

Enhanced Multi-Layer Protection in Multi-Service GMPLS Networks

Anna Urra, Eusebi Calle, Jose L. Marzo
Institute of Informatics and Applications
University of Girona (UdG)
Girona, Spain
{aurra, eusebi, marzo}@eia.udg.es

Abstract— This paper focuses on QoS routing with protection in an MPLS network over an optical layer. In this multi-layer scenario each layer deploys its own fault management methods. A partially protected optical layer is proposed and the rest of the network is protected at the MPLS layer. New protection schemes that avoid protection duplications are proposed. Moreover, this paper also introduces a new traffic classification based on the level of reliability. The failure impact is evaluated in terms of recovery time depending on the traffic class. The proposed schemes also include a novel variation of minimum interference routing and shared segment backup computation. A complete set of experiments proves that the proposed schemes are more efficient as compared to the previous ones, in terms of resources used to protect the network, failure impact and the request rejection ratio.

Keywords— quality of service; reliability; shared segment protection; traffic engineering; fault recovery time

I. INTRODUCTION

New technologies have enabled increasingly higher volumes of information to be transported over the networks. A number of different kinds of traffic are now being transported over these networks. The telephone customers are accustomed to high network reliability, and they expect a similar level of reliability for their internet traffic services when the required transmissions are critical or prioritized. In this scenario a new definition of traffic services in terms of quality of protection, such as failure recovery time or network level of reliability, must be carried out. On the other hand, Internet Service Providers (ISPs) obviously aim to achieve the required level of protection with minimum resource consumption. Minimum interference routing has become one of the most effective technique in order to reduce the request rejection ratio and, consequently, improving the resource consumption. However, most of the minimum interference routing proposals [1, 2] are only oriented for a working path selection, without taking into account the protection.

In order to enhance the network reliability, different recovery methods applied at different network layers and time scales are used. The use of optical network technology in core network combined with Multi-Protocol Label Switching (MPLS) for offering traffic-engineering capabilities has been

selected as a suitable choice by many ISPs. This combination, MPLS over optical network, is covered by Generalized MPLS (GMPLS). Both optical and MPLS layers deploy their own fault management methods. However, some of the current recovery methods, such as [3, 4, 5], are only applied to a specific layer. On the other hand, fault management can be offered at link or node level. However, node failures can be seen as the failure of all the links within this node. Thereby, in this paper we take into account the single link failures.

We mainly focus on enhancing the online MPLS routing when protection duplications are avoided. Thus, the multi-layer fault management is simplified and the resource consumption is reduced. In order to deploy this idea, the new definition of link-disjoint path using Shared Risk Link Group (SRLG) defined in [6] is taken into account. This paper also encompasses recovery methods with traffic differentiation. Each traffic service is categorized based on its failure impact, evaluated in terms of failure recovery time and reliability requirements.

This paper is organized as follows. In Section II, the existing routing algorithms are analyzed. Section III proposes novel multi-service protection schemes to improve network reliability and reduce the impact in the case of link failure, minimizing the failure recovery time. The simulation scenarios and performance results are presented in Section IV. Section V concludes the paper.

II. LITERATURE SURVEY

Network protection is usually based on the establishment of a link-disjoint path pairs: the working path (WP) and the backup path (BP). When a link failure occurs the WPs, which are affected by the link failure, switch over the traffic to their respective BP. One example of disjoint path-pairs routing algorithm introduced by Suurballe [7] is only oriented towards dedicated protection. Since resources are not shared in dedicated protection, there is poor resource utilization. Shared protection outperforms dedicated protection in terms of resource consumption but, in order to provide efficient resource consumption, the WP links must be known before BP computation [4]. Therefore, a two-step routing algorithm is necessary when shared protection is used. In this section, some existing routing algorithms are analyzed.

This work was supported by the COST 293 and the Spanish Research Council (CICYT) under contract TIC2003-05567. The work of A. Urra was also supported by the Ministry Universities, Research and Information Society (DURSI) and European Social Funds.

A. QoS Routing Algorithms

Traditional QoS routing algorithms, such as the well-known Widest-Shortest Path (WSP) [8], use two different objective functions to optimize network performance, where by the shortest path is selected for minimizing cost and the least loaded path is selected for load balancing.

There is a third objective, which is the minimization of the number of request rejections. Minimum interference routing has become one of the most effective techniques. This set of algorithms was introduced in [1] with the Minimum Interference Routing Algorithm (MIRA). This family of algorithms improves previous QoS routing proposals, however it includes complex computation with large computation times. A proposal that overcomes this drawback was presented in [2] and termed as the Light Minimum Interference Routing (LMIR) algorithm.

B. Reliable QoS Routing Algorithms

A crucial aspect in the development of a fault management system is the selection of backup paths (BPs). Although routing algorithms reviewed in the above section (WSP, MIRA, LMIR) can be used to compute the BP, they do not include any objective to actually improve the protection level such as the maximization of the shared bandwidth or the minimization of the fault recovery time.

Shared protection schemes are developed depending on the available network information. A proposal to compute shared BP based on a Partial Information Routing (PIR) was introduced in [9]. In [10] a proposal of Full Information Routing (FIR) was presented. The main idea of FIR is to assign a weight to each link based on the maximum bandwidth needed if any of the links of the protected path fail and if any of the network links fail. FIR performs better compared to the previous proposals only when the required routing information is available. This drawback can be solved using signaling techniques.

Marzo [12] presents local, segment and global MPLS protection methods. Local and global protection can be shown as particular cases of the segment protection based on the notification time, i.e. the time required to notify the fault from the node detecting the failure and the node responsible for the switchover. Notification time is probably one of the main aspects to be reduced in order to minimize the fault recovery time and offer faster protection [5]. In the case of local protection, the notification time is always 0. In the global case, the node that detects the failure must send a Fault Indication Signal (FIS) to the source node reporting large recovery time when the failure occurs close to the destination node. A trade-off exists between the resource consumption and the failure recovery time minimization. Therefore, our proposed algorithms compute the BP using Shared Segment Protection (SSP). We present heuristic approaches because of the NP-completeness of the SSP problem [12].

III. PROBLEM STATEMENT

In this section the basis of our novel proposed algorithms are discussed in order to offer reliable services with faster

protection. The network scenario and the problem formulation are also described.

A. Protection Routing in the Multi-Layer and Multi-Service GMPLS Network: Basic Ideas

1) Multi-Layer: Avoiding protection duplications

Once the WP is known, a variation of the Partial Disjoint Path (PDP) algorithm [6] is used to compute the BP. As presented in [6], the PDP may overlap with the links of the WP that are already protected at the optical layer and the nodes of the WP. Therefore, no extra resource is necessary in the MPLS layer against failure of protected links in the optical layer. When the PDP overlaps the WP, more than one Segment Backup Paths (SBP) are established. An example is shown in Fig. 1. In Fig. 1, two WPs are sharing the link 5-6 that is protected at the optical layer. The same PDP is used to protect both the WPs. In the first case Fig. 1a), two segment backup paths (SBP₁ and SBP₂) are established between the protected segment paths 3-4-5 and 6-7 since the link 5-6 is already protected. Moreover, the SBP bandwidth is shared in both cases (Fig. 1a and 1b) since the link 5-6 is already protected at the optical layer and, consequently, the SBP defined at the MPLS layer is not activated against the failure of link 5-6. This is possible if the new definition of link-disjoint path based on Shared Risk Link Group (SRLG) presented in [6] is considered. For more details refer to [6].

2) Multi-Service: Resilient Traffic Services.

Not all the current and future traffic services have the same protection requirements. Moreover, in many cases improving the protection involves very expensive fault recovery methods in terms of resource consumption, which cannot be deployed throughout the whole network. In this work we have characterized the traffic protection requirements by using different traffic service categories as shown in Table I.

Three traffic services are defined according to the level of reliability offered and the fault recovery time needed: Low Reliability (LR), Medium Reliability (MR) and High Reliability (HR). The links of the WP that are not protected at

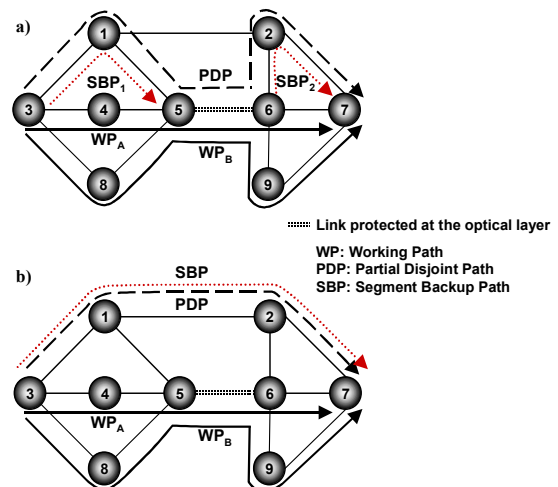


Figure 1. MPLS protection when the Partial Disjoint Path a) overlap protected links at the optical layer b) does not overlap the protected links at the optical layer.

the optical layer are protected using the PDP. For instance, in the case of LR, the PDP can also overlap these links giving them a Partial Protection (PP). Moreover, since this traffic does not require high reliability, faster protection is not required. Thus, global, segment and local protection methods may be used. This is not the case for HR traffic, where faster protection is required and, consequently, only local protection method is used. Moreover, dedicated bandwidth allocation is also used in order to reduce the recovery time. Obviously, in the HR case, full protection is applied.

TABLE I. TRAFFIC SERVICES CLASSIFICATION

Traffic Services	Low Reliability (LR)	Medium Reliability (MR)	High Reliability (HR)
Fault Recovery Time ⁽¹⁾	Medium - Slow (>50 ms)	Very Fast (< 50 ms)	$\equiv 0$
Bandwidth Allocation	Shared	Shared	Dedicated
Protection method	Global, segment, local backups	Segment, local backups	Local backups
Level of protected links ⁽²⁾	Partial	Full	Full

⁽¹⁾Maximum recovery time evaluated in terms of fault notification time (see section II.B).

⁽²⁾With full protection, all the links except the ones protected at optical layer are protected. With partial protection only those links that can reach a shared segment BP with enough bandwidth are protected.

B. Network Scenario

Let $G=(V, E)$ describe the given network, where V is the set of network nodes, and E is the set of network links. Each link $(i, j) \in E$ has an associated L_{ij} physical length; R_{ij} residual bandwidth; D_{ij} total dedicated bandwidth; S_{ij}^{uv} total bandwidth reserved to protect link (u, v) ; and T_{ij} the total shared bandwidth allocated in link (i, j) . Note that S_{ij}^{uv} is equal to 0 when the link (u, v) is protected at the optical layer and $T_{ij} = \max_{(u, v) \in E} (S_{ij}^{uv})$.

Assuming that there is a set of distinguished node pairs P , which may be thought of as a set of potential ingress-egress node pairs, all connection set-up requests occur between these pairs. We denote a generic element of this set by (s, d) .

The setup request is defined by (s, d, b, t) where b specifies the amount of bandwidth required for this request and t specifies the class of traffic. For each setup request, a working path (WP) has to be set-up and a backup path (BP) must also be setup if the WP has at least one link to protect. If there isn't a sufficient bandwidth in the network for either the WP or the BP for the current request, the request is rejected. We neither assume any knowledge about future requests nor any statistical traffic profile.

C. Reliable Services with Fast Protection Routing Algorithm

In this proposal the routing algorithms used to compute the WP and the BP are defined considering multi-layer protection using three traffic classes (see Table I).

Working Path: The k-Minimum Interference Algorithm

In our proposal, the working path routing algorithm aims at minimizing the resource consumption based on minimum interference and the links protected at the optical layer. We

define the k-Minimum Interference (KMI) routing algorithm that selects the k-paths with the minimum interference, using a variation of LMIR, from among all feasible paths. Then, one path is selected according to the traffic class of the request:

- LR: the one with high number of links to protect is selected.
- MR: the one with minimum interference is selected.
- HR: the one with a low number of links to be protected is selected.

Note that LR requests are partially protected, so for this method, only those links that can reach a shared segment BP with enough bandwidth are protected. Note that avoiding a high number of links to protect in the HR case, the number of backup paths with dedicated bandwidth is reduced. This minimizes the resource consumption. If the request is accepted, all links on its WP will reserve b units of bandwidth.

Backup Path: Partial Disjoint Path Algorithm

We propose a variation of the Partial Disjoint Path (PDP) [6] algorithm in order to identify the segment backup paths necessary to protect the working path (see section III.A). First, a weight w_{ij} is assigned on each link according to Equation 1:

$$w_{ij} = \begin{cases} 0 & \text{if } (i, j) \in WP \text{ and } p_{ij} = 1 \\ M & \text{if } (i, j) \in WP \text{ and } p_{ij} = 0 \text{ and } t = LR \\ c_{ij} & \text{if } (i, j) \notin WP \text{ and } (t = MR \text{ or } t = LR) \text{ and } R_{ij} + T_{ij} - A \geq b \\ c_{ij} & \text{if } (i, j) \notin WP \text{ and } t = HR \text{ and } R_{ij} \geq b \\ \infty & \text{otherwise} \end{cases} \quad (1)$$

Where M is a high constant value ($\neq \infty$) that allows the use in the PDP algorithm of the unprotected WP links when partial protection (LR) is considered; A is the maximum capacity necessary if one of the unprotected WP links fails; c_{ij} is the cost assigned to link (i, j) according to LMIR algorithm [2]; and p_{ij} contains 1 if link (i, j) is protected at the optical layer, 0 otherwise. Note that $c_{ij} \leq M$. Once the weight is assigned the PDP is computed.

Algorithm PartialDisjointPath

```

For all ( $v \in V$ ) do
     $Cost(v) = \infty$ 
     $Pred(v) = \text{null}$ 
     $WPlast(v) = s$ 
 $Cost(s) = 0;$ 
 $Q \leftarrow s$ 
while ( $Q$ ) do
     $u \leftarrow \min\_cost(Q)$ 
    for all  $v \in \text{adjacency}(u)$  do
        if ( $Cost(u) + w_{uv} < Cost(v)$ ) then
            if ( $v \in WP$ ) then
                 $WPlast(v) = v$ 
            else  $WPlast(v) = WPlast(u)$ 
            if ( $\text{distance}(WPlast(u), WPlast(v)) < DIST(t)$ ) then
                 $Pred(v) = u$ 
                 $Cost(v) = Cost(u) + w_{uv}$ 
             $Q \leftarrow v$ 

```

In this algorithm $Cost(v)$ is a vector which contains the path cost from s to v ; $Pred(v)$ contains the v 's predecessor node; and $WPlast(v)$ contains the last WP node visited before treating node v . Q represents the list of adjacent vertices which were not yet visited. Function $\min_cost(Q)$ returns the element $u \in Q$

with the lowest $Cost(u)$; $adjacent(u)$ represents the adjacency list of vertex u ; $DIST(t)$ returns the maximum failure notification distance accepted by traffic class t ; and $distance(x,y)$ is the maximum failure notification distance between nodes x and y of the WP.

Once the PDP is computed, the BP links are identified. The links of the PDP, which do not belong to the WP, are the backup links. Other links are considered as unprotected at MPLS layer since they are either protected at the optical layer or they are unprotected because partial protection is applied. The reserved bandwidth will depend on the amount of bandwidth that may be shared in each backup link and the links that are protected at MPLS layer for the shared backup case. In the dedicated backup case, each backup link will reserve b units of bandwidth.

D. Online QoS Restorable Routing Algorithms

We propose three routing schemes based on the two routing algorithms (KMI and PDP) as follows (see Table II):

Reliable Service with Fast Protection (RSFP). This algorithm uses the KMI to compute the WP and the PDP to compute the BP. This algorithm was explained in section III.C.

Semi-Reliable Services (SRS). This algorithm uses the WSP to compute the WP and a variation of the PDP to compute the BP. In SRS, the cost c_{ij} given in Equation 1 is assigned according to FIR algorithm. For this case, dedicated bandwidth allocation cannot be applied using this method. Therefore, the requirements of HR requests are not offered.

Semi-Reliable Service with Minimum Interference (SRSMI). This algorithm uses the KMI to compute the WP and the variation of the PDP used on SRS.

In order to compare our proposals, the next two algorithms without multi-layer and multi-service differentiation are also considered:

No-Reliable Services (NRS). This algorithm has the objective of minimizing the resource consumption used in the backup path. Therefore, FIR is used to compute the backup path, whereas the working path is computed using WSP.

No-Reliable Services with Minimum Interference (NRSMI). This scheme takes into account the minimization of interference. The LMIR is used to compute the WP and the FIR to compute the backup path.

TABLE II. ROUTING SCHEMES

Routing Alg.	Path		Traffic Services		
	WP	BP	LR	MR	HR
RSFP	KMI	PDP	Partial protection using shared backups.	Full protection using shared backups.	Full protection using dedicated backups. $\cong 0$ notification time
SRS	WSP	PDP ⁽¹⁾	Medium\Slow recovery time.	Very fast recovery time.	Full protection using shared backups. $\cong 0$ notification time
SRSMI	KMI	PDP ⁽¹⁾	Medium\Slow recovery time.	Very fast recovery time.	Full protection using shared backups. $\cong 0$ notification time
NRS	WSP	FIR	Full protection using shared backups.		
NRSMI	KMI	FIR	Medium\Slow recovery time.		

⁽¹⁾ Variation of the PDP: the cost c_{ij} (Equation 1) is assigned according to FIR algorithm.

IV. PERFORMANCE EVALUATION

A. Network Topology and Traffic Request Parameters

For this set of experiments the KL topology described in [2] was used. The capacity of the links was 1200 and 4800 units, representing OC-12 and OC-48 rates, respectively. Each link was bi-directional i.e., they acted like two unidirectional links of the same capacity. There were 15 nodes and 28 links. The 40% of links were protected in the optical layer.

Requests arrived 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, λ/μ was 150. Ten independent trials were performed over a window of 10,000 requests to set-up.

The simulations considered LR, MR and HR traffic classes defined in Table I. Fifty percent of the requests were LR, 40% MR and 10% HR. In order to limit the failure notification time of the MR requests, segment backup paths had to guarantee a maximum of 400 miles of failure notification distance. A link length was assigned randomly between 200 and 1000 miles for each network link.

B. Figures of Merit

To evaluate the algorithm performances, three figures of merit were used in the experiments viz. 1) the *request rejection ratio*; 2) *restoration overbuild*, percentage of bandwidth used as a BP with respect to the bandwidth used as a WP; and 3) *failure notification distance*, analysis of the LR and MR failure notification time in terms of notification distance.

C. Simulation Results

First of all, the protection requirements of each traffic class are analyzed in terms of failure notification distance. In the LR case shown in Fig. 2a, the failure notification distance is variable since the notification distance is not limited for LR traffic class. In the case of MR requests shown in Fig. 2b, our proposals accumulate the notification distance between 0 and 400 miles because the notification distance for this traffic class is limited to 400 miles. In the case of HR requests shown in Fig. 2c, our proposals have a notification distance equal to 0 since only local protection is used. On the other hand, NRS and NRSMI algorithms exhibit a random behavior in all cases since the traffic class requirements are not considered.

Figure 3.a shows the performance of the proposed algorithms with Semi-Reliable Services (SRS and SRSMI). Our proposed algorithms offer low request rejection ratio throughout the experiment since HR requests are also protected with shared backup paths (see Table II). This loses reliability required for such a traffic class (see Table I). On the other hand, the RSFP algorithm presents better request rejection ratio compared to the algorithms that do not consider multi-layer protection and multi-service differentiation (NRS and NRSMI).

Finally, in Fig. 3.b, the restoration overbuild is analyzed. In this case our proposal RSFP shows a better behavior since less bandwidth is used as a BP than the rest of the algorithms.

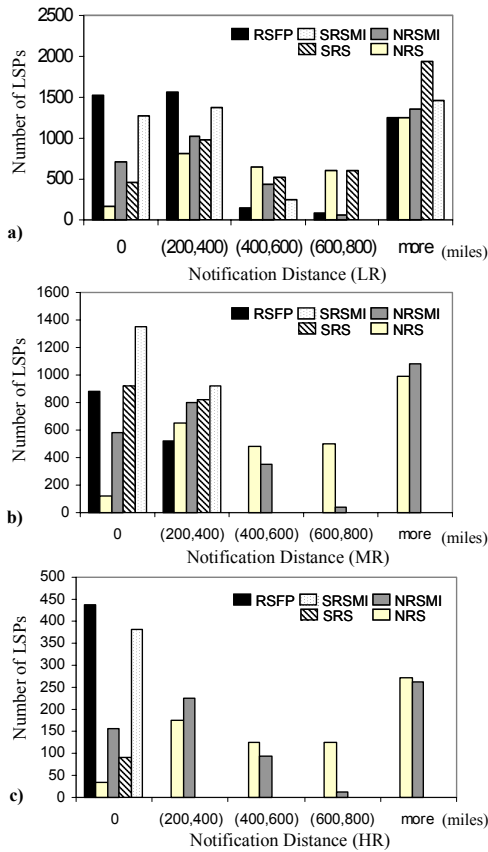


Figure 2. Failure notification distance for a) LR traffic class b) MR traffic class c) HR traffic class.

V. CONCLUSIONS

In this paper novel QoS with protection routing algorithms were introduced in a GMPLS-based network where MPLS requests were set up over an optical layer. The proposed algorithms took into account the multi-layer scenario in order to minimize the resource consumption. A partially protected optical layer was proposed and links that were protected at this layer were not again protected at MPLS layer. Moreover, a new definition of link-disjoint path based on Shared Risk Link Group (SRLG) was made in order to share more backup bandwidth, minimizing the resource consumption. This paper took into consideration different levels of reliability and failure impact in terms of recovery time depending on the traffic class.

Results showed that RSFP algorithm offered the requirements of all the traffic classes without adding resource consumption and request rejection ratio of previous proposals that did not consider traffic differentiation. Moreover, our proposals improved upon the previous ones. SRSMI and SRS are the variations of the RSFP. Although, they both presented a better request rejection ratio, they did not offer the requirements of all traffic and had higher restoration overbuild and recovery time as compared to the RSFP.

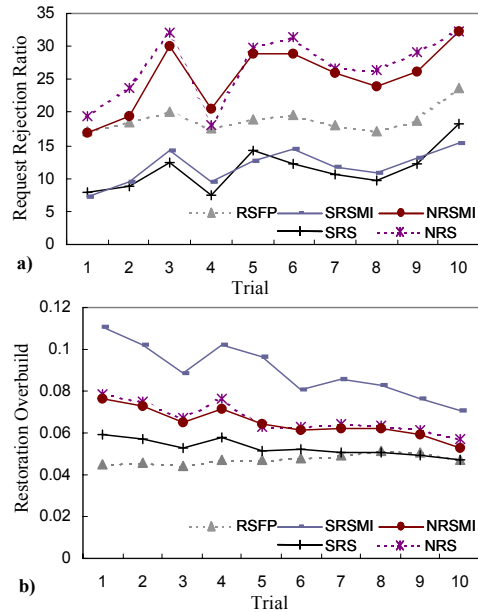


Figure 3. a) Request rejection ratio b) Restoration overbuild.

ACKNOWLEDGMENT

This research was carried out at the Broadband and Wireless Networking Laboratory, Georgia Institute of Technology. Special thanks to Prof. Ian Akyildiz for facilitating my visit at his laboratory, to Dr. Caterina Scoglio for her constructive comments and to Dr. Apurva Mody for his support throughout the paper.

REFERENCES

- [1] M. Kodialam and T. V. Lakshman. "Minimum interference routing with applications to MPLS traffic engineering", in Proc. of IEEE Infocom, Mar. 2000.
- [2] G. B. Figueiredo, N. L. S. Fonseca and J. A. S. Moneiro, "A minimum interference routing algorithm", in Proc. of ICC, Jun. 2004.
- [3] K. Kar, M. Kodialam and T. V. Lakshman, "Routing restorable bandwidth guaranteed connections using maximum 2-route flows," IEEE/ACM Trans. on Networking, col. 11, no. 5, Oct. 2003.
- [4] P.-H. Ho et al. "On achieving optimal survivable routing for shared protection in survivable next-generation Internet," IEEE Trans. on Reliability, vol. 53, no. 2, Jun. 2004.
- [5] E. Calle et al. "Enhancing fault management performance of two-step QoS routing algorithms in GMPLS," in Proc. of IEEE ICC, Jun. 2004.
- [6] A. Urrea, E. Calle and Jose L. Marzo, "Partial Disjoint Path for Multi-layer Protection in GMPLS Networks", in Proc. of DRCN, Oct. 2005.
- [7] R. Bhandari, "Survivable networks: algorithms for diverse routing," Kluwer Academic Publishers, 1999.
- [8] R. Guerin, D. Williams, A. Orda. "QoS routing mechanisms and OSPF extensions", in Proc. of IEEE Globecom, Nov. 1997.
- [9] M. Kodialam and T. V. Lakshman. "Dynamic routing of bandwidth guaranteed tunnels with restoration", in Proc. of IEEE Infocom, Mar. 2000.
- [10] G. Li et al. "Efficient distributed path selection for shared restoration connections", in Proc. of IEEE Infocom, Jun. 2002.
- [11] J. L. Marzo et al. "QoS on-line routing and MPLS multilevel protection: a survey," IEEE Communication Magazine, Oct. 2003.
- [12] J. Tapolcai and P.-H. Ho, "Deeper study on segment shared protection," in Proc. of IEEE ISPAN, 2004.