Adding new Components to the Knowledge Plane in GMPLS over WDM Networks

Anna Urra, Eusebi Calle, J. L. Marzo
Institut d'Informàtica i Aplicacions (IIiA)
Universitat de Girona, Avinguda Lluís Santaló s/n, 17071 Girona
{aurra, eusebi, marzo}@eia.udg.es

***Abstract*— A recent study defines a new network plane: the knowledge plane. The incorporation of the knowledge plane over the network allows having more accurate information of the current and future network states. In this paper, the introduction and management of the network reliability information in the knowledge plane is proposed in order to improve the quality of service with protection routing algorithms in GMPLS over WDM networks. Different experiments prove the efficiency and scalability of the proposed scheme in terms of the percentage of resources used to protect the network.**

Keywords- Knowledge Plane, Quality of Service, GMPLS, WDM.

I. Introduction

The evolution of the multilayer architecture in optical networks has resulted in the reduction of the number of network layers. This is due to the scalability limitation and the high cost added to the entire network [1]. When the number of layers used is less, then the scalability of the network is enhanced and the cost of the network is reduced. We consider two layers in optical architecture: IP/Generalized Multi-Protocol Label Switching (GMPLS) layer and Wavelength-Division Multiplexing (WDM) layer. However, a new layer is introduced to add intelligence to the network. This layer is called knowledge plane (Fig. 1).

Clark [2] has suggested the knowledge plane in his recent proposal. The knowledge plane is a construct that embodies cognitive tools and learning. One of the goals of this layer is to enhance the ability to manage the network intelligently, without disturbing the control and data plane. This new layer adds intelligence into the network management information that can be used to prevent failures and for smart routing.

In this paper we consider a knowledge plane that introduces additional information into the Quality of Service (QoS) with protection routing algorithms. The knowledge plane gathers information of the whole network and analyses and infers new information in order to improve the routing algorithms. With this accurate information obtained and managed by the knowledge plane, future network states can be predicted and taken into account to enhance the network reliability (failure probabilities). In this work, link failures are taken into account only for the study of the network reliability.

Network reliability is an important issue for optical networks because of the high volume of the traffic that they carry. Hence, a failure can result in a loss of several terabits of data per second. This makes the study of failure recovery methods and their impact extremely necessary. Some of the recovery methods studied in the literature include the ones by Mannie [3], Banerjee [4], and Calle [5]. The mechanisms suggested in these papers are applied to only a specific layer. In this paper we mainly focus on enhancing the GMPLS routing while simultaneously taking into account the requirements of the WDM layer.

In Section II, a brief overview of the WDM and GMPLS are provided. The pros and cons of using the protection mechanisms in each layer are enumerated. Afterwards, the network reliability parameters are defined. The resulting model and experimental results are shown in Section IV and Section V respectively. Section VI concludes the paper.

II. GMPLS over WDM Networks: An Overview of Protection Methods

A. *Review of WDM layer*

WDM is an optical network technology that allows efficient use of the high bandwidth. WDM layer uses the physical topology of the network. In this layer, a called lightpath is created to connect a node pair with a fixed path (a sequence of physical links).

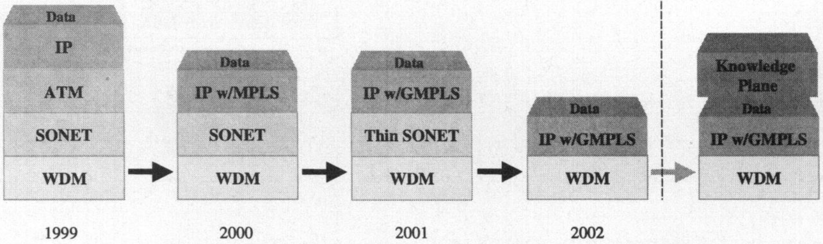

Figure 1. Multilayer architecture evolution in optical networks.

This work was partially supported by the Spanish Research Council (CICYT) under contract TIC2003-05567.

The work of Anna Urra was supported by the Ministry Universities, Research and Information Society (DURSI) and European Social Funds under contract 2003FI 00923.

0-7803-8836-4/04/$20.00 ©2004 IEEE.

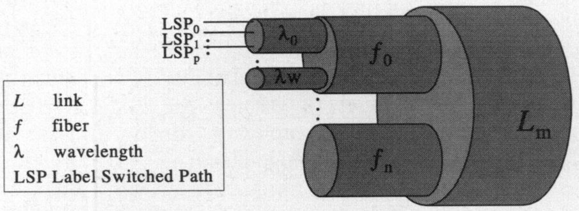

Figure 2. Link hierarchy

In the WDM-based networks, different lightpaths cannot share the same wavelength over the same fiber. When a lightpath is configured, a unique wavelength is assigned to it. This means a reduction of the possibilities to find a future path between a node pair. To solve this issue two methods are defined. Both methods can be jointly used in the WDM networks. First method solves this issue by interconnecting two nodes with many fibers (Fig. 2). Second method is based on adding a wavelength conversion capability at the nodes. A node has a wavelength conversion capability when it can assign the incoming traffic using one wavelength to the outgoing traffic using another wavelength.

B. Review of the GMPLS layer

In the Generalized Multi-Protocol Label Switching (GMPLS) layer, Label Switched Paths (LSPs) are created for connecting a node pair through a sequence of lightpaths defined in WDM layer. Depending upon the characteristics of the WDM layer (node wavelength conversion capability) and the requirement of LSPs, the wavelength continuity constraint has to be realized, i.e., the same wavelength must be used along the entire LSP.

Different LSPs can share the same lightpath (wavelength) as it is shown in Fig. 2. In Fig. 3 the mapping of the WDM layer (Fig. 3a) and the GMPLS layer (Fig. 3b) is shown. The LSP_2 connects the nodes 1 and 5 through the lightpaths L_2 and L_4, i.e., through the physical links, 1-3, 3-4 and 4-5. The LSP_1 connects the same pair nodes through the lightpath L_5 (physical links 1-4 and 4-5).

C. GMPLS and WDM Layer Protection

A trade-off exists between the protection in the WDM layer and protection in the MPLS layer in terms of resource consumption and signaling overheads.

Protection in the WDM layer means switching over to a backup lightpath if one of the lightpaths fails. The number of lightpaths is much smaller than the number of LSPs carried by them. This reduces signaling overheads to notify the end nodes of the failed lightpaths and to activate the backup lightpaths. Therefore, this guarantees fast recovery within a few tens of milliseconds.

On the other hand, the drawback of WDM layer recovery is that the backup lightpaths only carry protected traffic and the working lightpaths only carry working traffic [6]. A backup lightpath is shared by multiple protected lightpaths, but it is not used to carry working traffic. So, resources are used poorly.

D. Review and Analysis of Recovery Methods

Some authors have proposed protection methods related to the recovery of a link failure in WDM and GMPLS [4, 3]. Most of them are based on the establishment of a backup lightpath/LSP where the traffic is switched when the failure occurs. The backup LSPs on the GMPLS layer can be computed before the failure (pre-established), or at the moment when a failure occurs. In this work, we consider that backup LSPs are pre-established.

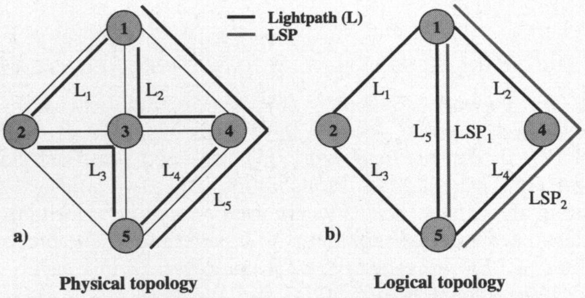

Figure 3. Mapping a) WDM layer over physical topology b) GMPLS layer over logical topology (WDM layer)

Recent studies take into account the link failure probability in the recovery methods [5, 7]. In [7], the failure link probability in WDM layer is defined as the conditional probability when a considered physical link fails due to an occurrence of a single fault. It is assumed that only one physical link can fail at a time in the network, i.e., the failures of two or more physical links are considered to be negligible.

However, this assumption is not applicable to the GMPLS layer. When a physical link failure occurs then all the lightpaths, which this link carries, are broken. As it is shown in Fig.4, when the physical link 4-5 is broken, then the lightpaths L_4 and L_5 fails. For this case, there is two link failures in GMPLS layer: the logical links 1-5 and 4-5.

To solve this inconvenience, the concept of Shared Risk Link Group (SRLG) is introduced in [8] at each layer. A path p belongs to a SRLG k when the failure of k produces the failure of p. So, when a path p is established then the backup path cannot belong to the same SRLG of p. Moreover, two protected LSPs that share backup bandwidth cannot belong to the same SRLG. In Fig. 4, lightpaths L_4 and L_5 belong to the same SRLG in WDM layer, i.e., the LSP_1 and the LSP_2 are in the same SRLG. Thus, in GMPLS layer, when a backup path is established for LSP_2, it does not use the logical link L_5. For such a case, the path with the logical links 1-2(L_1) and 2-5(L_3) are used to create the backup path (BP). Moreover, both LSPs cannot share the backup path capacity because they belong to

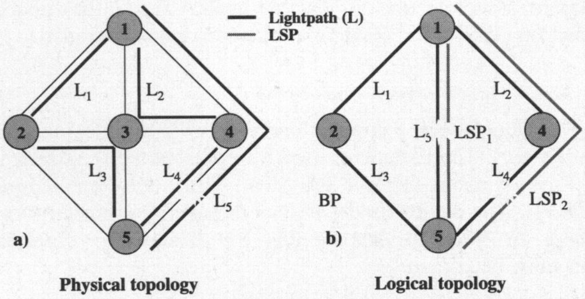

Figure 4. Single physical link failure impact in a) WDM b) GMPLS layer

the same SRLG.

III. Parameters Relating to Network Reliability

The network reliability (failure probabilities) can be provided at different network layers. Our works focus on link failures. In our previous work [5], we used pre-fixed static values of Link Failures Probabilities (LFPs) to improve the routing algorithms. The LFPs are used on routing algorithms in order to decrease the probability of a path failure. The prefixed values of LFP are related to only one layer. In this paper, we take into account both GMPLS and WDM layers in order to differentiate the Physical Link Failure Probability (P_LFP) and the Logical Link Failure Probability (L_LFP). Both Physical and Logical LFPs and the measure of reliability (Mean Time Between Failures) are discussed in this section.

A. *Physical Link Failure Probability*

The calculation of failure probabilities of physical links is discussed in [9]. It assumes that the probability of failure is the same for all physical links with similar physical characteristics. However the probability expression is derived taking into account the physical link only.

The Failure Rate (FR) follows a bathtub curve. First, there is the infant mortality rate that decreases until there is a stable failure rate. After a long period of time, the failure rate tends to increase as a function of time. This behavior must be taken into account on the calculation on the LFP. In addition, there might be failures due to accidents, natural catastrophes caused by the temporary manufacturing process mistakes and other reasons which are statistically not frequent enough but which can be obtained from the tests. These factors determine the actual value of the Physical LFP (P_LFP) at a given moment.

B. *Logical Link Failure Probability*

The Logical LFP (L_LFP) depends on the P_LFP. The P_LFP is a dynamical value since it changes due to the lifetime of the link, geographical conditions, etc. hence, the L_LFP is also dynamic. In this work, we consider that L_LFP is equal to the addition of the probabilities at time *t* of the physical links that the lightpath (*u,v*) crosses.. Therefore:

$$L\_LFP_{uv} = \sum_{(i,j)\in V_{uv}} P\_LFP_{ij} . \qquad (1)$$

where V_{uv} is the set of physical links that the lightpath (*u,v*) crosses.

Moreover, we consider that L_LFP is equal to 0 when the lightpath is protected at WDM layer. Thus, the double protection (WDM and GMPLS protection) can be avoided.

C. *Mean Time Between Failures*

The fibers have a low failure rate with a huge range of failure times. The parameter used to represent the reliability in this kind of components is the Mean Time Between Failures (MTBFs). The MTBF is defined as the average time between failures. In order to calculate this, the distribution of failure times must be known.

IV. Reliability Management through the Knowledge Plane

In this section the concept of reliability is applied to the knowledge plane in order to enhance the GMPLS routing algorithms without adding complexity. In this analysis, the complexity moves to the knowledge plane.

A. *Management of the Information related to Network Reliability*

The knowledge plane evaluates the P_LFP in order to obtain the L_LFP (1). Once P_LFPs are evaluated at time *t*, if they present a significant variation then L_LFPs are recalculated. In order to evaluate the P_LFP we take into account the Failure Rate (FR), the external conditions and the behavior of the physical link.

The amount of traffic that flows through a link can be monitored and a pattern of its behavior obtained. Using this information, a significant variation in link behavior can be detected. At a certain instant, if the statistics increase (for example, in the case of consecutive failures in a short space of time), the possibility of link failure is higher; therefore, this increase must be taken into account in the probability associated with the link failure. This information is calculated and managed by the knowledge plane in order to obtain accurate values of the L_LFP. If the knowledge plane analysis results in significantly different values compared to the current ones, then the information of the GMPLS layer is upgraded.

Another factor used on knowledge plane is the MTBF. If a failure occurs, the time of the next failure can be approximated. Therefore, when a link enters into its failure time interval then the knowledge plane can avoid the use of this link on the new LSPs. The knowledge plane may also be used to perform the activation of the backup paths for these links, in order to avoid losses and delays produced when a link failure occurs. The backup path activation before a failure improves the network reliability. The drawback of this action is that the failure may not occur always and the action taken may not be necessary.

B. *Management of the SRLG*

The management of MTBF, L_LFP and SRLG is also used in this proposal to choose the working and backup LSP. The resource utilization using shared backup LSPs according to the demand reliability requirements improves the resource consumption. The demand reliability requirement is expressed in terms of Maximum Logical LFP (ML_LFP). This means that the total failure probability of a LSP (sum of all the L_LFP of non protected lightpaths of the LSP) must be minor or equal to ML_LFP. The network scenario on Fig. 4 shows this improvement. Let us suppose that all the lightpaths have a L_LFP equal to $3\cdot10^{-4}$ and LSP_1 and LSP_2 have a bandwidth demand of 5 units. When a shared backup path protection is applied the total backup capacity consumed is 10 units since both LSPs belong to the same SRLG and the whole path must be protected. However, when the reliability of the network and ML_LFP are taken into account, the total bandwidth consumption can be reduced. For instance, if ML_LFP of LSP_1 is set to 0 and ML_LFP of LSP_2 is set to $3\cdot10^{-4}$ then the backup LSP_2 can only protect the lightpath L_2 and the backup LSP capacity can be shared. Therefore the total backup capacity consumed is reduced to 5 units.

C. Protection Routing Algorithms with Knowledge: an Approach

The proposal interaction diagram to manage and improve QoS with protection routing algorithms is shown in Fig. 5. This diagram also shows the modules and functionalities of both GMPLS and knowledge plane.

There are two main functionalities of knowledge plane. First functionality is to obtain the Residual Network Module (RNM) that is a simplification of the current network in order to use it for the QoS with protection routing algorithms. This simplification improves the time required to calculate the LSP between a node pair. The L_LFP, the residual capacity of links and the newly created LSP (information about the SRLG) are used to reduce the size of the network in order to calculate the backup LSP.

Second functionality is based on the activation of backup LSPs (Backup LSP Activation Module) according to the MTBF and L_LFP. This allows the reduction of packet loss. Other modules are defined to release these functionalities:

- *P_LFP Module*. It manages the physical layer in order to obtain the failure probability of the physical links. A fuzzy logic method can be used in order to obtain the final value based on geographical conditions, fiber probability and congestion of the link.
- *L_LFP Module*. It calculates the failure probabilities of the lightpaths (logical links at WDM layer) based on (1).
- *MTBF Module*. It manages the MTBF and the information of the last failures.
- *SRLG Module*. It contains all information about the set of SRLG in order to manage the shared backup paths. It is also used to determine the lightpaths that the backup LSP cannot cross.
- *Residual Bandwidth Module*. It contains the information about the residual bandwidth for all the links (lightpaths). This module determines a set of links that must be removed on the residual network because the residual bandwidth is less than the bandwidth requested for the LSP.
- *Fault Management Methods Module*. This module uses the residual network and the LSP request information in order to obtain both LSP and backup LSP optimizing the requirements of the LSP request applying recovery methods. If the LSP can be established, the network state is modified.

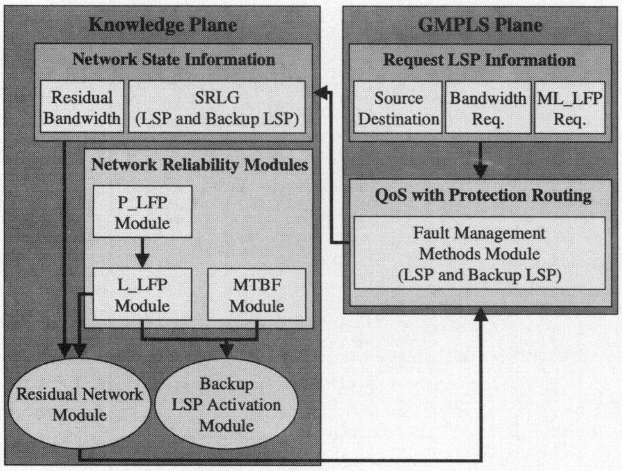
Knowledge Plane
Network State Information
Residual Bandwidth
SRLG (LSP and Backup LSP)
Network Reliability Modules
P_LFP Module
L_LFP Module
MTBF Module
Residual Network Module
Backup LSP Activation Module
GMPLS Plane
Request LSP Information
Source Destination
Bandwidth Req.
ML_LFP Req.
QoS with Protection Routing
Fault Management Methods Module (LSP and Backup LSP)

Figure 5. Modular diagram proposal

D. Agent Role Definition

Implementation proposal is based on using an agent architecture located at the knowledge plane. The agents are defined according to the different functionalities (modules) of the knowledge plane as follows:

- *P_LFP Calculation*: This agent manages the variables (failure statistics, topology, traffic type) and updates the local value of the PLFP for the router in which this link is found. Since the links are bi-directional, each link has two agents to manage it (one for each end of the link). In this way, the agents that manage the same link have to communicate with each other to reach an agreement on the value of the failure probability.
- *MTBF Analysis*: This agent studies the last failures and the MTBF for a set of links in order to determine if there is a possibility of a link failure at a time t.
- *Backup Activation Analysis*: This agent uses the reliability information (L_LFP and MTBF) in order to determine if it is necessary to activate some backup LSPs in order to avoid packet loss due to an expected link failure.
- *Residual Network Calculation*: This agent calculates the residual network for LSPs and once the LSP is known, it is used to calculate the backup LSP (two-step routing algorithm is applied [5]).

V. Experimental Results

In order to evaluate the performance of our proposal scheme, a large set of experiments has been conducted using the well-known NSF network topology with 18 nodes and 30 links, where the link capacity has been chosen to be equal to 480 capacity units. We assume that each link is bi-directional, i.e. it acts like two unidirectional links of half that capacity. In the simulation experiments, LSP requests arrive randomly, at the same average rate for all ingress-egress node pairs. LSPs arrive according to a Poisson process with an average rate λ, and exponentially distributed holding times with a mean value of $1/\mu$. In this set of experiments, $\lambda/\mu = 150$. 10 independent trials were performed over a window of 10,000 LSP set-up requests. For the first set of experiments (figures 6a and 6b) Link Failure Probabilities are randomly assigned to the 47% of the network links. We assume that the rest of the links do not have to be protected. Bandwidth requirement for each LSP is uniformly distributed between 1, 2 or 3 capacity units. The same bandwidth required by the working paths is allocated when establishing the backup paths.

In order to compute the LSPs the well known Widest Shortest Path (WSP) routing algorithm [11] is used. For backup path computation we use two recovery methods in different scenarios: the path protection (Global Backups) without

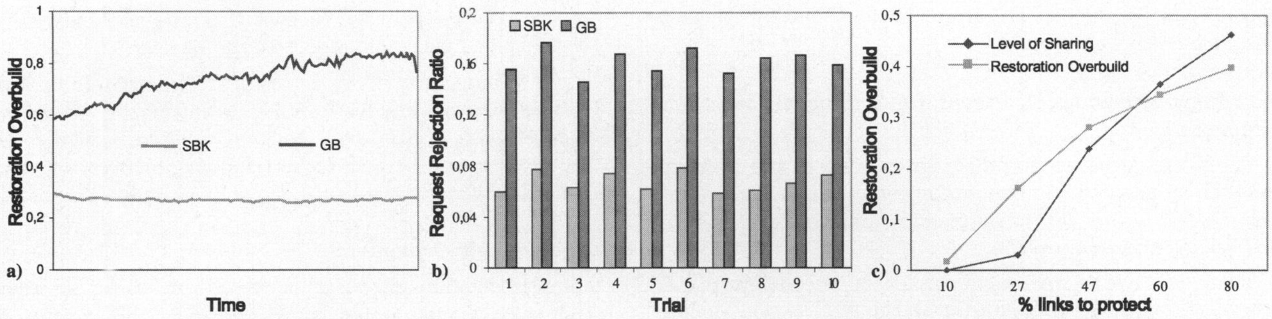

Figure 6. a) SBK and GB Restoration Overbuild. b) SBK and GB Request Rejection Ratio c) Level of Sharing and Restoration Overbuild depending on the network protection requirements.

knowledge plane (GB) and the Segment Backups using the Knowledge plane (SBK). The acceptable Maximum Logical LFP (ML_LFP) is used by the knowledge plane to trigger the segment backup paths computation.

To evaluate the algorithm performances, three figures of merit are used in the experiments: the restoration overbuild (percentage of bandwidth allocated for backup paths divided by the percentage of bandwidth allocated for working paths), the level of sharing (percentage of bandwidth shared in the backup paths divided by the percentage of bandwidth allocated in the backup paths) and the request rejection ratio.

In the first set of experiments we compare the knowledge plane (SBK) and the use of path (global) protection (GB) methods in terms of restoration overbuild (Fig. 6a) and request rejection ratio (Fig. 6b). Results for the Segment Backups using Knowledge plane (SBK) show that this scenario dramatically improves the restoration overbuild in comparison with GB. As shown in Fig. 6b, the number of rejected requests using Segment scenario is approximately half of the requests are rejected when using the Global scenario. For SBK the ratio achieved is really very small (between 0.04 to 0.08). In this case the use of segment protection involves more accurate design of the Network Reliability Module in order to compute the LSP failure probabilities. However, if the ML_LFP are known, segment backup computation improves the use of path protection (GB) in terms of restoration overbuild and request rejection ratio.

For this second set of experiments we only compute segment backups using the knowledge plane. The scalability of our proposal is evaluated increasing the percentage of the network that must be protected. A reasonable percentage of resources is needed to protect the whole network, as the protection requirements increase. In Fig. 6c only a 40% of restoration overbuild is used when a 60% of the network should be protected. One of the reasons to achieve this good results is the use of shared backups. Figure 6c also shows the level of sharing, as the percentage of links to be protected increases.

VI. Conclusions and Future Work

This paper addresses the problem of the QoS with protection routing algorithms on GMPLS over WDM-based networks. In order to improve upon the current methods suggested in the literature, we take into account a new layer, called the knowledge plane. We propose to add some functionalities to the knowledge plane which enables us to manage the information about the current network state and reliability. This is done through agents, which are based upon the modules. These functionalities allow adding more knowledge to the routing algorithms on the GMPLS layer. An added advantage of our scheme is the reduction in the time required for the routing algorithm computation since we use the residual network and not the entire network.

Results have shown that the resources used to protect the network can be reduced using the knowledge plane together with a segment shared backup path computation. Results have also shown that our proposal is scalable, as the network protection requirements increase.

Further simulations and studies on the interaction of the agents to analyze the performance of the routing algorithms with and without the knowledge plane will be included in our future work.

References

[1] A. Banerjee et al. "Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements". IEEE Communications Magazine, January 2001.

[2] David D. Clark, Craig Partridge, J. Cristopher Ramming. "A Knowledge Plane for Internet". In Proceedings of ACM SIGCOMM 2003.

[3] E. Mannie, D. Papadimitriou. "Recovery (Protection and Restoration) Terminology for GMPLS". Internet draft. Work in progress. April 2004.

[4] A. Banerjee et al. "Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and recovery Techniques". IEEE Communications Magazine, July 2001.

[5] E. Calle, J.L. Marzo, A. Urra, Ll. Fabrega. "Enhancing fault management performance of two-step QoS routing algorithms in GMPLS". ICC 2004.

[6] Q. Zheng, G. Mohan. "Protection Approaches for Dynamic Traffic in IP/MPLS over WDM Networks". IEEE Optical Communications, 2003.

[7] M. Tacca et al. "Differentiated reliability in Optical networks: Theoretical and Practical Results". Journal of Lightwave Technology, November 2003.

[8] A. Sebos, J. Yates, G. Hjalmtysson, A. Greenberg. "Effectiveness of Shared Risk Link Group Auto Discovery in Optical Networks". In Proceedings of OFC, 2002.

[9] T. Kuwabara, Y. Mitsunaga, H. Koga. "Calculation Method of Failure Probabilities of Optical Fiber". Journal of Lightwave Technology, July 1993.

[10] E. Calle, J.L. Marzo, A. Urra. "Protection Performance Components in MPLS Networks". In Proceedings of SPECTS 2003.

[11] R. Guerin, D. Williams, A. Orda "QoS Routing Mechanisms and OSPF Extensions", Proceedings of IEEE Globecom. November 1997.