probability.

$$P(B/A,X) = (\frac{n1+n2-m}{n1+n2-M1}) \quad \mathbf{(3.24)}$$

d) $n_1 \geq m$ and $n_1 \geq M1$:

In this case , the number of failed gold connections exceeds the number of operating backups and quota

d.1) $m > M1$ and $n_1 + n_2 > m$

Given condition “d” , when the number of operating backups exceeds the quota, while the total number of failed connections exceeds the number of operating backups, then the restored silver connections can be the difference between total number of operating backups and the quota, divided by the total number of failed connections minus the quota.

$$P(B/A,X) = (1- \frac{m-M1}{n1+n2-M1}) \quad \mathbf{(3.25)}$$

d.1) $m \leq M1$

In this case ,the number of operating backups is less than the quota and the number of failed gold exceeds the number of operating backups, thus there is no chance for any silver connection to be restored.

$$P(B/A,X) = 1 \quad \mathbf{(3.26)}$$

$P(D/C,X) \neq 0$ when :

a) **$n_1 \geq m$ and $n_1 < M1$:**

In this case all the backups are occupied by Gold connections, therefore the remaining failed Gold connections will hard preempt the available silver connections.

If ($n_1 - m \geq N_2 - n_2$)

The remaining failed Gold connections will hard preempt all the available silver connections.

$$P(B/A,X) = 1 \tag{3.27}$$

If ($n_1 - m < N_2 - n_2$)

The remaining n_1-m failed Gold connections will hard preempt silver connection t , under study ,with probability:

$$P(B/A,X) = \frac{n1-m}{N2-n2} \tag{3.28}$$

b) **$n_1 > m$ and $n_1 \geq M1$ and $m < M1$:**

In this case, the number of failed Gold connections exceed the number of available backup paths as well as they exceed the quota , given that the quota is more than the available backups. So (M1-m) failed Gold connections will hard preempt some of the available ($N_2 - n_2$) silver connections. Thus the probability of hard preempting a silver connection is:

$$P(B/A,X) = \frac{M1-m}{N2-n2} \tag{3.29}$$

3.3 Analysis

In this section we will evaluate the benefits of the Hard Preemption scheme. We will compare this new enhanced scheme with the Priority-Aware shared Protection scheme in order to pin point the improvements introduced. Hard preemption scheme will be studied with and without quota. We will also analyze the effect of quota in order to have a clearer comparison with other schemes discussed in this document, in an attempt to find an optimal value for quota.

3.3.1 Comparison with Priority Aware scheme

Improving the Gold connection availability is one of the major benefits achieved by introducing hard preemption. This major improvement in Gold connection availability can aid in reducing the number of backup paths installed. Backup paths are the longest disjoint links between a source and destination nodes. Reducing the number of such long redundant paths will result in a remarkable decrease in the cost of installing, maintaining and operating the network.

To view the improvement introduced, we will compare the hard preemption protection scheme with the priority aware protection scheme. We will study the priority aware scheme with 1 backup and 2 backups, while consider only 1 backup path for the hard preemption scheme. In this example, we base our calculation on equations 3.6 .We vary the distance between 3200 and 4000 Km. We consider 6 gold connections and 2 silver, while we set the MTTR to be 12hrs and the cut rate to be 4.39 cuts/yr / 1000miles.

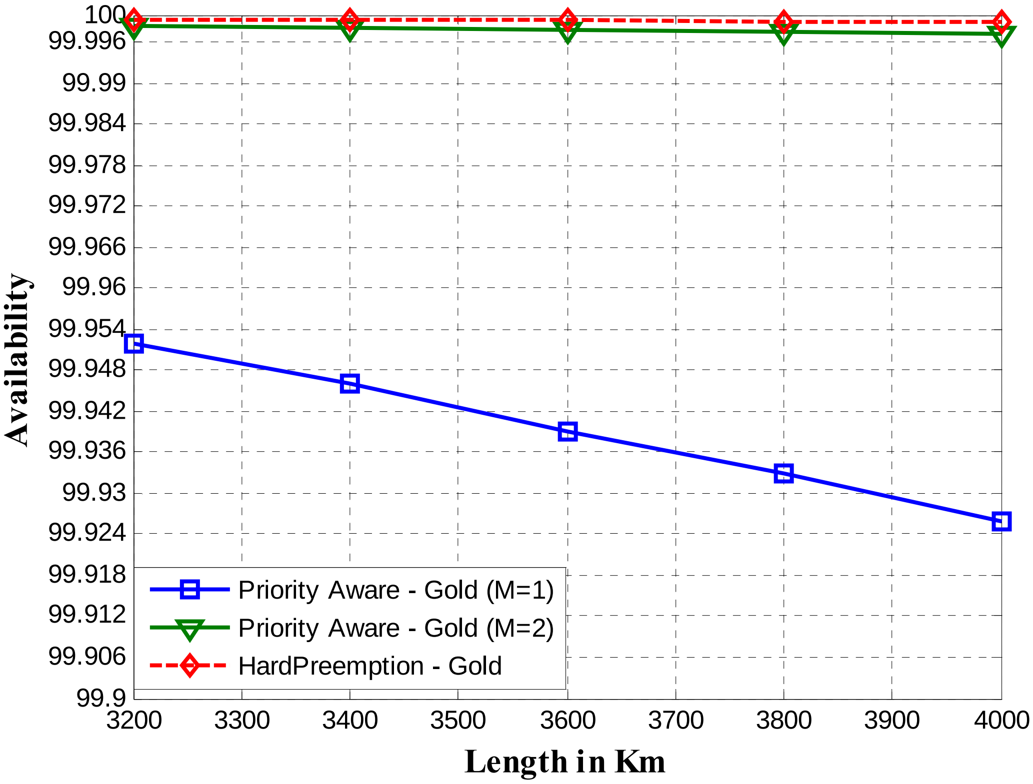


Figure 3. 1 Gold connections' availability due to Hard Preemption and priority aware protection schemes

We observe in Figure 3.1, that introducing Hard preemption improved the availability of Gold connection by approximately 0.082% while adding another backup improved the availability by 0.073%. Thus, we can deduce that applying hard preemption technique is enough to save operators the cost of an additional backup path.

As shown in Figure 3.1, Hard Preemption improved the availability to exceed 99.999% over long distances varying between 3200 and 4000 Km. This high availability can provide stability for Gold connections in cases where cut rate or mean time to repair increase dramatically.

In hard Preemption scheme, primary paths holding silver connections are considered as additional backup paths for the failing Gold connections. The process of preempting a silver connection on its primary path is “hard preemption”. This technique has resulted in a remarkable increase in the availability of Gold connection, but on the other hand penalized the silver connections. We will study the availability of silver connections using the same example analyzed for Gold connections.

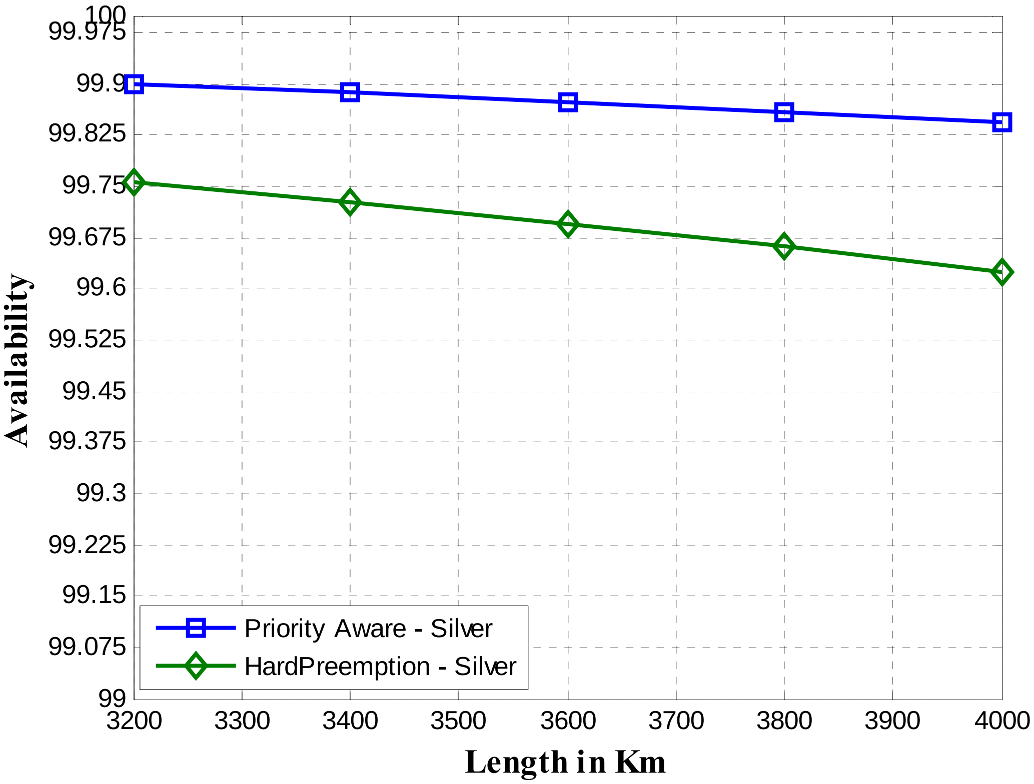


Figure 3. 2 Silver connections’ availability due to Hard Preemption with quota M1=2 and priority aware protection schemes

Figure 3.2, depicts that the availability of silver connections is penalized and the loss in availability is approximately 0.136%. This loss in the availability can be clearly explained since the system studied above has only 1 backup and thus the probability of having hard preemption is high. This loss in availability is expected to decrease when considering huge systems with multiple backups. Another factor contributing to the high penalty is the distance which ranges between 3200 and 4000Km. On the other hand, considering distances in the range of 800Km can give minor loss in availability approximately 0.03%.

3.3.2 Gold Stability on High cut rates

Cut rates vary according to the causes of cable cuts and the average cut rate can differ notably depending on the geographic location where the fiber network is located. We will study the effect of cut rate on the availability of Gold connections benefiting from the Hard preemption technique. We will consider an extreme case scenario where the number of Gold connections (8) is 2.6 times the number of silver connections (3). We will also consider the mean time to repair to be 20 hrs on a distance of 4000Km.

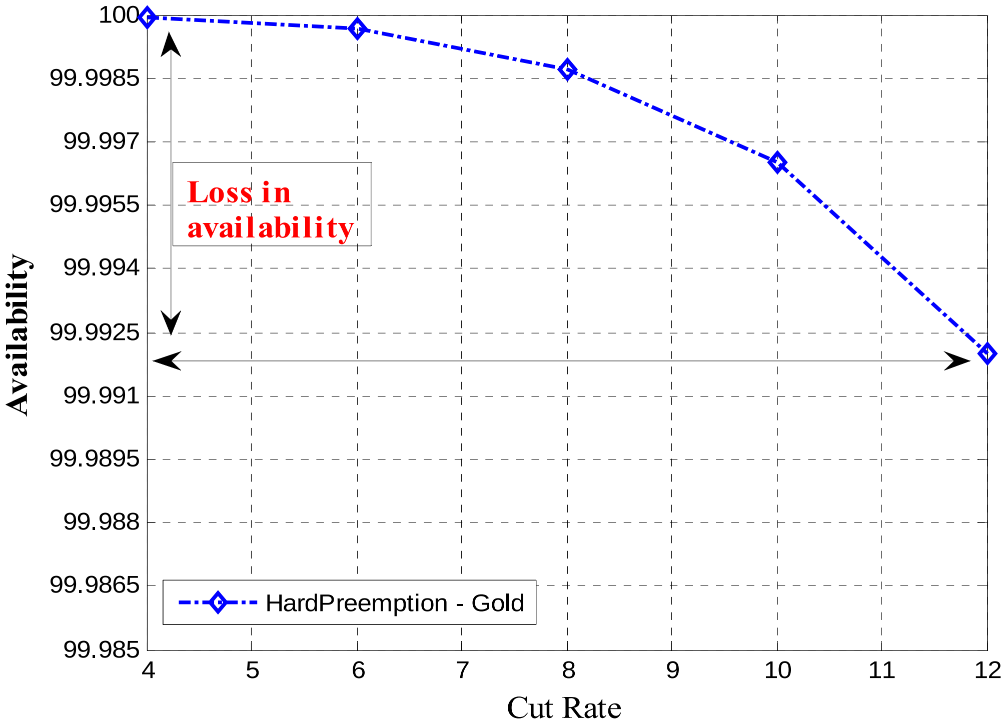


Figure 3. 3 Gold stability on high cut rates

As shown in figure 3.3, even on high Mean time to repair (20hrs) and long distances (4,000Km) the availability of the gold connections has preserved availability close to 100% when considering low cut rates. As cut rates increased, we started having a drop in the availability. We were able to retain availability of 99.999% for cut rates below 10, while the availability reached 99.992% with a cut rate of 12. Indeed our hard preemption technique enables us to satisfy SLA requirements for Gold connections, while those requirements are impossible to be satisfied using the priority-aware and classical shared protection schemes.

3.3.3 Effect of quota variation on availability

Adding quota on the number of preemptions allowed, minimizes the loss in availability for silver connections and limits the number of silver connections being hard preempted by failing Gold connections. In an attempt to evaluate the effect of quota, we will study the variation of quota and its effect on the availability for both gold and silver connections. We consider the example having 8 gold connections, 4 silver connections and 1 backup path, while we set the MTTR and cut rate to be 12hrs and 4.39cuts /yr/1000miles respectively. We will base the study on equation 3.11 and fix the cable length to 3,000Km.

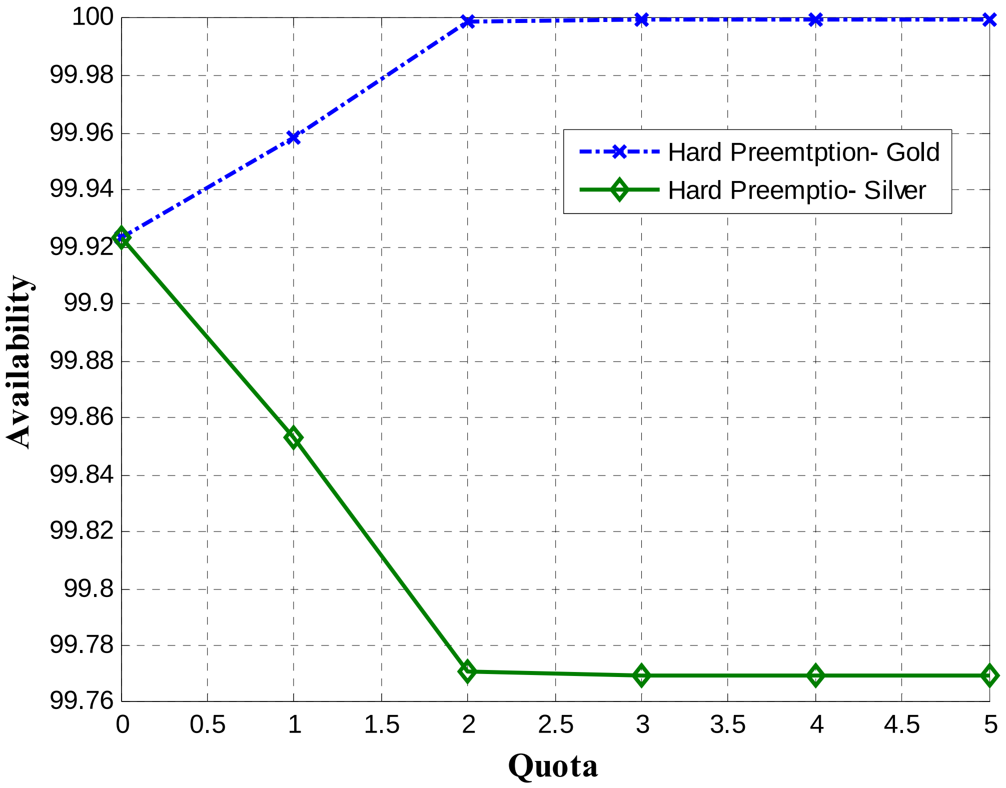


Figure 3. 4 Gold stability on high cut rates

We observe from figure 3.4, that when quota is 0, then no preemption is permitted and both silver and gold connections are treated similarly which results in equal availability of 99.924% (classical shared protection). When quota increases to 1, we started having class differentiation in restoring failed connections. Furthermore, since; as mentioned in the example, we consider 1 backup path then when a Gold connection fails, it either occupies the available backup path or hard preempts another silver connection if the backup path was unavailable. This procedure will drop the silver connection availability and increases that of the Gold. As quota increases, the availability of both classes of connections approaches steady state.

Using the above analysis procedure, operators can always select an optimal quota for hard preemption that satisfies the requirements agreed on with their clients in the SLA.

3.4 Conclusion

The introduction of hard preemption scheme has provided major improvements on the priority aware scheme proposed in chapter 2. Providing the High class connections with the capability to utilize primary path of the lower class connections as additional backups, has improved the availability of higher class connections remarkably. Based on the analytical study, high levels of availability for high class connections were achieved even with high cut rates and long distances. This new approach proved to be cost effective, since less backup paths had to be deployed in the system. As well as it proved to give satisfactory quality of service for the clients.

The major drawback has been the drop in availability of the low class connections. A slight improvement in availability was achieved by introducing quota on the number of preemptions. Therefore, another improvement must be added to the current scheme in order to attain an approach that provides acceptable quality of service for the different priority classes.

Chapter 4

Hybrid Preemption Protection Scheme

In the prior proposed schemes, we were able to improve the availability of high class connections and ensure high levels of availability in a cost effective manner. Achieving that firm availability for high class had its drawbacks on the availability of lower class connections which paid off for the introduced improvements.

4.1 Proposal

In this chapter, we introduce an additional enhancement to the protection schemes under study. Our newly proposed scheme is the Hybrid Preemption Protection scheme, which is an improvement on the hard Preemption scheme introduced in Chapter 3. In Hybrid protection we consider the "Mutation probability" parameter that defines whether a failing High class connection should be considered as a high class connection or it should be downgraded to a low class connection. The main purpose behind this parameter is to minimize the probability of having low class connections penalized after failure of high class connections.

For simplicity we will consider two classes of service; Gold and Silver. When a primary path holding connection t belonging to Gold class fails, the connection will be treated as a Gold connection with probability p'. Furthermore, when a primary path holding connection t belonging to silver class fails, the connection will be treated as a silver connection with probability q' = 1-p' . Thereafter, the mutated connection will follow the hard preemption scheme discussed in section 3.1.

4.2 Mathematical Model

In this section, we derive the analytical expression for the availability of connections using the hybrid preemption technique. Since the hybrid preemption is an improvement for the hard preemption scheme, we will base our derivations on section 3.2 and introduce the new parameter. We will develop the complete analytical expression for M:N Hybrid preemption scheme for two classes of service: gold and silver.

We consider the same basic assumptions mentioned in section 3.2.1.

Consider a system having M backup paths and N primary paths. For simplicity we consider 2 classes of service gold and silver.

We also consider that all paths including backup have identical λ and μ.

The availability of path is denoted by p and unavailability is q where:

$p= \frac{\mu}{\lambda+\mu}$ and $q = 1- p$

Let N_1 and N_2 be the number of Gold & Silver connections respectively.

$N_1 + N_2 = N$ which is the total number of primary connections

Let M be the number of Backup paths

Let M1 be the quota on preemptions allowed.

Let p' be the mutation probability, and $q' = 1- p'$. **(4.1)**

Define the state descriptors as follows:

n_1= # of failed gold connections

n_2= # of failed silver connections

n' = # of failed gold connections treated as gold class connections during failure.

m= # of operational backups

We set the state X to have probability P(X) where

$P(X) = p(n_1)\, p(n_2)\, p(m)\, p(n'/n_1)$ **(4.2)**

Then as proven in the section 2.2.2.3,

$P(n_1) = \binom{N1}{n1} q^{n1}\, p^{N1-n1}$

$P(n_2) = \binom{N2}{n2} q^{n2}\ p^{N2-n2}$

Whereas the probability of m *operating* backups can be defined by:

$P(m) = \binom{N2}{n2} p^{m}\ q^{M-m}$

The probability of having n' gold connections out of the n_1 failed ones:

$$P(n'/n_1) = \binom{n_1}{n'} p'^{n'}\ q'^{(n_1-n')} \quad \textbf{(4.3)}$$

Calculating Unavailability for Gold connections

A connection t belonging to Gold class is unavailable in a system in state X , if both conditions are satisfied :

1) A = Primary path, holding connection t, is down

2) B = t is not restored by neither the backup path nor a primary path of silver connections.

- ⇨ Unavailability of Gold $U_{gold} = \sum_{x=(n1,n2,m)} P(A, B, X)$
- ⇨ $U_{gold} = P\ \{B/A, X\}.\ P\{A/X\}\ .P\ \{X\}$

$\mathbf{P(X) = P(n_1)\ P(n_2)\ P(m)\ \ P(n'/n_1)}$

The probability of having primary path holding connection t down, given state X is:

$\mathbf{P\ (A/X) = \frac{n1}{N1}}$

The probability of having condition B applied given condition A and state X is always equal to zero except in the following conditions:

Probability that P(B/A,X) ≠ 0 can be similarly derived as in chapter 4, except the following substitutions:

1- **$n' = n_1$, we substitute n_1 by n' since only n' out of the n_1 failed Gold connections will be treated as a Gold class connection, while the remaining (n_1- n') will be demoted to silver class connections.**
2- **$n_2= n_2 + (n'-n_1)$, since the demoted failed gold connections will be added to the number of failed silver connections.**

Calculating Unavailability for Silver connections

A connection t belonging to Silver class is unavailable in a system in state X, if both conditions are satisfied:

1) A = Primary path ,holding connection t , is down

2) B = t is not restored by the backup path

3) C = Primary path ,holding connection t , is up
4) D = t is hard preempted on its primary path.

⇨ Unavailability of Silver U_{silver}

$$U_{silver}= \sum_x P(A,B, X) + \sum_x P(C,D, X)$$
$$U_{silver} = \sum_x P(B/A,X) P (A/X) P(X) + \sum_x P(D/C,X) P (C/X) P(X)$$

$P(X) = P(n_1) P(n_2) P(m) P(n'/n_1)$

The probability of having primary path holding connection t down, given state X is:

$P (A/X) = \frac{n2}{N2}$

While the probability of having primary path holding connection t up, given state X is simply 1- P (A/X), therefore:

P (C/X) = $1 - \frac{n2}{N2}$

Probability that P(B/A,X) & P(D/C,X) $\neq 0$ can be similarly derived as in chapter 3, except the following substitutions:

1- **$n' = n_1$, we substitute n_1 by n' since only n' out of the n_1 failed Gold connections will be treated as a Gold class connection, while the remaining (n_1- n') will be demoted to silver class connections.**

2- **$n_2 = n_2 + (n' - n_1)$, since the demoted failed gold connections will be added to the number of failed silver connections.**

4.3 Analysis

In this section we will evaluate the benefits of the Hybrid Preemption scheme. We compare this new improved scheme with the Hard Preemption Protection scheme in order to pin point the improvements introduced. We will study the availability achieved by hybrid Preemption scheme over a varying distance. Moreover, we will focus our analysis on the effect of mutation probability, in an attempt to find an optimal value that satisfies the quality of services for both gold and silver clients.

4.3.1 Comparison with Hard preemption scheme

The major benefit behind introducing Hybrid preemption is improving the availability of silver connections while retaining high level of availability for Gold connections. To view the enhancement introduced, we will compare the hybrid preemption protection scheme with the hard Preemption protection scheme. In the following example we will consider both Gold and Silver classes in both schemes to have a comprehensible idea on the variations occurring in availability. We consider 6 primary connections (4 gold & 2 silver) and 1 backup while we set the cut rate and MTTR to be 5 cuts/yr/1000miles and 15 hrs respectively.

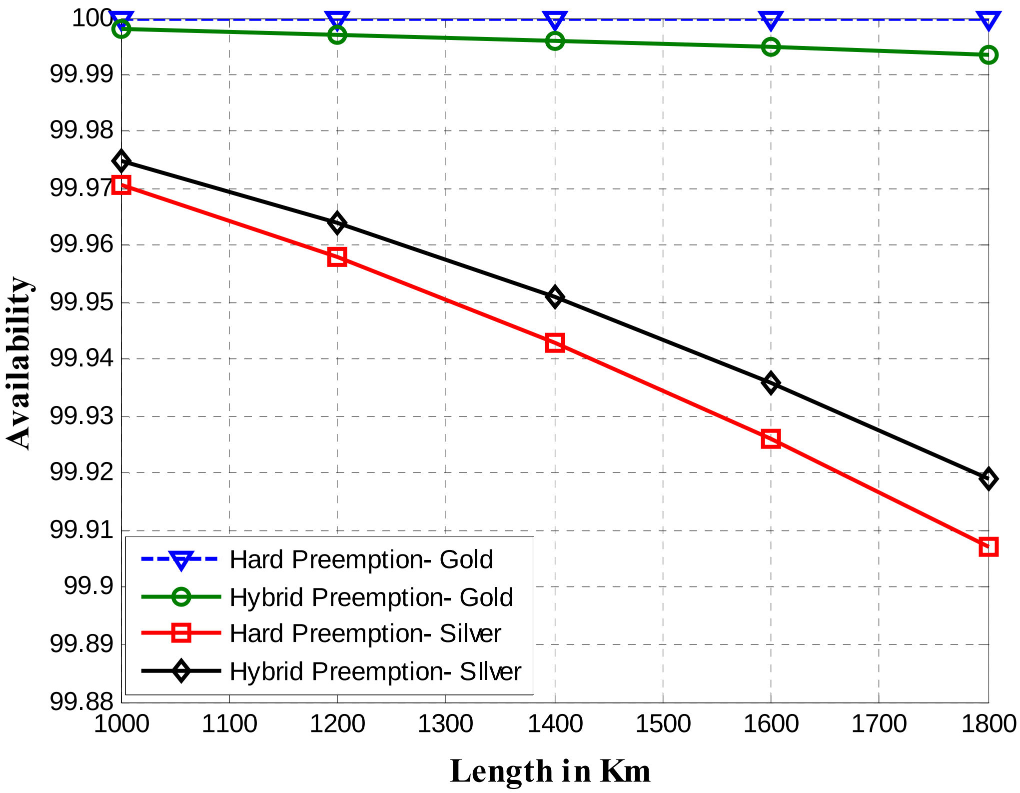


Figure 4. 1 Hybrid preemption Scheme with P'=0.85 & M1=2

Figure 4.1 shows that the availability of Silver connections is improved by approximately 0.05%. The effect of introducing mutation probability equal to 0.85 has treated 15% of the failed Gold connection as Silver, which resulted in minimizing the penalty paid by silver connection due to hard preemption scheme. On the other hand, the Gold connection availability has decreased due to the introduction of mutation probability, without going beyond 99.992%. In summary, introducing the mutation quota made it possible for us to regulate the availability of both classes of services to achieve the required levels.

4.3.2 Effect of Mutation Probability on availability

The introduction of Mutation Probability is the key that operators and network designers need in order to attain certain availability levels in their networks. In this section, we will study the effect of varying the mutation probability on both Gold and silver classes. We will set the range of mutation probability to be between 0.6 and 1, while we fix the cable length to 2000Km. We also consider 6 primary paths 4 of which are occupied by gold connections, while we consider 1 backup path. We keep same assumptions as previous example for MTTR and cut rate to be 12hrs and 4.39 cuts/yr/1000 miles respectively.

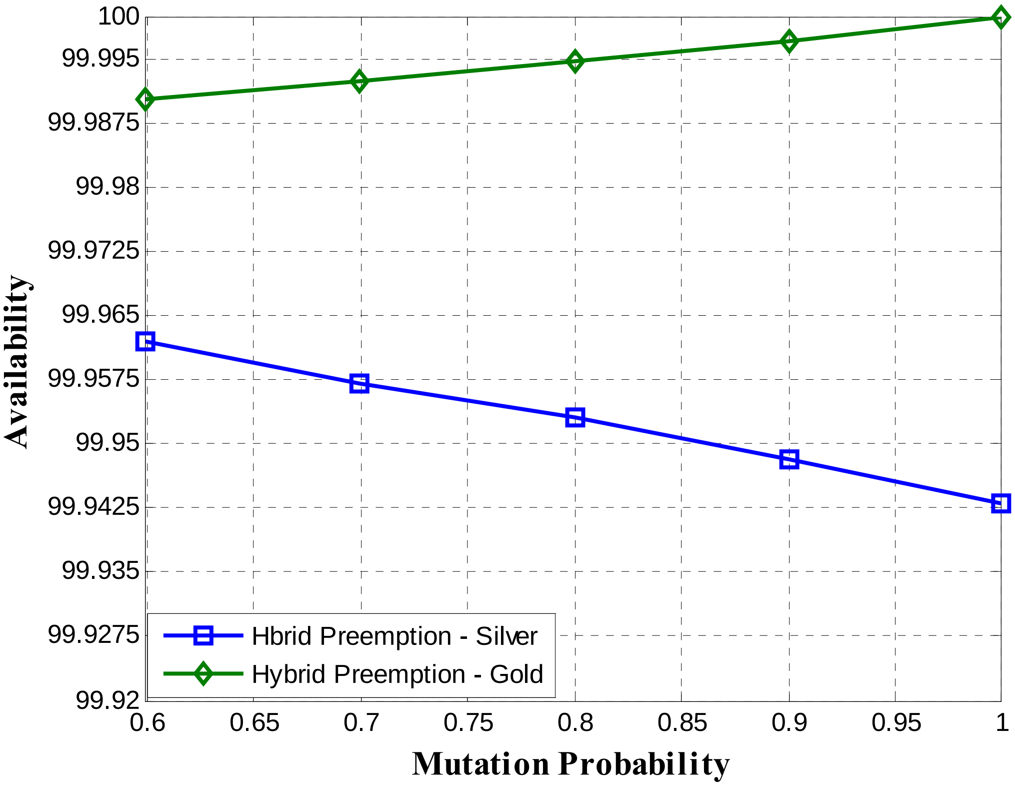


Figure 4. 2 Effect of Mutation probability with Quota M1=2

As shown in figure 4.2, increasing the mutation probability has increased the divergence between the availability of Gold and Silver class connections. When the mutation probability approaches 0, all the Gold connections are treated as silver connections and therefore the system performs as described in the classical shared protection scheme. On the other hand, when the mutation probability approaches 1, the system performs as described in the hard preemption scheme. Choosing the right mutation probability can provide a reliable network without penalizing severely the low class connection while achieving high levels of availability for the high class connections.

4.4 Conclusion

The introduction of Hybrid protection scheme has provided major improvement on the quota based Hard preemption scheme proposed in chapter 4. The introduction of mutation probability has resolved the drawbacks of the hard preemption scheme by improving the availability of the low class connections. Based on the analytical study, setting the optimal mutation probability is the key to achieve the requirements of both service classes. In short, the mutation probability parameters give operators and network designers the flexibility to vary the availabilities of both high and low class connections to suit the requirements of the SLA.

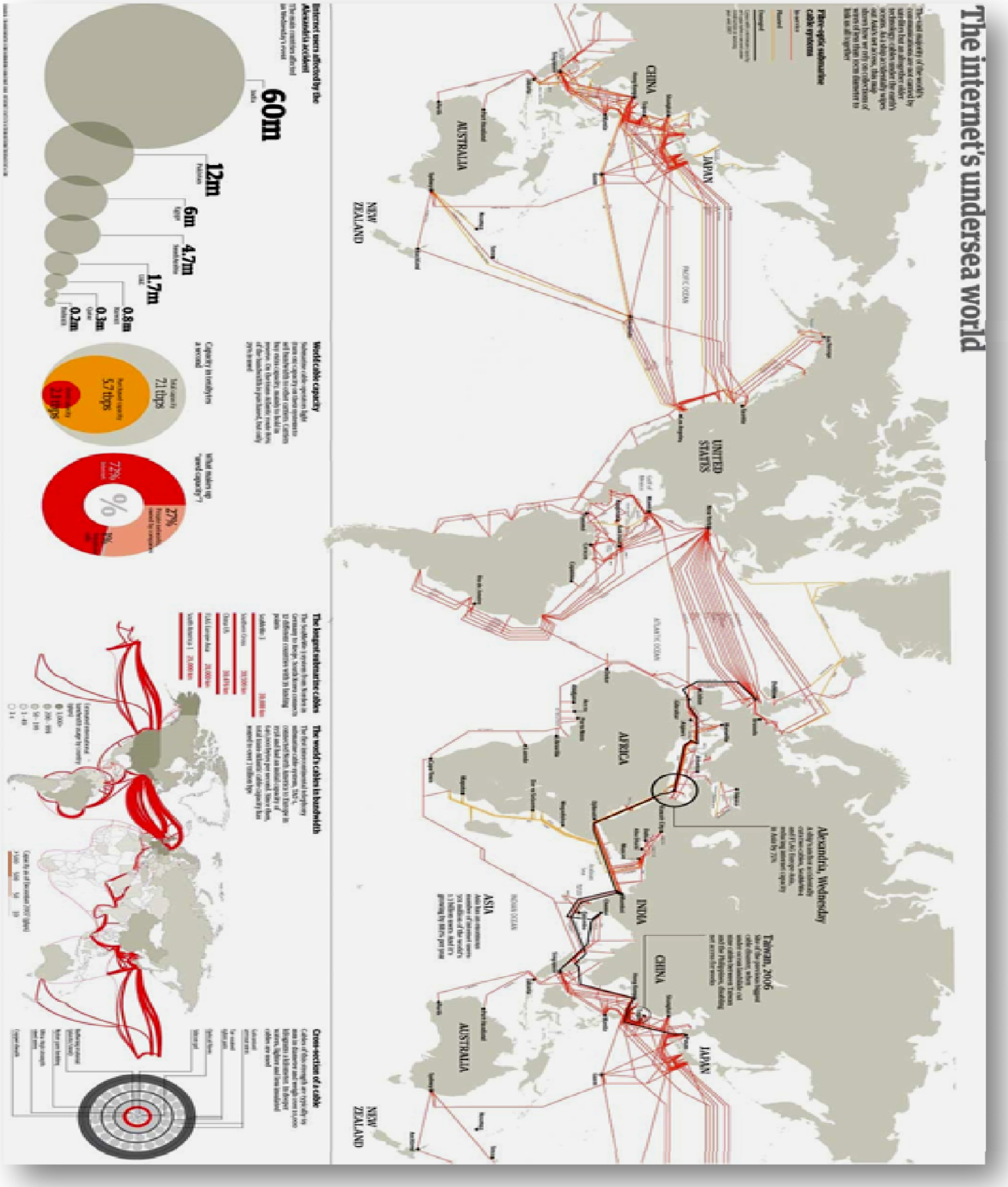
Chapter 5

Conclusion

The frequent occurrence of fiber cuts and the tremendous loss that a cut may cause are motivating the design of survivable optical networks. Parallel to this, there is increasingly a strong need for quality of service differentiation due to the introduction of new services, each presenting different quality of service requirements. Hence, a great deal of effort is being put into the design of quality of service aware fault resilient strategies.

Contributing to the design of such strategies, this work proposed three novel availability-aware protection schemes that provide predictable levels of availability for the different client classes. The first proposed scheme introduced relative priority among the failing primary connections contending for the use of the shared backup resources. The second protection scheme uses a hard preemption strategy that equips gold connections with the capability of hardly preempting silver connections and thus improves the availability of gold connections. In an attempt to prevent gold connections from severely penalizing silver connections, we opted to place an upper limit on the number of preempting gold connections. The enhanced hard preemption strategy to which we referred as the quota-based hard preemption strategy allowed us to protect the silver connection in the face of the greediness of gold connections. Our results in this respect show that the improvement the silver connections witness as a result of the introduction of quotas is not sufficiently high. This is especially true since we were still unable to accommodate the requirements of silver connections with the quota-based hard preemption strategy. This led us to the development of a third availability-aware protection scheme which we referred to as the hybrid protection scheme. For this scheme, we envisaged having a failing gold connection act as a silver connection with a predefined probability called the mutation probability. It was made clear through our numerical results that the third protection scheme outperforms the other schemes since it ensures a reasonable compromise between resource usage and connections' availability satisfaction.

Appendix A: Under Sea -Fiber Optic Map



References

[MAN 06]
MANNIE E., PAPADIMITRIOU D., « Recovery (protection and restoration) Terminology for GMPLS », RFC 4427, Mars 2006.

[ZAN 04]
ZHANG J., MUKHERJEE B., "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges", IEEE Network, P. 41-48, Marc/April 2004.

[PAP 06]
PAPADIMITRIOU D., MANNIE E., «Analysis of GMPLS-based Recovery Mechanisms (including Protection and Restoration) », RFC 4428, March 2006.

[CRA 92]
CRAWFORD D., "Fiber Optic Cable Dig-ups – causes and cures", Network Reliability and Interoperability Council website, 1992.

[GRO 02]
GROVER W., "Mesh-Based Survivable Networks", *Prentice Hall*, 2004.

[RAM 99]
S.Ramamurthy and B.Mukherjee. SurvivableWDMMesh Networks, Part I – Protection. In *Proceedings of INFOCOM'99*, pages 744–751, March 1999.

[KAM 80]
F. Kamoun and L. Kleinrock, "Analysis of shared finite storage in a computer network node environment under general traffic conditions," *IEEE Transactions on Communications*, vol. 28, no. 7, pp. 992–1003, July 1980.

[CHO 95]
G. L. Choudhury, K. K. Leung, and W. Whitt, "Efficiently providing multiple grades of service with protection against overloads in shared resources," *AT&T Technical Journal*, vol. 74, pp. 50–63, Aug. 1995.

[FAW 04]
W.Fawaz and al. SLA and Provisioning in Optical Networks. In *IEEE Communications Magazine*, pages 36–43, January 2004.

[SZY 07]
A.Szymanski, A.Lason, J.Rzasa, and A.Jajszczyk. Grade-of-Service-Based Routing in Optical Networks. In *IEEE Communications Magazine*, pages 82–87 vol.45, February 2007.

[CHE 01]
Y.Chen, M.Hamdi, and D.H.K.Tsang. Proportional QoS over WDM Networks: Blocking Probability. In *6th IEEE Symp. Comp. and Commun.*, pages 210–15, July 2001.

[TAC 04]
T.Tachibana and S.Kasahara. QoS-Guaranteed Wavelength Allocation for WDM Networks with Limited-Range Wavelength Conversion. In *IEEE Trans. Commun.*, pages 1439–50 vol.6, June 2004.

[MIY 04]
Y.Miyao and H.Saito. Optimal Design and Evaluation of Survivable WDM Transport Networks. In *IEEE Journal on Selected Areas in Communications*, pages 1190–1198, September 2004.