Reliable services with fast protection in IP/MPLS over optical networks

Anna Urra, Eusebi Calle, and Jose L. Marzo

Institute of Informatics and Applications (IIiA), University of Girona,
Girona 17071, Spain
aurra@eia.udg.es; eusebi@eia.ud.es; marzo@eia.udg.es

Received February 2, 2006; revised August 30, 2006; accepted September 8, 2006; published October 26, 2006 (Doc. ID 67709)

We define new quality-of-service (QoS) routing schemes with protection in Internet Protocol (IP)/Multiprotocol Label Switching (MPLS) over optical networks. The novelty of the proposed routing schemes is the use of the knowledge of the logical links already protected by the optical layer. The logical topology defined by the optical layer is given and fixed, and we assume that it is partially protected. Thereby, at the IP/MPLS layer, spare capacity is reserved to protect only those links that are unprotected. Moreover, we also characterize the traffic services based on their level of reliability and QoS requirements. In order to guarantee fast protection, segment protection and shared backups are combined, resulting in suitable fault recovery time and resource consumption. A complete set of experiments proves that the proposed schemes are more efficient than the previous ones in terms of resources used to protect the network, failure impact, and blocking probability. © 2006 Optical Society of America

OCIS codes: 060.4510, 060.4250.

1. Introduction

The use of wavelength-division-multiplexing (WDM) optical network technology in a core network in combination with Internet Protocol (IP)/Multiprotocol Label Switching (MPLS) for offering traffic-engineering capabilities has been selected as a suitable choice by many Internet service providers (ISPs) [1]. In particular, generalized MPLS (GMPLS) [2] offers the instruments for traffic engineering, constraint-based routing, and many other services required by future Internet applications in this network architecture. Many of these applications, such as e-business critical transactions, require high reliability and quality-of-service (QoS) guarantees from the network.

Ensuring reliability in this scenario is becoming crucial, since a fiber cut results in a large volume of traffic loss. Moreover, single link failures occur and frequently cause disruptions in the service of affected applications [3]. Therefore, survivability is an important issue in guaranteeing such reliability and QoS requirements against network failures. Not all the applications require the same level of reliability. Moreover, some applications are more stringent about their QoS requirements than others. Furthermore, in many cases, improving fault recovery involves very expensive mechanisms in terms of resource consumption, which cannot be deployed throughout the whole network. 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, ISPs obviously aim to achieve the required level of protection with minimum resource consumption. Minimum interference routing has become one of the most effective techniques for reducing the request rejection ratio and, consequently, improving resource consumption. However, most of the minimum interference routing proposals [4,5] are oriented only for a working path selection, without taking into account the protection.

To enhance the network reliability, different recovery mechanisms applied at different network layers and time scales are used. Both optical and IP/MPLS layers deploy their own fault management methods. However, some of the current recovery methods such as those in Refs. [6–8] are applied only to a specific layer.

This paper aims at improving the QoS with protection (QoSP) routing algorithms for IP/MPLS over optical networks. The proposed routing schemes apply segment pro-

1536-5379/06/110870-11/$15.00

tection for fast recovery and consider in their objectives the shareable capacity. The logical topology where the working paths are routed is given, and some of the logical links are already protected at the lower (optical) layer. We exploit this information and, hence, we avoid the protection at the IP/MPLS level of those links that are already optically protected. In order to deploy this idea, a new definition of link-disjoint path using Shared Risk Link Group (SRLG) [9] is introduced. This paper also encompasses different levels of protection. Each traffic service is categorized based on its failure impact and evaluated in terms of failure recovery time and reliability requirements.

The remainder of the paper is organized as follows. In Section 2, the existing routing algorithms are analyzed. Section 3 proposes novel multiservice protection schemes to improve network reliability and reduce the impact in the case of link failure, thus minimizing failure recovery time. The simulation scenarios and performance results are presented in Section 4. Section 5 concludes the paper.

2. Literature Survey

Network protection is usually based on the establishment of 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 BPs. One example of the disjoint-path-pairs routing algorithm, introduced by Suurballe in Ref. [10], is oriented only toward 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 [7]. Therefore, a two-step routing algorithm is necessary when shared protection is used. In this section, some existing routing algorithms are analyzed.

2.A. QoS Routing Algorithms

Traditional QoS routing algorithms such as the well-known Widest-Shortest Path (WSP) [11] use two different objective functions to optimize network performance, whereby 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 Ref. [4] 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 Ref. [5]; this algorithm is termed as Light Minimum Interference Routing (LMIR).

2.B. Reliable QoS Routing Algorithms

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

2.B.1. Routing Information

The accuracy and performance of the shared protection schemes are based on the available network information. The shared backup capacity should be taken into account for reducing the amount of spare capacity. Therefore, the following link-state information is flooded by the routing protocols:

1. *Working capacity* A_{ij}. Total amount of capacity used by WPs.
2. *Spare capacity* S_{ij}. Total amount of capacity reserved. This capacity is not used when the network is in a nonfailure condition.
3. *Residual capacity* R_{ij}. Total amount of capacity that is free to be allocated by WPs or BPs. Note that $R_{ij}=C_{ij}-A_{ij}-S_{ij}$.
4. *Cost* W_{ij}. The cost of using link i is set by the network operators. A path with a smaller cost is typically preferable. In the case of the min hop algorithm the cost is a constant $W_{ij}=1\ \forall(i,j)\in E$.

2.B.2. Full Information Routing Algorithm

Given the accurate information of the additional backup capacity that needs to be reserved on each link, the BP that minimizes ΣS_{ij} may be selected. One approach with full information routing (FIR) was presented in Ref. [12].

In FIR, after selecting the working path, WP, the source node collects the array T_{ij}, $(i,j) \in E$, where T_{ij} is the maximum capacity needed on link (i,j) if a link along the WP fails. This computation is based on the network state before the new restoration connection is routed. The source node then assigns a weight to each link in the network:

$$w_{ij} = \begin{cases} \min(b, T_{ij} + b - S_{ij}) \times W_{ij} & \text{if } T_{ij} + b - S_{ij} > 0 \text{ and } (i,j) \notin WP \\ \varepsilon & \text{if } T_{ij} + b - S_{ij} \leqslant 0 \text{ and } (i,j) \notin WP \\ \infty & \text{if } (i,j) \in WP \end{cases} . \quad (1)$$

Then Dijkstra's algorithm is used to select the backup path, BP, using these weights. The collection of the array T_{ij} is done during signaling exchanges without flooding link-state information, as explained in Ref. [12].

2.B.3. Segment Backup Routing Algorithms

The FIR algorithm uses the global backup method to protect the WP. Hence, when a failure occurs, the source node is responsible for switching over the traffic to the BP. However, the global backup method is one of the slowest methods owing to the fault notification time [13].

Literature includes recent proposals for reducing the recovery time by accounting for notification distance [7,14,15]. These proposals consider segment backup methods that focus on the BP computation given a WP. Although proposals in Refs. [14] and [15] consider sharing the backup capacity, this is considered only when the BP is established and not during the BP computation. Therefore, a reduction of the recovery time is achieved, but an efficient use of the spare capacity is not guaranteed.

3. Problem Statement

In this section we discuss the basis of our proposed algorithms as means for reliable services with fast protection. The network scenario and the problem formulation are also described.

Our proposal aims at improving the QoSP routing algorithms for IP/MPLS-based networks. Thus its objectives are as follows:

- Improve the spare capacity using shared backups.
- Reduce the recovery time by applying segment backup methods.
- Assume the knowledge of the logical links protected at the lower (optical) layer in order to avoid protection duplications.
- Classify each traffic class according to its QoS requirements.
- Select the BP and WP according to the QoS requirements of the requests. Segment protection and shared backups are combined in order to guarantee fast protection, which results in suitable fault recovery time and resource consumption.

3.A. Protection Routing in the Multilayer and Multiservice Network: Basic Ideas

3.A.1. Avoiding Protection Duplications Using Multilayer

This proposal is IP/MPLS-based, and the logical topology where the WPs are routed is assumed to be given. The proposed routing schemes use the knowledge of the logical links already protected by the optical layer. Hence, at the IP/MPLS layer, spare capacity is reserved only to protect those links that are unprotected. An example is shown in Fig. 1.

The WP between node pair (3, 2) does not need to establish a BP because logical link (3, 2) at the IP/MPLS layer, i.e., lightpath $L_1(3-1-2)$ at the optical layer is already protected by the backup lightpath $BL_1(3-4-2)$. Thus, the multilayer fault management is simplified, and the resource consumption is reduced.

In this proposal, the logical topology used to route the WPs and BPs is considered to be partially protected at the optical layer. Thus, in the IP/MPLS network scenario, protected and unprotected logical links coexist:

- *Protected links*. Links of the IP/MPLS network that are already protected by the

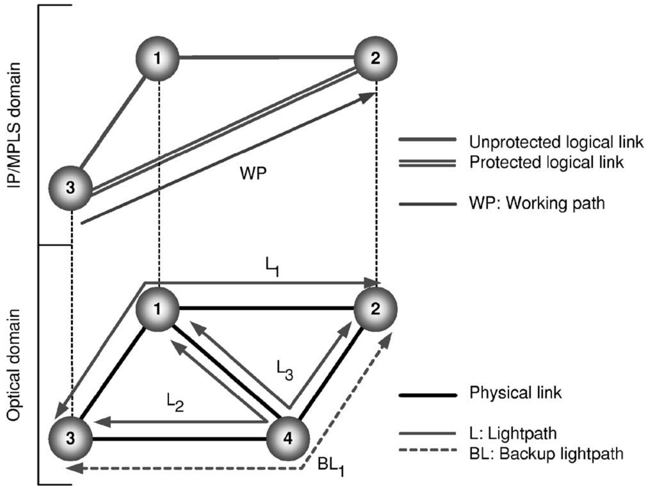

Fig. 1. Multilayer protection.

lower (optical) layer recovery mechanisms. These links do not need extra recovery resources at IP/MPLS layer against their failure.

- *Unprotected links*. Links of the IP/MPLS network that are not protected. Some mechanism must be offered at the IP/MPLS layer in order to recover the traffic from their failure. Therefore, no extra resources are necessary in IP/MPLS against failure of protected links at the optical layer. Once the WP is known, the BP can be computed. As a novelty, the BP is proposed to be a partial disjoint path (PDP), since it may overlap with the nodes of the WP and the links of the WP already protected at the optical layer. When the PDP overlaps with the WP, more than one BP is established, i.e., segment backup paths (SBPs) are established. Hence, when a PDP is computed, the optical protected links may either belong to the protected segment path or not belong to the protected segment path. Both cases are shown in Figs. 2(a) and 2(b), respectively. In Fig. 2, two WPs are established and share link 3–4, which is protected at the optical layer. The same PDP is used to protect both of the WPs. In the first case (a), the computed PDP overlaps WP_A and WP_B. This means that two segment BPs (SBP_1 and SBP_2) are established between the protected segment paths $s-3$ and $4-d$, since link 3–4 is already protected. Moreover, the SBP capacity is shared in both cases [Figs. 2(a) and 2(b)], since the shared link 3–4 does not need to be protected at the MPLS layer.

This is not possible if the definition of link-disjoint path based on shared risk link group (SRLG) is considered [9]: *two data paths are link-disjoint if no two links on the two paths belong to the same SRLG*. As shown in Fig. 2(b), both the WP_A and the WP_B belong to the same SRLG, since they are sharing link 3–4, thus BP capacity is not shareable. However, this link is already protected at the optical layer and, consequently, the SBP defined at the MPLS layer is not activated against the failure of link

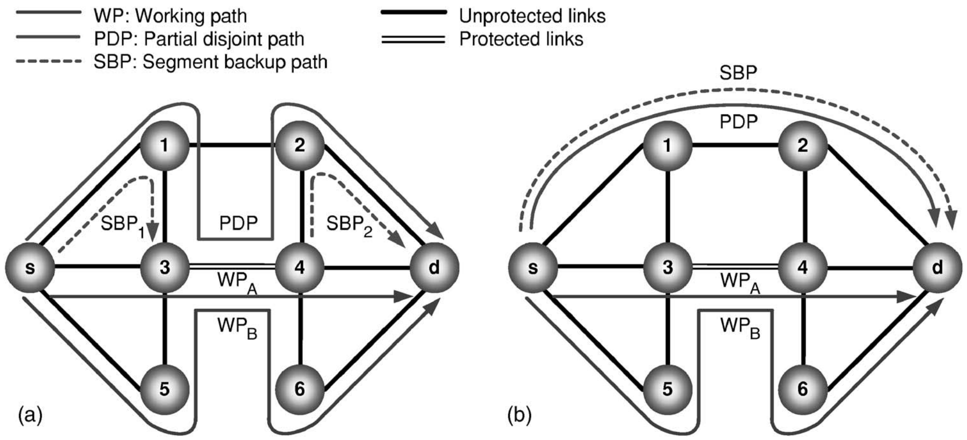

Fig. 2. IP/MPLS protection when the partial disjoint path (a) overlaps protected links (b) does not overlap protected links.

3–4. Therefore, in the multilayer scenario considered in this paper, two data paths are link-disjointed if the links that are ***unprotected do not belong to the same SRLG.***

3.A.2. Multiservice: Resilient Traffic Services

Another aspect of expanding QoS routing performance is the use of the traffic-profile concept to characterize the sensibility of a class of traffic in the case of a failure. Thus, the routing algorithm may act in different ways depending on the traffic class.

In this work we have characterized the traffic protection requirements by using different traffic service categories as shown in Table 1. Three levels of reliability are considered according to the requirements of the traffic services:

- *Low Reliability* (LR). Protection is offered if there are sufficient network resources. Partial protection is applied for LR traffic. With partial protection only those unprotected links that can reach a BP with sufficient capacity are protected. Fast protection is not required, thus global, segment, and local protection methods may be used.
- *Medium Reliability* (MR). Full protection is required, i.e., all the unprotected links must be protected. In order to reduce the fault recovery time, only segment and local methods may be used.
- *High Reliability* (HR). Fast recovery is required for protecting all the unprotected links. Consequently, only the local protection method is used to protect HR traffic. Moreover, dedicated capacity allocation is also used in order to reduce the recovery time. The level of reliability is decided by the ISPs. ISPs determine the most suitable recovery mechanism with low network cost (in terms of spare capacity, scalability, and simplicity) for each new connection by means of the service level agreement (SLA) [16]. The SLA framework is beyond the scope of this paper.

3.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 capacity; S_{ij} spare capacity; and T_{ij} the maximum capacity needed on link (i,j) if a link along the *WP* fails.

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 setup 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 capacity required for this request and t specifies the class of traffic. For each setup request, a WP has to be set up and a BP must also be set up if the WP has at least one link to protect. If there is not sufficient capacity 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.

3.C. Reliable Services with Fast Protection Routing Algorithm

3.C.1. WP: k-Minimum Interference Algorithm

In this proposal, the WP routing algorithm aims at minimizing the resource consumption based on minimum interference and the knowledge of 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 t of the request:

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

Table 1. Traffic Services Classification

Traffic Services	Low Reliability (LR)	Medium Reliability (MR)	High Reliability (HR)
Level of protected links	Partial	Full	Full
Fault recovery time	Medium, slow	Fast	Very fast (≃0)
Protection method	Global, segment, Local backups	Segment, local Backups	Local Backups
Protection architecture	Shared	Shared	Dedicated

- *LR*: the one with a high number of links to protect is selected. Note that LR requests are partially protected, so for this method, only those links that can reach a shared segment BP with sufficient capacity are protected. Note that avoiding a high number of links to protect in the HR case reduces the number of BPs with dedicated capacity. This minimizes the resource consumption. If the request is accepted, all links on its WP will reserve b units of capacity.

3.C.2. BP: Resilient Partial Disjoint Path Algorithm

We propose the Resilient Partial Disjoint Path (RPDP) algorithm in order to identify the segment BPs necessary to protect the WP (see Subsection 3.A.1). First, a weight w_{ij} is assigned to each link as

$$w_{ij} = \begin{cases} 0 & \text{if } (i,j) \in WP \text{ and } p_{ij}=1 \\ M & \text{if } (i,j) \in WP \text{ and } p_{ij}=0 \text{ and } t=LR \\ c_{ij} & \text{if } (i,j) \notin WP \text{ and } (t=MR \text{ or } t=LR) \text{ and } R_{ij}+S_{ij}-E \geqslant b \\ c_{ij} & \text{if } (i,j) \notin WP \text{ and } t=HR \text{ and } R_{ij} \geqslant b \\ \infty & \text{otherwise} \end{cases}, \qquad (2)$$

where M is a high constant value ($\neq\infty$) that allows the use of the unprotected WP links in the RPDP algorithm when partial protection (LR) is considered; E 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 the LMIR algorithm [5]; and p_{ij} identifies the unprotected links. Note that $c_{ij}<M$. Once the weight is assigned, the RPDP is computed (see Algorithm 1).

In the RPDP algorithm $Cost(v)$ is a vector that 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 that were not yet visited. Function $min\_cost(Q)$ returns the element $u \in Q$ with the lowest $Cost(u)$; $adjacency(u)$ 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.

```
Algorithm 1 Resilient Partial Disjoint Path
INPUT
$s$: source node;
$d$: destination node;
$G=(V,E)$: network graph;
WP: working path;
ALGORITHM
for all $v \in V$ do
  $Cost(v)=\infty$
  $Pred(v)=s$
  $WPlast(v)=s$
end for
$Cost(s)=0$
$Q \leftarrow s$
while ($Q$) do
  $u \leftarrow min\_cost(Q)$
  $Q=Q-\{u\}$
  for all $v \in adjacency(u,G)$ do
    if $(Cost(u)+w_{uv}<Cost(v)$ then
      if $v \in WP$ then
        $WPlast(v)=v$
      else
        $WPlast(v)=WPlast(u)$
      end if
      if
$distance(WPlast(u),WPlast(v))<DIST(t)$
then
```

```
                $Pred(v)=u$
                $Cost(v)=Cost(u)+w_{uv}$
                $Q \leftarrow v$
            end if
        end if
    end for
end while
```

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 the IP/MPLS layer, since they are either protected at the optical layer or they are unprotected because partial protection is applied. The reserved capacity will depend on the amount of capacity that may be shared in each backup link and the links that are protected at IP/MPLS layer for the shared backup case. In the dedicated backup case, each backup link will reserve b units of capacity.

3.D. Routing Information

The information required by the algorithms, such as the maximum reservable capacity, is available in current extensions of Open Shortest Path First (OSPF) and Intermediate System-Intermediate System Protocol (IS-IS) for GMPLS. Either OSPF or IS-IS can be used to distribute link-state information by flooding. Other information, such as the total reserved restoration resources over all network links, used by the FIR algorithms to compute shared backups, can be obtained using signaling [12].

3.E. Online QoS Restorable Routing Algorithms

We propose three routing schemes based on KMI and RPDP as follows (see Table 2):

- *Reliable Services with Fast Protection* (RSFP). This routing scheme uses the KMI to compute the WP and the RPDP to compute the BP.
- *Semi-Reliable Services* (SRS). This routing scheme uses the WSP to compute the WP and uses a variation of the RPDP to compute the BP. In SRS, the cost c_{ij} given in Eq. (1) is assigned. For this case, dedicated capacity allocation cannot be applied. Therefore, the requirements of HR requests are not offered.
- *Semi-Reliable Services with Minimum Interference* (SRSMI). This routing scheme uses the KMI to compute the WP and the variation of the RPDP used on SRS.

In order to set a basis of comparison for our proposed routing schemes, the next two routing schemes without multilayer and multiservice differentiation are considered:

- *No Reliable Services* (NRS) [14]. This scheme has the objective of minimizing the resource consumption used in the BP. Therefore, FIR is used to compute the BP, whereas the WP 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 BP.

Table 2. Routing Schemes

Routing Schemes	Path		Traffic Services		
	WP	BP	LR	MR	HR
RSFP	KMI	RPDP Eq. (2)	Partial protection, shared backups, medium, slow recovery time	Full protection, shared backups, fast recovery time	Full protection, dedicated backups, very fast recovery time ($\simeq 0$)
SRS	WSP	RPDP Eq. (1)			Full protection, shared backups, very fast recovery time
SRSMI	KMI	RPDP Eq. (1)			
NRS	WSP	FIR	Full protection, shared backups, medium, slow recovery time		
NRSMI	LMIR	FIR			

4. Performance Evaluation

4.A. Network Topology and Traffic Request Parameters

For this set of experiments the KL topology described in Ref. [4] is used. The KL topology consists of 15 nodes and 28 links. Each link is bidirectional, i.e., they act like two unidirectional links of the same capacity. The bandwidth of the links is 1200 and 4800 units, representing OC-12 and OC-48 rates, respectively. Algorithms are evaluated under the KL topology with 15%, 30%, 45%, 60%, 70%, and 85% of unprotected links at the optical layer.

Requests arrive according to a Poisson process with an average rate λ and with exponentially distributed holding times having a mean value of $1/\mu$. In this set of experiments, λ/μ is 150. Ten independent trials are performed over a window of 10,000 requests. The allocated capacity for the requests is uniformly distributed to 10, 20, or 30 capacity units. Thereby, the performance of the schemes is analyzed under a high network load. This will lead to a higher blocking probability than the acceptable blocking probability in real networks. However, these simulations tend to evaluate the routing schemes at extreme conditions.

The simulations consider LR, MR, and HR traffic classes defined in Table 1. One of the objectives of this paper is to analyze the behavior of the algorithms in a multiservice environment. Even after our extensive literature search, statistical patterns for traffic class distribution could not be found. Thus we assume that 50% of the requests are considered LR, 40% MR, and 10% HR.

In order to limit the failure notification time of the MR requests, segment BPs have to guarantee a maximum of 400 miles of failure notification distance. The link length is assigned randomly between 200 and 1000 miles for each network link.

4.B. Figures of Merit

To evaluate the algorithm performances, three figures of merit are used:

- *Blocking Probability*. This value corresponds to the request rejection ratio for the whole network.
- *Restoration Overbuild*. This value corresponds to the average of the total spare capacity, S_{ij}, and working capacity, A_{ij}, for the whole network: $\Sigma_{(i,j)\in E}S_{ij}/\Sigma_{(i,j)\in E}A_{ij}$.
- *Fault Notification Time*. Analysis of the LR, MR, and HR fault notification times. This value is expressed in terms of fault notification distance.

4.C. Simulation Results

First, the amount of network resources used by the routing schemes is evaluated in terms of blocking probability and restoration overbuild. As shown in Fig. 3(a), the proposed RSFP scheme outperforms the schemes that do not consider multilayer protection and multiservice differentiation (NRS and NRSMI) for network scenarios with less than 60% (low/medium) of unprotected links. However, for the network scenarios with a high percentage of links to protect, the RSFP blocking probability increases, and it results in either similar or worse behavior than NRS and NRSMI. This is because of the dedicated local backups that are set up to protect HR requests. Thus, for a large number of unprotected network links, more dedicated local backups are needed, which requires high network resource consumption. On the other hand, the proposed SRS and SRSMI routing schemes are significantly better than the rest of the

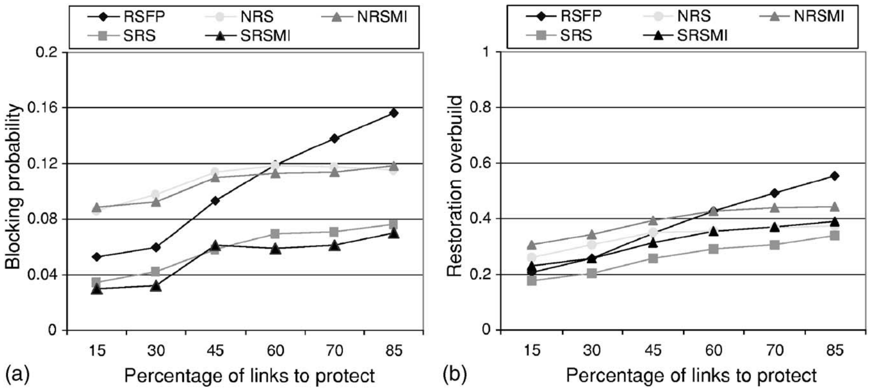

Fig. 3. (a) Blocking probability, (b) restoration overbuild.

routing schemes throughout the experiment. SRS and SRSMI schemes show improvement over the RSFP scheme due to the shared backup mechanism used to protect HR requests (see Table 2). It can be concluded from this simulation that using the RPDP scheme shows improvement over the previous routing schemes (NRS and NRSMI) for (1) all network scenarios when a shared backup mechanism is used to protect HR requests (SRS and SRSMI) and (2) low/medium protected network when a dedicated backup mechanism is used to protect HR requests (RSFP).

In terms of restoration overbuild, results presented in Fig. 3(b) show that the proposed RPDP-based schemes (RSFP, SRS, and SRSMI) use low backup network resources. However, RSFP performance, as expected, degrades when a high percentage of links have to be protected due to the dedicated capacity reservation as pointed out above in the analysis of blocking probability. Our proposed SRS scheme combines the benefits of the RPDP algorithm and the sharing-oriented (FIR) backups resulting in performance improvement over the proposed KMI-based RSFP and SRSMI schemes.

Next, the protection requirements of each traffic class are analyzed in terms of fault notification distance when only 45% of the links are unprotected for clarity because the behavior of all the routing schemes is similar in all cases in terms of recovery time. In the LR case shown in Fig. 4(a), the fault notification distance is variable, since the notification distance is not limited for the LR traffic class. In the case of MR requests shown in Fig. 4(b), 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. 4(c), our proposals have a notification distance equal to 0, since only local protection is used. On the other hand, NRS and NRSMI schemes exhibit a random behavior in all cases, since the traffic class requirements are not considered. Consequently, they suffer from extended recovery times.

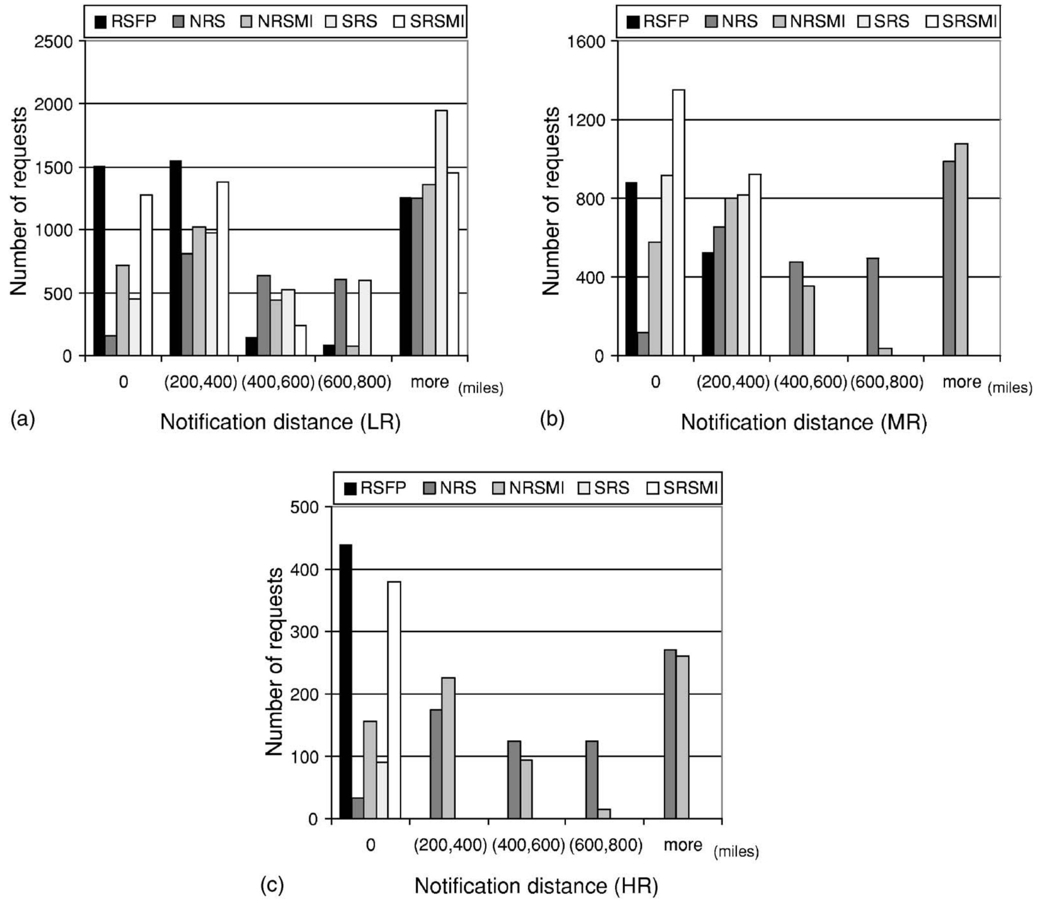

Fig. 4. Fault notification distance for (a) LR, (b) MR, and (c) HR traffic class.

5. Conclusions

In this paper, novel QoS with protection routing schemes have been introduced, where IP/MPLS requests have been set up over an optical layer. The proposed routing algorithms take into account the knowledge of the logical links already protected at the lower/optical layer. Thus, those links that are protected at the optical layer are not again protected at IP/MPLS layer, which reduces the network resources reserved for protection. Moreover, a new definition of link-disjoint path based on Shared Risk Link Group (SRLG) has been made in order to share more backup capacity and thus minimize the resource consumption.

In order to guarantee fast protection, segment protection and shared backups have been combined, resulting in a suitable fault recovery time. This paper has also taken into consideration different levels of reliability and failure impact in terms of recovery time depending on the QoS traffic class requirements.

Results have shown that for the network scenarios with low and medium unprotected links, the proposed RSFP scheme offers the requirements of all the traffic classes and improves upon previous proposals that do not consider traffic differentiation. For a high percentage of unprotected links, SRS and SRSMI outperform the existing schemes. Our proposed SRS scheme combines the benefits of the RPDP algorithms and the sharing-oriented FIR backups, resulting in performance improvement over the proposed KMI-based RSFP and SRSMI algorithms. SRSMI and SRS schemes present a better request rejection ratio, though they do not offer the requirements of all traffic and have a higher recovery time as compared with the RSFP.

Acknowledgments

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. Special thanks are given to Apurva Mody for his constructive comments and support throughout the paper.

References

1. J. Y. Wei, “Advances in the management and control of optical Internet,” IEEE J. Sel. Areas Commun. **20**, 768–785, (2002).
2. E. Mannie, “Generalized Multi-protocol Label Switching (GMPLS) Architecture,” IETF RFC 3945 (Internet Engineering Task Force, 2004).
3. W. D. Grover, “*Mesh-based Survivable Networks: Options and Strategies for Optical, MPLS, SONET, and ATM Networking*” (Prentice Hall PTR, 2004).
4. M. Kodialam and T. V. Lakshman, “Minimum interference routing with applications to MPLS traffic engineering,” in *Proceedings of IEEE Infocom* (IEEE, 2000), pp. 884–893.
5. G. B. Figueiredo, N. L. S. Fonseca, and J. A. S. Moneiro, “A minimum interference routing algorithm,” in *Proceedings of the International Conference on Communications (ICC)* (IEEE, 2004), pp. 1001–1005.
6. K. Kar, M. Kodialam, and T. V. Lakshman, “Routing restorable bandwidth guaranteed connections using maximum 2-route flows,” in *Proceedings of the IEEE Infocom* (IEEE, 2002), pp. 772–781.
7. P.-H. Ho, J. Topolcai, and H. T. Mouftah, “On achieving optimal survivable routing for shared protection in survivable next-generation Internet,” IEEE Trans. Reliab. **53**, 216–225 (2004).
8. E. Calle, J. L. Marzo, A. Urra, and L. Fabrega, “Enhancing fault management performance of two-step QoS routing algorithms in GMPLS,” in *Proceedings of the International Conference on Communications (ICC)* (IEEE, 2004), pp. 1932–1936.
9. P. Sebos, J. Yates, G. Hjalmtysson, and A. Greenberg, “Auto-discovery of shared risk link groups,” in *Optical Fiber Communication Conference (OFC)* (Optical Society of America, 2001).
10. R. Bhandari, “*Survivable Networks: Algorithms for Diverse Routing*,” (Kluwer Academic, 1999).
11. R. Guerin, D. Williams, and A. Orda, “QoS routing mechanisms and OSPF extensions,” in *Proceedings of IEEE Globecom* (IEEE, 1997), pp. 1903–1908.
12. G. Li, D. Wang, C. Kalmanek, and R. Doverspike, “Efficient distributed path selection for shared restoration connections,” in *Proceedings of IEEE Infocom* (IEEE, 2002), pp. 140–149.
13. J. L. Marzo, E. Calle, C. Scoglio, and T. Anjali, “QoS on-line routing and MPLS multilevel protection: a survey,” IEEE Commun. Mag. **41**(10), 126–132 (2003).
14. L. Li, M. Buddhikot, C. Chekuri, and K. Guo, “Routing bandwidth guaranteed paths with local restoration in label switched networks,” in *Proceedings of the IEEE International Conference on Network Protocols (ICNP)* (IEEE, 2002), pp. 110–120.

15. D. Xu, Y. Xiong, and C. Qiao, “Novel algorithms for shared segment protection,” IEEE J. Sel. Areas Commun. **21**, 1320–1331 (2003).
16. W. Fawaz, B. Daheb, O. Audouin, M. Du-Pond, and G. Pujolle, “Service level agreement and provisioning in optical networks,” in IEEE Commun. Mag. **42**(1), 36–43 (2004).