Scalable Shared Protection Approach for Mesh WDM-routed Networks

Florence Touvet, David Harle
University of Strathclyde, Glasgow
florrie@comms.eee.strath.ac.uk, d.harle@eee.strath.ac.uk

Abstract

The paper proposes an approach for calculating the protection pool size on each link in a mesh WDM-routed network. The protection pool evaluation is part of a shared protection scheme applied to a failure dependent scenario and based on aggregated information dissemination. Two models based on a probabilistic approach are proposed to provide a scheme that is scalable as the number of optical cross-connects (OXC), fibres and wavelength multiplexing in a core network increases. Precisely, two models based on a binomial and a beta-binomial distribution are presented. The evaluation of the models by simulation shows that both models are attractive propositions to offer protected λ-services that do not require an absolute protection guarantee offered by (1:1) schemes or shared protection schemes requiring full network state information, or using partial information but with less efficient use of the fibre utilisation.

Keywords: mesh WDM networks, partial information, protection pool size, shared protection

1 Introduction

The consideration of protection in the optical layer is of importance since monitoring statistics show that failures in backbone optical networks are not uncommon [1, 2]. Survivability is introduced by adding protection mechanisms which incur the need for additional capacity, named *protection pool*. The protection channels are either allocated or reserved at the acceptance of a protected lightpath. The allocation of protection implies that a protection channel is reserved for one protection lightpath only. Protection channel reservation falls into one of two modes: failure independent and failure dependent. In a failure independent mode, specific protection channels are assigned to specific lightpaths when their protection path is computed. A look-up table, with an entry for each protection channel and failure case, enables fast cross-connection of the drop ports along the protection paths. In the failure dependent case, the reserved protection channels are assigned, on a first-requested first-served basis, to the protection lightpaths only after a failure affecting that lightpath has occurred. In this latter mode, the protection channels share a common protection pool. A higher sharing corresponds to a more efficient use of the channels and thus enables the acceptance of more connections. In the case of shared protection, the protection channels can *only be reserved* and the channel allocation can only be made after the detection of the failure, depending on which connections are to be recovered. Upon the detection of a failure, intermediate OXCs between the end nodes of each failed connection, along the protection path, receive restoration messages. The protection path has been pre-calculated and is stored in the end nodes for each connection. On reception of these messages, the cross-connection to a protection wavelength between drop ports is performed. The protection channels are dynamically selected by the cross-connects.

Shared protection schemes that maximise protection-channel sharing require the knowledge of all the paths used by the lightpaths established in the network. These schemes use *full* network state information. Moreover, the schemes guarantee 100% robustness for pre-defined failure sets, e.g. single link failures.

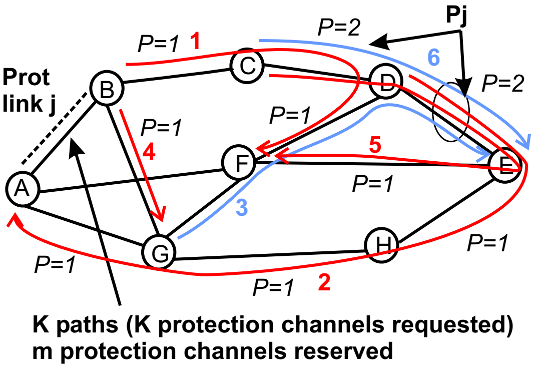
Pj
P=2
P=1 1
C
6
Prot
link j
B
D
P=2
P=1
P=1
4
F
5
A
E
P=1
3
G
H
P=1
P=1
P=1 2
K paths (K protection channels requested)
m protection channels reserved

Figure 1: Exemplar Network with Established Lightpaths

Figure 1 shows an example of a link, $\{A, B\}$, that is shared by the protection lightpaths associated with the connections 1, 2, 4 and 5, and provided that full conversion is available. The lightpaths shown are the active lightpaths of the connections. In each protection link (here link AB is the protection link of interest), K protection lightpaths share m protection wavelengths, thus a sharing ratio of $\frac{K}{m}$ is achieved. There are at most m working lightpaths that can fail simultaneously, m protection wavelengths are reserved. In other terms, there are at most m working lightpaths that share a common link. Lightpaths 3 and 6 use the link $\{D, E\}$ but their associated protection lightpaths do not use the link $\{A, B\}$ (denoted j). From the diagram, $K = 4$, as 4 connections have a protection lightpath that uses link j. The protection pool used by the deterministic shared protection scheme is devised in such a way that the number of protection channels reserved on the links along the protection lightpaths is equal to $m = P_j = \max\{P\}$, where P is the number of active lightpaths using the same link. In the example shown in Figure 1, P_j is obtained on link $\{D, E\}$ and on link $\{C, D\}$ ($P_j = 2$), and 2 channels are therefore reserved in link j. Indeed, on link $\{C, D\}$, 2 rather than 3 channels are reserved because the protection lightpaths for connection 6 does not use link j. Moreover, on link $\{D, E\}$, 2 rather than 4 channels are reserved because the protection lightpaths for connections 3 and 6 do not use link j. The obtained sharing ratio for the example is therefore $\frac{4}{2}$. The evaluation of a value for P_j is possible because the OXCs have complete knowledge of all the paths.

2 Proposal of a Probabilistic Approach

2.1 Motivation

Three main factors influence the use of the approach:

- Failures do not occur often. Thus, the protection pool size can be estimated based on failure probabilities in order to minimise the number of protection channels that must be reserved.
- The calculation of the protection pool is not tied to a specific failure set, e.g. single link failures. The pool size can be sufficient to reroute failed lightpaths after single or multiple failures. It should be noted, however, that the failure of both active and protection lightpaths is not considered.
- Only *aggregated* information is necessary to evaluate the number of required protection channels [3]. Per-lightpath information dissemination is avoided, which renders the decision-making relatively simple and the scheme scalable.

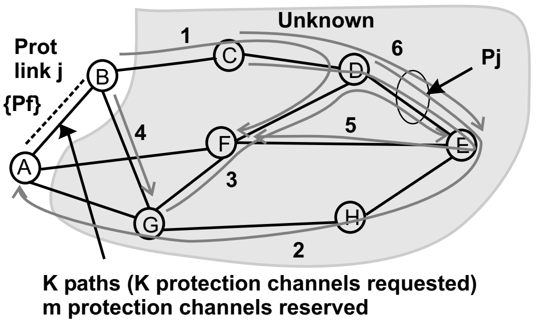
Unknown
1
6
Pj
Prot
link j
{Pf}
B
C
D
4
5
F
E
A
3
G
H
2
K paths (K protection channels requested)
m protection channels reserved

Figure 2: Exemplar Network with Established Lightpaths - Hidden Information Shadowed

Figure 2 illustrates that by using the probabilistic scheme, some information about the network state is hidden, as only aggregated information is distributed to every OXC, i.e. the fibre utilisation: number of "active" and "protection" channels used on each link. Unlike the deterministic case, the value of P_j is unknown and the size of the protection pool on link j is evaluated by using a unique parameter, denoted P_f. P_f represents the mean lightpath failure (i.e. the mean failure probability of the connections (active lightpaths) whose protection lightpaths share a common protection link) or, alternatively, P_f can be thought of as the mean probability that a protection channel is required.

2.2 Protection Pool Size Calculation

One of the task of the protection scheme, with the choice of the protection paths, is to reserve sufficient protection channels along all the links. A technique is to employ a probabilistic approach in order to determine how many protection channels are required, i.e determine the protection pool size. The proposed scheme uses the technique previously proposed in [3] and suggests a modification in order to make a better calculation of the required protection pool of channels.

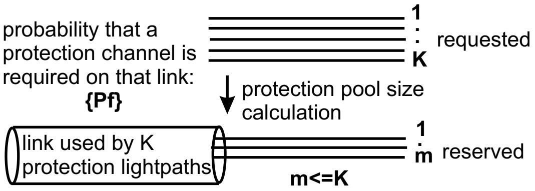

Figure 3: Requested and Required (Reserved) Protection Channels in a Link

Figure 3 illustrates the sharing of the protection channels in a link. Indeed, provided that K connections requiring protection are established and whose protection lightpaths share a common link, K protection channels are requested on that link. Using the value of P_f allocated for that link, which represents the probability that a protection channel is required, the number of protection channels, m, that are actually reserved is evaluated. The sharing ratio obtained is $\frac{K}{m}$. A value of P_f set to 1 ensures that $m = K$ and can be used for obtaining a protection scheme equivalent to a (1:1) protection. Based on the binomial distribution, the probability that at any instant of time m protection channels are required is equal to $C_m^K P_f^m (1 - P_f)^{K-m}$. The protection pool size on a specific link can be evaluated using that simple binomial distribution and the expression used is the following:

$$\begin{array}{lll}
\text{If } P_f^K > p^* & , & \text{m=K} \\
\text{If } \sum_{k=K-1}^{K} (C_k^K P_f^k (1 - P_f)^{K-k}) > p^* & , & \text{m=K-1} \\
\text{If } \sum_{k=m+1}^{K} (C_k^K P_f^k (1 - P_f)^{K-k}) \leq p^* & , & 1 < m < K - 1 \\
\text{If K=1} & , & \text{m=1}
\end{array}$$

Expression 1

Expression 1 states that, given that a given link protects K connections, m is determined so that more than any m protection channels are required simultaneously with a probability less or equal to p^*. If m is smaller than $K-1$, starting with $m = K-2$, the value of m is decreased until the sum becomes greater than p^*.

Figure 4 shows the number of reserved wavelengths per link, m, as a function of shared backup connections per link, K, for different values of P_f. Using Expression 1, for a protection link, the values of m have been calculated for different numbers of established lightpaths, K.

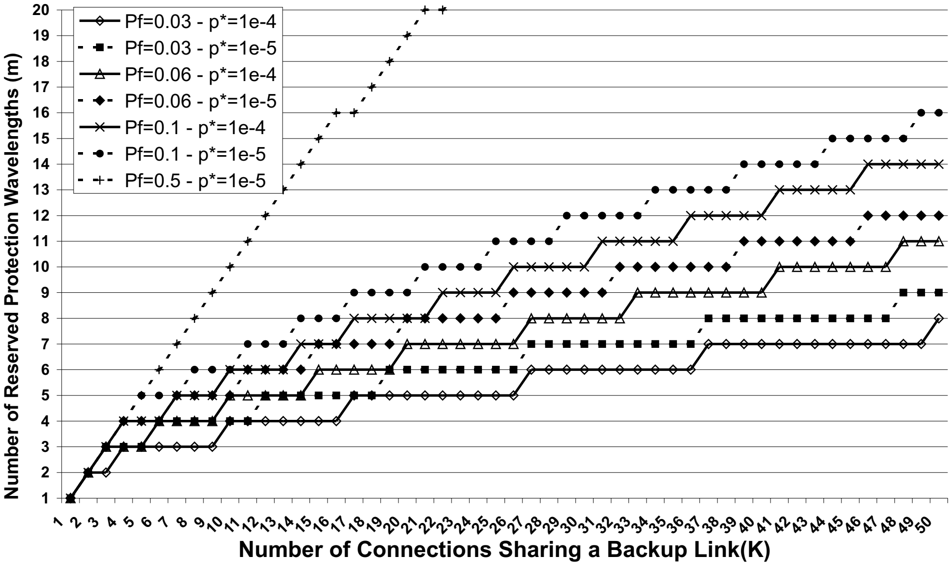

Figure 4: Minimum Number of Reserved Shared Protection Wavelengths

From Expression 1, it can be noted that the assumption made is that failures of the lightpaths are *independent*. This assumption is valid in the case of highly uncorrelated active lightpaths. The protection scheme based on the use of Expression has been evaluated [3] and offers the potential for the protection of a large number of connections.

3 Improvement of the Protection Guarantee

The probabilistic scheme based upon a binomial distribution makes the assumption that the lightpaths failures are independent. This assumption suggests that the value of P_f would remain constant regardless of the active paths of the connections whose protection lightpaths share a common link. This assumption under-estimates the probability of simultaneous failures (as shown in the example of P_{fail} in section 3.1), which corresponds to a smaller protection pool than needed and therefore deteriorated robustness. Although the lightpaths are routed independently, their failure behaviour is correlated, as they are subject to common inputs, i.e. the links used by the paths. In the following section, an alternative distribution to the binomial is proposed in order to take into account of the correlated failures of the lightpaths and therefore obtain more adequate protection pool sizes on each link.

3.1 Failure Behaviour Correlation

A beta-binomial distribution is proposed in order to take into account the failure behaviour correlation of the lightpaths when calculating the protection pool required by a link. The reasons for the choice of this distribution are that only one additional parameter, a correlation level, is required; if this parameter is set to 0 then the distribution reduces to a binomial distribution.

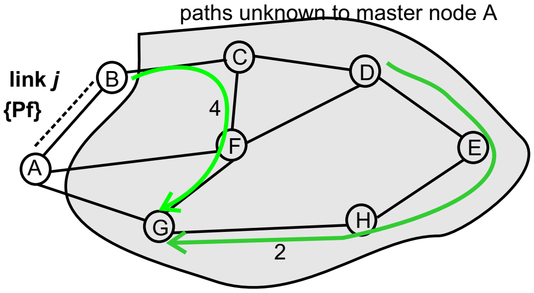

Figure 5: Example of a protection link whose active lightpaths are *link-disjoint*

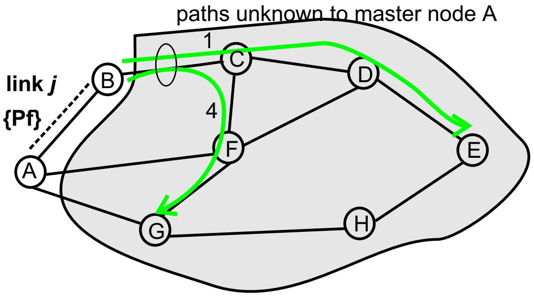

Figure 6: Example of a protection link whose active lightpaths are *overlapping*

Figures 5 and 6 are used to explain the influence of the input, i.e. used link by the active lightpaths, on the variation of the mean probability that a protection channel is required. Indeed, in Figure 5, assuming that only the protection paths of connections 2 and 4 use a common link ($\{A, B\}$), P_f can be considered as constant as the active lightpaths are link disjoint. The value of P_f derived directly from the mean value of the probability of failure of connection 2 and 4. However, in Figure 6, the active lightpaths of the connections 1 and 4 are overlapping on link $\{B, C\}$. Depending on the paths used, the mean probability of lightpath failure changes. Due to the overlapping, the failures of the lightpaths 1 and 4 are correlated. In Figure 5, the probability of two simultaneous failures is equal to $P_{fail} = P_f^2$. This is not true for Figure 6, where P_{fail} would be expected to be higher than P_f^2 as the chance of requiring 2 protection channels is higher. Using the beta-binomial distribution "factors in" the risk of overlapping paths, without the requirement of knowing the specific paths and overlaps.

3.2 Protection Pool Size Calculation

The beta-binomial distribution has been previously used to model correlated events such as the failures in multiversion software [4]. The definition of the beta-binomial depends on the use of a probability mass function (or intensity function) $f_p(p)$. Considering the failures of paths due to link failures, $f_p(p)$ indicates that, with a probability $f_p(p)$, a fraction p of all possible paths would fail. For N paths, the beta-binomial distribution is defined as follows:

$$b_N(i) = \int_0^1 C_i^N p^i (1-p)^{N-i} f_p(p) dp \tag{1}$$

$b_N(i)$ represents the probability that i paths fail upon a link failure. If the path failures are assumed uncorrelated, $f_p(p)$ is reduced to a constant and the distribution $b_N(i)$ becomes the binomial $C_i^N p^i (1-p)^{N-i}$, as used in Expression 1. The details for obtaining the final beta-binomial distribution as a function of only two parameters are given in [4]. The final beta-binomial distribution is given by expression 2:

$$b_N(i) = C_i^N \frac{(p+(i-1)\alpha)(p+(i-2)\alpha)\cdots p(\chi+(N-i-1)\alpha)(\chi+(N-i-2)\alpha)\cdots\chi}{(1+(N-1)\alpha)(1+(N-2)\alpha)\cdots 1} \tag{2}$$

p is the mean path failure probability (equivalent to P_f) and α represents the correlation level. χ is the equal to $1 - p$. The correlation level is a measure of the variation of the mean probability of lightpath failure (or mean probability that a protection channel is required), which occurs due to the overlapping of the active lightpaths.

4 Performance Results

For the evaluation of the schemes by simulation, 10 networks composed of 20 nodes and 34 dual fibre links with connectivity no lower than 2 were randomly generated. The networks generated are close to the real networks ARPANet, UKNet and EON, regarding the number of nodes, links and the minimal and maximal nodal degrees. For each connection request, a lightpath is established between source and destination nodes using one wavelength in each link along the path; the same set of wavelengths are reserved for the reverse path. Connection requests follow a Poisson distribution while the mean holding time of the lightpath is normalised and negative exponentially distributed. The admission control is a lost-calls-cleared system. Moreover, a connection is admitted only if an active lightpath can be established and a protection lightpath reserved. In the simulations, fixed paths have been pre-computed using Bhandari's algorithm [5] for selecting the shortest pair of node disjoint paths. Although this path selection is not the most appropriate for shared protection schemes, as it does not take into account the backup sharing on each link [6], it is used for preliminary comparisons of the schemes. The wavelength allocation adopts a first fit policy; 32 wavelengths per link have been used and full wavelength conversion is possible. Finally, a fatal failure probability p^* of 10^{-6} was used. Different parameters of P_f and α were used for comparison: a value of 0.1 and 0.04 was set for P_f and α was either 0 (which corresponds to the binomial case), 0.01 or 0.03.

The evaluation of the robustness implies the simulation of link failures. Indeed, one interesting aspect of the probabilistic schemes is the adaptation of the values of P_f, α and p^* to provide an appropriate level of protection guarantee. Although the probabilistic schemes are not devised according to pre-defined failure sets, only single failures have been considered here assessing the robustness. Link failures are simulated periodically, depending on the network state changes, in order to capture as many possible lightpath configurations as possible. In the simulations, a single link is chosen at random and then broken. Thus, the probability that a particular link has failed equals $\frac{1}{\#\text{Links in the network}}$. In practice, the reliability of a link is a function of its length, but for simplicity all links are considered to be equal length. For "real" networks, the link lengths could be considered and the probability that a particular link fails could be taken as $\frac{\text{Link Length}}{\text{Total Mileage}}$.

The metrics of interest for the evaluation of the protection scheme are the blocking probability, the sharing ratio (the mean number of connections that share the same protection channel) and the mean protection grade.

The mean protection grade (or robustness) corresponds to the protection level offered to the connections. It was evaluated as the "worst" $\frac{\#\text{reserved channels}}{\#\text{required channels}}$ value. Upon a single link failure, the number of protection channels, m, was compared to the number of lightpaths that have failed, i.e. the number of required protection channels. The number of required channels correspond to the number of correlated paths, denoted P and used in section 1. To illustrate what the worst value represents, Figure 7 shows an example of a link failure affecting two lightpaths and the protection paths employed.

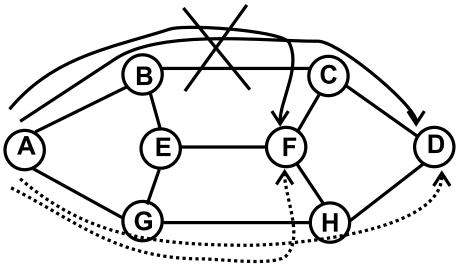

Figure 7: Example of link failure and employed protection lightpaths

From Figure 7, link $\{B, C\}$ is the broken link. Two active lightpaths are affected and the traffic is rerouted onto the protection lightpaths (dotted lines). The ratio $\frac{\#\text{reserved channels}}{\#\text{required channels}}$ is calculated in every link of the protection lightpaths, i.e. links $\{A, G\}$, $\{G, H\}$, $\{H, F\}$ and $\{H, D\}$. The smallest ratio obtained in one of the link is chosen as the robustness value for that link failure. The value plotted for each traffic load corresponds to the mean value obtained after a number of random link failures have been generated.

Figure 8 shows the probability of connection request rejection. A connection (one active lightpath and one protection lightpath set up) is rejected due to a lack of available channels on one or more link along the active or/and protection lightpath. Figure 9 shows the variation of the mean sharing ratio of the protection channels on each link. The sharing ratio corresponds to $\frac{K}{m}$, where only m protection channels are reserved for K protection channels that are requested by K established connections. Figure 10 represents the mean protection grade obtained on each link.

The plots of Figure 10 represent the mean of the worst values of $\frac{\#\text{reserved channels}}{\#\text{required channels}}$ obtained in each protection link after a link link failure. The results show that the robustness of the protection increases when the probability that a protection channel is required, P_f, increases. Without any consideration of the possible correlation of active lightpath failures (α=0), the offered robustness is equal to 0.998 when $P_f = 0.1$, compared to a protection level is equal to 0.987 when $P_f = 0.04$. Using low values of P_f reflect a low probability of lightpath failure and therefore a low probability of requiring a protection channel. Consequently, low values of P_f induce less robustness. Figure 9 shows the increase of sharing when P_f decreases. Better sharing leads to a greater number of accepted connections; a lower blocking probability is obtained for lower values of P_f. For a constant value of P_f, the robustness is improved when a correlation level is used along with P_f. The higher the value of level of correlation, the higher the robustness. The improvement of the robustness is more noticeable for lower values of P_f. Figure 8 shows that using $\{P_f = 0.1,\ \alpha = 0.01\}$ or $\{P_f = 0.04,\ \alpha = 0.03\}$ enables to obtain the same blocking probability. However, the former offers higher robustness. It seems that the probability that a protection channel is required has a bigger impact on the robustness than the level of correlation between the lightpaths failures. Another observation is that, as the network load increases, the slope for the robustness is smaller as the level of correlation increases. When a binomial distribution is used, the level of protection deteriorates more rapidly with increasing traffic loads. The benefits of using a beta-binomial distribution are more pronounced for high network loads than low loads; higher robustness, that does not decrease dramatically with a network load increase, is offered.

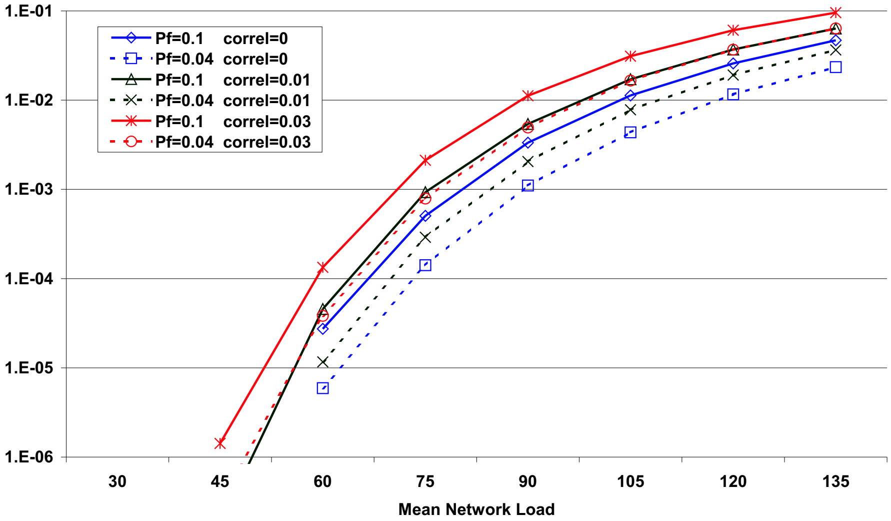

Figure 8: Blocking Probability (or Lightpath Request Rejection Probability)

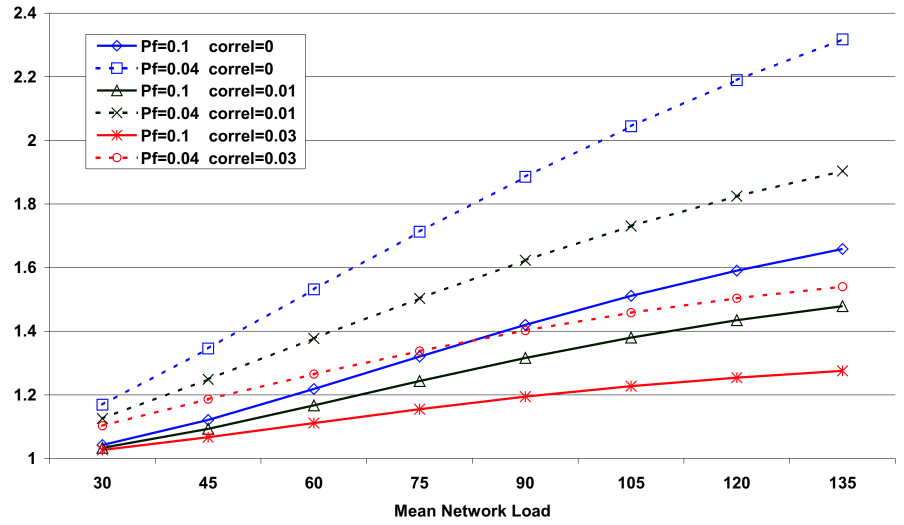

Figure 9: Sharing Ratio of the Protection Channels

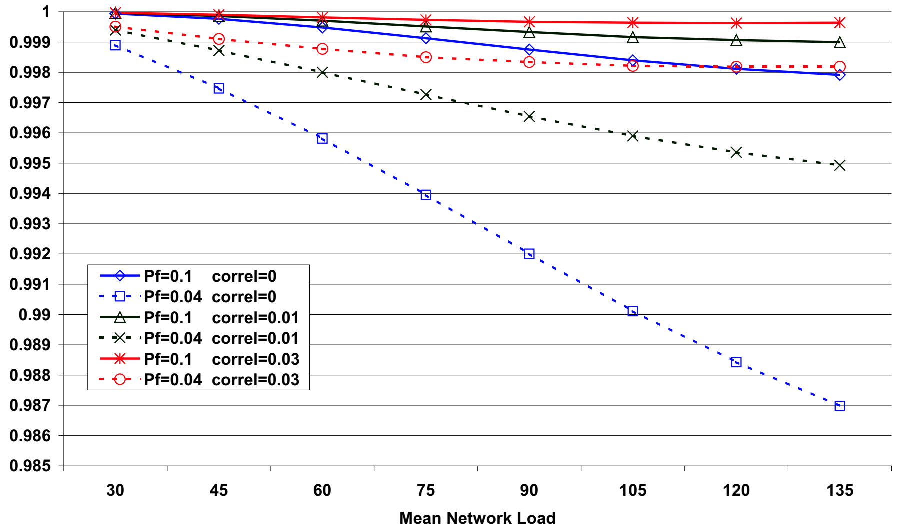

Figure 10: Mean Protection Grade on Each Link

5 Conclusion

Two models have been proposed for the provisioning of protection capacity in large network. The proposed mechanisms are attractive due to their scalability. Moreover, the simulations have shown that high levels of protection can be achieved. The parameters that need to be known for each link are $\{P_f,\ p^*,\ \mathrm{K}\}$ when the binomial distribution is employed and $\{P_f,\ p^*,\ \mathrm{K},\ \alpha\}$ when the beta-binomial distribution is used. The beta-binomial case is reduced to a binomial case when a value of 0 is set for α. The values of P_f and α are allocated for each link and therefore can be adjusted on a link basis. The models enable the variation of the protection level offered and are suitable for applications that do not require a 100% guarantee of protection. Moreover, as the scheme is simple, fast and does not rely on the distribution of per-connection information, it is particularly suited for short-lived connections.

References

[1] O. Gerstel and R. Ramaswami, *Optical Layer Survivability - An Implementation Perspective*, IEEE Journal on Selected Areas in Communications, Vol. 18, No10, pp 1885–1923, Oct. 2000.

[2] M. Sridharan and A. Somani, *Revenue Maximisation in Survivable WDM Networks*, in Proc. SPIE OPTICOMM, Dallas, Texas, Aug. 2000.

[3] F. Touvet and D. Harle, *Shared Backup Protection based on Aggregated Information in WDM Networks*, in Proc. of ICC 2003, Anchorage, Alaska, USA, 11–15 May 2003.

[4] V.F. Nicola and A. Goyal, *Modeling of Correlated Failures and Community Error Recovery in Multiversion Software*, in IEEE Transactions on Software Engineering, Vol.16, No3, March 1990.

[5] R. Bhandari, *Survivable Networks, Algorithms for Diverse Routing*, Kluwer Academic Publishers.

[6] S. Sengupta and R. Ramamurthy, *Capacity Efficient Distributed Routing of Mesh-Restored Lightpaths in Optical Networks*, IEEE GLOBECOM 2001, San Antonio, TX, November 2001.