Incorporating Protection Mechanisms in the Dynamic Multi-Layer Routing Schemes [⋆]

Anna Urra, Eusebi Calle, Jose L. Marzo and Pere Vila

Institute of Informatics and Applications (IIiA),
University of Girona, 17071 Girona, Spain

Abstract. In the next generation backbone networks, IP/MPLS over optical networks, the ability to maintain an acceptable level of reliability has become crucial since a failure can result in a loss of several terabits of data per second. Although routing schemes with protection exist, they generally relate to a single switching layer: either wavelength or packet switching oriented. This paper presents a new dynamic and multi-layer routing scheme with protection that considers cooperation between IP/MPLS and optical switching domains. A complete set of experiments proves that the proposed scheme is more efficient when compared to routing algorithms with full optical protection or full IP/MPLS protection.

1 Introduction

The use of optical technology in core networks combined with IP/Multi-Protocol Label Switching (MPLS) [1] solution has been presented as a suitable choice for the next generation Internet architecture. The integration of both layers is facilitated by the development of Generalized MPLS (GMPLS) [2]. In this network architecture, a single fiber failure can result in potentially huge data losses as the effects propagate up and through the network causing disruptions in the service of many applications. Thus, survivability has become a key issue to improve and satisfy the increasing requirements of reliability and Quality of Service (QoS) of these applications. Fault recovery schemes have been adopted in the network in order to provide such survivability. These schemes are based on switching the traffic affected by the failure to a backup path. The computation of the working and backup paths is a crucial step to offer the required QoS to the traffic services. Some relevant parameters, such as resource consumption and recovery time, could be affected negatively if suitable routing algorithms are not used.

According to the timing of backup path computation, recovery mechanisms are classified in protection and restoration [3]. Although restoration is flexible

[⋆] This work was supported by the Spanish Research Council (TEC2006-03883/TCM) and the Generalitat de Catalunya through grant SGR-00296. The work of A. Urra was also supported by the Ministry Universities, Research and Information Society (DURSI) and European Social Funds.

in terms of resource consumption, it offers low recovery time and the recovery action may not be successful because of insufficient network resources. Protection describes recovery schemes that are pre-planned for both spare capacity and backup paths achieving the shortest recovery time and providing high availability against network failures. The accuracy and performance of routing algorithms with protection in terms of resource consumption depends on the available network information. The availability of full or partial network information influences the management of the network capacity [4]. The reduction of the recovery time is another parameter to be considered for backup path selection and it is achieved by applying segment or local backup path methods instead of path protection [5].

Nowadays different QoS routing algorithms exist that consider protection mechanisms, full/partial network information and local/segment backups [4, 6–8]. However, these routing schemes operate in a single switching layer: either optical and wavelength oriented or IP/MPLS and Label Switched Path (LSP) oriented. Thus, both optical and IP/MPLS layers independently deploy their own fault recovery methods.This results in protection duplications making fault management more difficult and poor resource utilization. Two network scenarios may be considered in order to improve network management and resources: 1) the static multi-layer network scenario or 2) the dynamic multi-layer network scenario. In the *static multi-layer network scenario* [9, 10], the logical topology defined by the optical layer is given, fixed and partially protected. Some of the logical links are assumed to be already protected at the optical layer. Thereby, at the IP/MPLS layer, spare capacity is reserved to protect only those logical links that are unprotected. In the *dynamic multi-layer network scenario*, interoperability between each IP/MPLS and optical switching domain is considered. Although effort has been devoted in developing dynamic multi-layer routing schemes that consider both switching domains [11], protection is not considered amongst them. In this paper, a dynamic cooperation between wavelength and LSP domain is taken into account in order to provide protected paths cost-effectively.

2 Multi-layer Architecture Overview

In the multi-layer architecture, Label Switched Paths (LSPs) are routed in the optical network through lightpaths. For better utilization of the network resources, LSPs should be efficiently multiplexed into lightpaths and then, these lightpaths should be demultiplexed into LSPs at some router. This procedure of multiplexing/demultiplexing and switching LSPs onto/from lightpaths is called traffic grooming. Traffic grooming is an important issue for next generation optical networks. Photonic multi-layer routers have the technology to implement traffic grooming [11]. Each consists of a number of Packet-Switching Capable (PSC) ports (p) and number of wavelengths (w). The number of PSC indicates how many lightpaths can be demultiplexed into this router, whereas the number of wavelengths corresponds to the number of wavelengths connected to the same adjacent router. Three scenarios are associated with p according to the following switch architectures [12]:

- Single-hop grooming: $p = 0$. Using this type of switching architecture, the network does not offer packet switching capability at intermediate nodes. Thus, traffic from a source node is multiplexed onto a direct lightpath to the destination node. In this case, either backup lightpaths at the optical domain or global backup LSPs (path protection) at the IP/MPLS domain are established to protect the connections.
- Multihop partial-grooming: $0 < p < w$. In this case, some wavelengths may be demultiplexed at the intermediate nodes for switching at finer granularity. Therefore, some LSPs will be able to perform segment/local protection.
- Multihop full-grooming: $p = w$. Every wavelength on each fiber link forms a lightpath between adjacent node pairs. Thus, the logical topology is predetermined and exactly the same as the physical topology. All the IP/MPLS protection strategies, i.e. global, segment and local, are suitable for all LSPs.

Note that, although the PSC ports at intermediate nodes allow performing packet segment/local protection, the number of optical-electrical-optical (o-e-o) conversions increases. Thus, the cost of o-e-o conversions must be considered during the path computation because they represent a bottleneck to network throughput and also influence the overall delay.

The granularity of the recovery strategy is also an important parameter in terms of time recovery and fault management. Diverse switching granularity levels exist into the optical IP/MPLS network scenario. Going from coarser to finer, there is fiber, wavelength (lightpath) and LSP switching. The level of recovery at the optical layer is bundle of lightpaths or individual lightpaths. Since recovering at the optical layer recovers affected connections in-group, the recovery action is fast and easier to manage than recovering each affected LSP individually in the IP/MPLS layer. However, the coarser is the granularity; the higher the resource consumption. The finer IP/MPLS granularity results in better resource consumption.

3 Problem Statement

In this section we discuss the basis of our proposed routing scheme. A tradeoff exists between the resource consumption and the cost added to the network in terms of recovery time, failure management and node technology. Better use of network resources is achieved by recovering at IP/MPLS layer due to its finer switching granularity. However, the recovery actions at optical domain are much faster and easier to manage, since the affected connections are recovered in group. Therefore, a cooperation between both layers seems to be the solution in order to take the advantages of each switching domain.

The proposal presented in this paper is a first order approach that takes into account the dynamic multi-layer network scenario. This proposal is based on the establishment of link-disjoint lightpath/LSP pairs: the lightpath/LSP and the backup lightpath/LSP. When a failure occurs at a lightpath, the traffic is switched to the respective backup lightpath. If no backup lightpath exists, the traffic is switched to the respective backup LSPs. The main objective is to take advantage of both switching domains.

3.1 Network Definition

Let $G_P = (V, E_P)$ and $G_L = (V, E_L)$ represent the physical topology and the logical topology respectively, where V is the set of photonic MPLS routers; E_P and E_L are the set of network physical links and lightpath respectively. Each router has p input and output PSC ports, where $PSCi(u)$ input ports and $PCSo(u)$ output ports of node u are already not assigned to any lightpath. Each physical link has w wavelengths. When a LSP is requested, the proposed routing scheme considers both physical links and lightpaths, i.e. $E_P \cup E_L$. In order to univocally identify the physical links and existing lightpaths that connect node pair (i, j) the 3-tuple (i, j, k) is used. Thus, the link (i, j, k) is a physical link if $k = 0$, otherwise $(k > 0)$ it is a lightpath.

Each (i, j, k) lightpath has an associated R_{ijk} residual capacity; S_{ijk}^{uv} total capacity reserved to protect the physical link $(u, v, 0)$; and T_{ijk} the total shared capacity allocated in link (i, j, k). LSP requests are defined by (s, d, b) where (s, d) is the source and destination node pair; and b, specifies the amount of capacity required for this request. For each request, a working LSP (WP) has to be set-up. A backup LSP (BP) must be also set-up, whenever the WP has, at least, one unprotected lightpath. If there are not sufficient resources in the network, for either the WP or the BP, the request is rejected.

3.2 Lightpath and LSP Computation

In the proposed scheme, a new procedure to compute the WP is presented. In this procedure the following cost parameters are taken into account:

1. The residual capacity of the link candidates, R_{ijk}.
2. The maximum number of hops, H, i.e. maximum number of lightpaths that the WP may traverse.
3. The free packet switching ports of each router, $PCSi$ and $PSCo$.

Note that the residual capacity of the physical links with free wavelengths is the capacity of the wavelength. The proposed procedure, called Dynamic Multi-Layer Routing (DMR) algorithm (Algorithm 1), computes the min-hop WP based on a variation of the Dijkstra algorithm. In this case, the number of hops coincides with the number of lightpaths. Thus, the consecutive sequence of physical links, that constitutes a lightpath, is only considered as one hop. The DMR procedure uses the network graph composed by lightpaths and physical links, i.e. $G = (V, E_P \cup E_L)$. This procedure ends when it reaches the destination node or there is no feasible path between source and destination nodes. If a feasible path exists then the procedure may return:

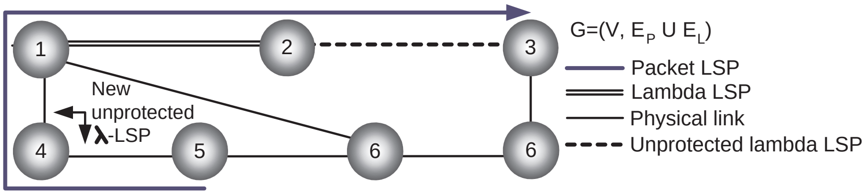

Fig. 1. Working p-LSP computation. Creation of a new unprotected lightpath using the physical links (5,4) and (4,1).

1. A sequence of existing protected lightpaths.
2. A sequence of physical links. In this case, a new unprotected lightpath is set up between source and destination node.
3. A sequence of physical links, protected and unprotected lightpaths. In this case, new unprotected lightpaths are setup for each consecutive sequence of physical links as shown in Fig. 1. In this example, a new unprotected lightpath is set up with the physical links (5,4) and (4,1).

Algorithm 1 Dynamic Multi-Layer Routing

```
for all $v \in V$ do
    $Cost(v) = \infty$
    $Pred(v) = s$
    $WPlast(v) = s$
$Cost(s) = 0$
$Q \leftarrow s$
while $(d \notin Q$ and $Q \neq \emptyset)$ do
    $u \leftarrow min\_cost(Q)$
    $Q = Q - \{u\}$
    for all $v \in adjacency(u, G)$ do
        for all $(u, v, k) \in E$ do
            if $(R_{ijk} \geq b)$ and $((k = WPlast(u) = 0)$
            or $(Cost(u) + 1 < Cost(v) < H))$ then
                if $(PSCi(v) > 0$ and $WPLast(u) > 0$
                and $k = 0)$ or $(PSCo(v) > 0$ and $k > 0$
                and $WPlast(u) = 0)$ or $(WPlast(u) > 0$
                and $k > 0)$ or $(k = WPlast(u) = 0)$ then
                    $Pred(v) = u$
                    $WPlast(v) = k$
                    $Q \leftarrow v$
                    if not $(k = WPlast(u) = 0)$ then
                        $Cost(v) = Cost(u) + 1$
```

In the DMR algorithm (Alg. 1), $Cost(v)$ is a vector containing the path cost from s to v; $Pred(v)$ contains the v's predecessor node; and $WPlast(v)$ contains the identifier k of link (u, v). Q represents the list of adjacent vertices which are not visited yet. Function $min\_cost(Q)$ returns the element $u \in Q$ with the lowest $Cost(u)$; and $adjacency(u)$ is the adjacency list of vertex u in graph G.

3.3 Backup Lightpath and LSP Computation

Once the WP is known, the BP is computed. Three different procedures could be applied depending on the WP characteristics:

Step 1. If the WP is a sequence of existing protected lightpaths, the computation of the BP is not required.

Step 2. If the WP is a new unprotected lightpath and an available and shareable backup lightpath exists, this is used to protect the lightpath. Otherwise, a new backup lightpath is set-up applying DMR algorithm (Algorithm 1) with $G = (V, E_P)$. If the procedure fails to find a backup lightpath, go to Step 3.

Step 3. If the WP is a combination of protected and unprotected lightpaths, then a variation of the Partial Disjoint Path (PDP) algorithm [9] is used to compute the BP. The variations are the ones included to the Dijkstra algorithm in order to consider the packet switching ports in the DMR algorithm. The PDP may overlap with protected lightpaths of the WP, since they are already protected, and the nodes of the WP. Therefore, no extra resources are necessary in the IP/MPLS layer against failure of protected lightpaths in the optical layer. When the BP overlaps the WP, more than one segment backup paths are established.

4 Performance Evaluation

4.1 Restorable Routing Algorithms

Our proposed Dynamic Multi-layer Routing scheme with Protection (DMP) is evaluated. DMP computes the WP using the DMR algorithm (Alg. 1) and the BP according to the criteria presented in Section 3.3. In order to compare the merits of the new routing scheme, the following algorithms based on Oki policies [11] are also considered:

- Policy 1 with Protection (P1P). The routing policy 1 first tries to allocate the LSPs to an existing lightpath. If a lightpath is not available then a sequence of existing lightpaths with two or more hops that connects the source and destination nodes are selected. Otherwise, a new one-hop lightpath is established. When a new lightpath is created, then a backup lightpath is also set up.
- Policy 2 with Protection (P2P). The routing policy 2 first tries to allocate the LSPs to an existing lightpath. If the lightpath is not available then a new one-hop lightpath is established and selected as the new LSP. Otherwise, a

Table 1. Routing schemes for multi-layer protection evaluation.

Routing scheme	**Working path**	**Backup path**	**Protection domain**	**Switching architecture**
DMP	DMR (Alg. 1)	DMR (Sec. 3.3)	IP/MPLS and optical protection	Multihop partial grooming
P1P	Policy 1	Backup lightpaths	Optical protection	Multihop partial grooming
P2P	Policy 2	Backup lightpaths	Optical protection	Multihop partial grooming
FIR	WSP	FIR	IP/MPLS protection	Multihop full grooming

sequence of existing lightpaths with two or more hops are selected. As in the case of the P1P algorithm, a backup lightpath is set up when a new lightpath is created.

If P1P and P2P fail to find a feasible LSP or backup lightpath, then the request is rejected.

As shown in Table 1, the Full Routing Information (FIR) algorithm [4] is also considered in order to evaluate the performance of the new routing scheme when only IP/MPLS protection is applied. In this case, the Widest Shortest Path (WSP) is used to compute the WP.

4.2 Simulation Results

For this set of simulations the request rejection ratio and the network resource consumption are analyzed according to the following parameters:

- H: The maximum number of lightpaths that a LSP may traverse. The number of hops is an important parameter since it cuts down the number of o-e-o conversions.
- p: The number of PSC ports per node.
- w: The number of wavelengths per fiber.

Note that the FIR scheme is simulated under *multihop full grooming*. Thereby, its performance is independent of p and w.

The NSFNET topology described in [11] is used. NSFNET topology consists of 14 nodes and 21 physical links. Each physical link is bi-directional, with the same number of wavelengths in each direction. The transmission speed of each wavelength is set to 10 Gbps. The number of PSC ports p is the same in each node.

Figure 2 shows the performance of the proposed scheme, DMP, compared to 1) optical oriented routing algorithms with protection, P1P and P2P, and 2) IP/MPLS oriented routing algorithm with protection, FIR. Results show that the proposed DMP outperforms P1P and P2P schemes because of the finer granularity. P2P is practically independent of the number of hops because of the first-create procedure used to compute the LSP. Hence, most of the LSPs have low number of hops. However, each lightpath may traverse several physical links, consuming high amount of wavelengths. On the other hand, FIR presents a sharp increase in the request rejection ratio from $H = 6$ because there are no many disjoint paths with number of hops ≤ 6 and, consequently, many requests are rejected for $H < 6$.

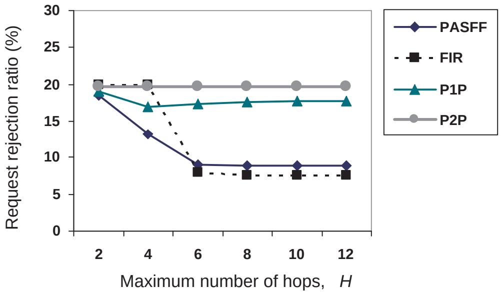

Fig. 2. Number of hops analysis ($p = 10$).

Next two results show the influence of the number of PSC ports per node for all routing algorithms when $H = 4$ and $H = 6$ (see Fig. 3). FIR operates under multihop full grooming ($p = w$), however, the results are shown in order to present the IP/MPLS bound of the solution in terms of capacity when $H = 6$. Again, DMP scheme results in better use of the network resources compared to P1P and P2P. When p is small, the rejections are due to few available PSC ports and, for all, optical protection is applied.

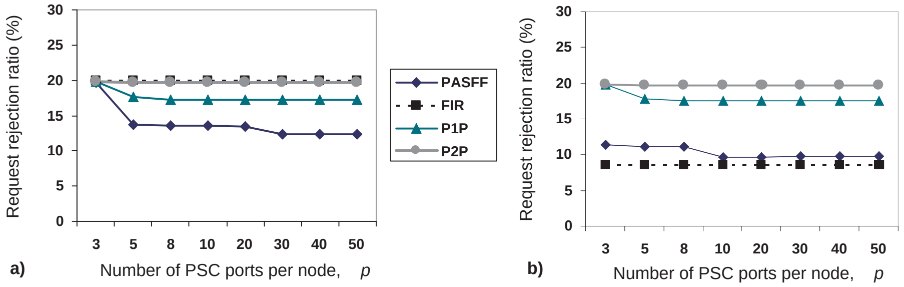

Fig. 3. Number of PSC ports per node analysis when a) $H = 4$ b) $H = 6$.

Figure 4 shows the influence of the number of wavelengths per fiber when $p = 10$ and $H = 4$ and $H = 6$. As shown, the number of rejected requests lineally increases for FIR when $H = 6$. Moreover, since P2P prioritize lightpaths that directly connects source and destination nodes, it outperforms P1P when $w > 24$. Plus, P2P also offers better performance than DMP when $H = 4$ for $w > 24$. Note that DMP and FIR behavior sharply change according to the maximum number of hops (see Fig. 2) while P1P and P2P do not.

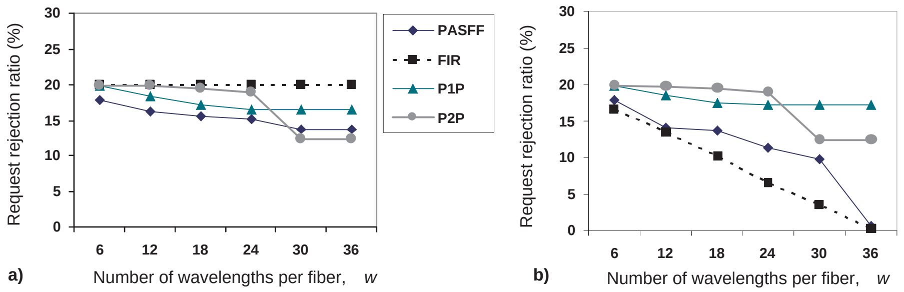

Fig. 4. Number of wavelengths per fiber analysis when $p = 10$ and a)$H = 4$ b)$H = 6$.

From these results, it can be concluded that the DMP algorithm allows decreasing the rejected requests due to the finest recovery granularity at the IP/MPLS domain. Additionally, DMP outperforms FIR algorithm when the number of o-e-o conversions is reduced (H). Moreover, when $H \geq 6$, DMP only outperforms FIR when the network nodes have high number of PSC ports.

In terms of resource consumption analysis, first the total number of lightpaths and backup lightpaths established is evaluated in Fig. 5. The case of $H = 4$ and $w = 18$ is only plotted for clarity since the behavior of all the schemes is similar in all cases in terms of network resources. Figure 5a shows the total number of lightpaths created. Since FIR operates under *multihop full grooming*, each wavelength is seen as a lightpath. Knowing that 1) the number of links of the NSF network is 21, 2) there is a bi-directional fiber per link and 3) each fiber has 18 wavelengths; the total number of lightpaths in the network for FIR is $21 \cdot 2 \cdot 18 = 756$. This number is an upper bound of the maximum number of lightpaths that may be established. In the DMP scheme, when the number of PSC ports increases, the number of new lightpaths slightly increases. On the other hand, the number of new lightpaths sharply increases from $PSC = 3$ to $PSC = 10$ for P1P and P2P algorithms. The number of PSC ports has higher impact to P1P and P2P schemes because of the full optical protection applied. This is shown in Fig. 5b, where the curve of new backup lightpaths has similar behavior than the one of new lightpaths for P1P and P2P. However, although P1P has similar number of new lightpath than P2P, it has lower number of new backup lightpaths respect to P2P; P1P scheme shares higher number of backup lightpaths. In the case of DMP scheme, few lightpaths are optically protected because most of the failures are recovered at IP/MPLS domain.

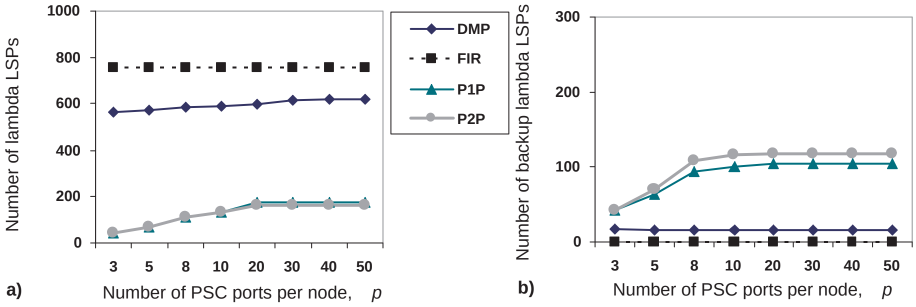

Fig. 5. Total number of a) lightpaths and b) backup lightpaths for $H = 4$ and $w = 18$.

Figure 6 analyzes the average of hops of the LSPs. P2P results into low average number of lightpaths per LSP since it gives priority at creating new lightpaths for each request, see Fig. 6. On the other hand, the rest of the algorithms offer an average of two lightpaths per LSP. Taking into account that $H = 4$, LSPs may traverse up to 4 lightpaths, thus, the theoretical average number is $\frac{1+2+3+4}{4} = 2.5$. Thereby, the new LSPs have usually less than 4 lightpaths when P1P, FIR and DMP algorithms are applied. Note that the best algorithm in terms of hops is P2P; it requires low amount of packet switching operations. However, it suffers from high request rejection ratio.

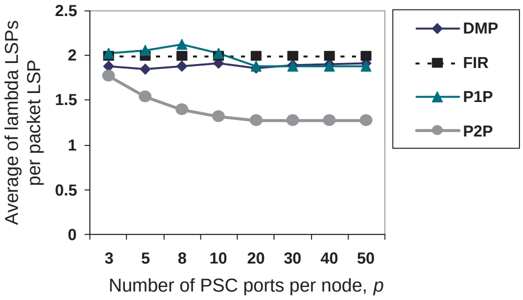

Fig. 6. Average of a) physical links per λ-LSP b) λ-LSPs per p-LSP and c) physical links per p-LSP, for $H = 4$ and $w = 18$.

5 Conclusions

In this paper a novel routing scheme has been proposed: the Dynamic Multilayer routing with Protection (DMP) scheme. DMP scheme considers a dynamic cooperation between packet and wavelength switching domain in order to minimize the resource consumption. Results have shown that FIR and DMP are the best schemes in terms of network resources. The use of IP/MPLS recovery mechanisms with finer granularity results into better filling of the capacity and less number of rejected requests comparing to P1P and P2P that apply protection at optical domain. Moreover, when the number of o-e-o conversions is limited (H), the proposed scheme outperforms the FIR scheme that only considers IP/MPLS recovery. Thus, DMP should be chosen to compute new lightpaths/LSPs and their backups; reducing the number of o-e-o operations and making an efficient use of the network resources.

References

1. E. Rosen, A. Viswanathan and R. Callon: Multiprotocol label switching architecture,IETF RFC 3031,(2001).
2. E. Mannie: Generalized Multi-Protocol Label Switching (GMPLS) architecture, IETF RFC 3945, (2004).
3. V. Sharma and F. Hellstrand: Framework for Multi-Protocol Label Switching (MPLS)-based recovery, IETF RFC 3469, (2003).
4. G. Li, D. Wang, C. Kalmanek and R. Doverspike: Efficient distributed path selection for shared restoration connections, IEEE Infocom, (2002) 140–149.
5. J. L. Marzo, E. Calle, C. Scoglio and T. Anjali: QoS on-line routing and MPLS multilevel protection: a survey, IEEE Commun. Mag. **41,** (2003) 126–132.
6. P.-H. Ho, J. Tapolcai and H. T. Mouftah: On achieving optimal survivable routing for shared protection in survivable next-generation Internet, IEEE Trans. Reliab. **53,** (2004) 216–225.
7. D. Xu, Y. Xiong and C. Qiao: Novel algorithms for shared segment protection, IEEE J. Sel. Areas Commun. **21,** (2003) 1320–1331.
8. K. Kar, M. Kodialam and T. V. Lakshman: Routing restorable bandwidth guaranteed connections using maximum 2-route flows, IEEE Infocom, (2002) 772–781.
9. A. Urra, E. Calle and J. L. Marzo: Reliable services with fast protection in IP/MPLS over optical networks, Journal of Optical Networking **5,** (2006) 870–880.
10. A. Urra, E. Calle and J. L. Marzo: Enhanced multi-layer protection in multi-service GMPLS networks, IEEE Globecom, (2005) 286–290.
11. E. Oki, K. Shiomoto, D. Shimazaki, N. Yamanaka, W. Imajuku and Y. Takigawa: Dynamic multilayer routing schemes in GMPLS-based IP+Optical networks, IEEE Commun. Mag. **43,** (2005) 108–114.
12. K. Zhu, H. Sang and B. Mukherje: A comprehensive study on next-generation optical grooming switches, J. Sel. Areas Comm. **21,** (2003) 1173–1186.