Multi-Layer Network Recovery: Avoiding Traffic Disruptions against Fiber Failures *

Anna Urra, Eusebi Calle and Jose L. Marzo

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

Abstract. The next generation backbone networks, optical IP/MPLS networks, enable increasingly higher volumes of information to be transported. In this network architecture, a fiber failure can result in a loss of several terabits of data per second and leads to multiple failures in the upper network layer. Thus, the ability of the network to maintain an acceptable level of reliability has become crucial. In this paper, a dynamic cooperation between packet and wavelength switching domain is considered in order to provide protected paths cost effectively. A new multi-layer routing scheme that incorporates recovery mechanisms in order to guarantee connectivity against any single fiber failure is presented.

1 Introduction

The use of Wavelength Division Multiplexing (WDM) optical network technology in core network combined with IP/Multi-Protocol Label Switching (MPLS) for offering traffic-engineering capabilities has been selected as a suitable choice by many Internet Service Providers (ISPs) [1]. In particular GMPLS offers the instruments for traffic engineering, constraint-based routing and many other services required by future Internet applications in this network architecture [2]. Many of these applications, like e-business critical transactions, require high reliability and QoS guarantees from the network. However, single fiber failures occur frequently causing disruptions in the service of affected applications [3]. Moreover, a fiber failure can result in a loss of several terabits of data per second and leads to multiple failures in the upper network layer at the same time. Recovery techniques are defined in order to avoid these disruptions and reduce the failure impact. Thus, the traffic affected by the failure is switched over from the working path to an alternative/backup path. The selection of both working and backup paths depends on the skill of the routing algorithm applied and the current network state.

In this paper, we propose and analyze a multi-layer routing scheme that incorporates recovery mechanisms against single fiber failures. A dynamic cooperation between packet and wavelength switching domain is taken into account in order to provide protected paths cost effectively. New metrics, such as the equipment cost, switching granularity and resource consumption are also considered.

* This work was supported by the COST293, the Spanish Research Council (TIC2003-05567) and the Ministry Universities, Research and Information Society (DURSI).

2 Recovery Considerations in Multi-layer Networks

2.1 Photonic MPLS Router: Packet Switching Capabilities

Diverse switching granularity levels exist into the optical IP/MPLS network scenario. From coarser to finer there is fiber, wavelength and packet switching. The new photonic MPLS routers offer packet and wavelength switching [4]. Thus, packet Label Switch Paths (p-LSPs) are routed in the optical network through wavelength paths, called lambda LSPs (λ-LSPs).

For a better utilization of the network resources, p-LSPs should be efficiently multiplexed into λ-LSPs and then, these (λ-LSPs) should be demultiplexed into p-LSPs at some router. This procedure of multiplexing/demultiplexing and switching p-LSPs onto/from λ-LSPs is called traffic grooming [5]. The photonic MPLS routers have the technology to implement traffic grooming. It consists of a p number of Packet-Switching Capable (PSC) ports and w number of wavelengths [6]. The number of PSC indicates how many lambda LSPs can be demultiplexed into this router, whereas the number of wavelengths corresponds to the number of wavelengths connected to the same adjacent router. Based on these parameters, a new resource constraint is added to the network. Three scenarios exists according to p: a) $p = 0$; b) $0 < p < w$ and c) $p = w$. Lets suppose a network scenario where w is equal to 2. If the value of p is equal to 0, then the network does not offer packet switching capability at intermediate nodes. Thus, the protection should be performed either at the optical domain and λ-LSP oriented or at the IP/MPLS domain and p-LSP using only path protection (global). On the other hand, if $0 < p < w$, then not all the wavelengths may be demultiplexed at the intermediate nodes. In this case only one wavelength may be demultiplexed at intermediate nodes. Therefore, not all the p-LSP will be able to perform segment/local protection. Finally, when p is equal to w all the protection strategies, i.e. global, segment and local, are suitable.

2.2 Routing Algorithms in the Multi-layer Architecture

Routing algorithms can be categorized in static or dynamic depending on the type of routing information used for computing LSPs. Static algorithms use network information that does not change with time, meanwhile dynamic algorithms use the current state of the network. In the multi-layer dynamic case, the λ-LSPs are set up, if necessary, whenever a new p-LSP is requested.

A first framework for dynamic multi-layer routing was proposed by Oki [6]. Oki proposed different policies to allocate the packet LSPs to an existing lambda LSP. If the lambda LSP is not available then either 1) a sequence of existing lambda LSPs with two or more hops that connects the source and destination nodes are selected or 2) a new one-hop lambda LSP is established and selected as the new packet LSP. The main drawback of these policies is that the network connectivity is not guaranteed. An example is shown in Fig. 1. Lets suppose that a new packet LSP between the nodes (1,3) is requested and a new lambda LSP (1,2,3), i.e. the λ-LSP$_1$, is set up according to the routing policies presented by

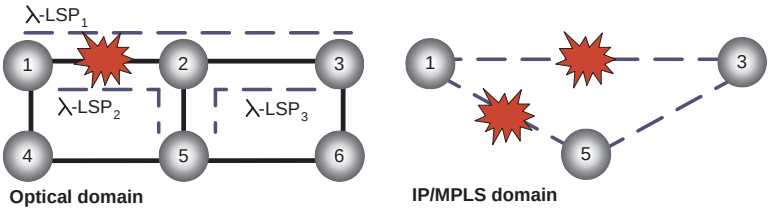

Fig. 1. Loss of connectivity at IP/MPLS domain due to a single link failure.

Oki [6]. In this example, both policies presented by Oki give the same result. The same procedure is applied to set-up two new LSPs between the nodes (1,5) and (3,5) obtaining the λ-LSP$_2$ and λ-LSP$_3$ respectively. Lets consider that the optical fiber (1,2) fails. Automatically the λ-LSPs λ-LSP$_1$ and λ-LSP$_2$ also fail. Considering only the IP/MPLS layer, node 1 is isolated, and the connectivity is lost, whilst the network has still enough resources to recover the failure. For instance, instead of selecting the optical fibers 1-2-5 and 5-2-3 for setting up the λ-LSP$_2$ and λ-LSP$_3$ respectively, the optical fibers 1-4-5 and 5-6-2 should be selected. Thus, the connectivity will remain against any single fiber failure. In this paper, an on-line dynamic multi-layer routing scheme is proposed. This scheme establishes the λ-LSPs and p-LSPs whenever a new path is requested. Protection resources are reserved at either IP/MPLS or optical layer according to the current network resources, resulting in efficient resource consumption.

3 Reliable and Dynamic Multi-layer Routing

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 λ-LSPs respectively. Each router has p input and output Packet Switching Capable (PSC) ports, where $PSCi(u)$ input ports and $PCSo(u)$ output ports of node u are already not assigned to any λ-LSP. Each physical link has w wavelengths. When a p-LSP is requested, the proposed routing scheme considers both physical links and λ-LSPs, i.e. $E_P \cup E_L$. In order to univocally identify the physical link and the existing λ-LSPs 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 λ-LSP.

Each (i, j, k) λ-LSP has an associated B_{ijk} residual bandwidth; total bandwidth reserved to protect physical link $(u, v, 0)$; and T_{ijk} the total shared bandwidth allocated in link (i, j, k). Note that $T_{ijk} = \max_{(u,v,0)\in E_P} S^{uv}_{ijk}$. Each (i, j, k) λ-LSP is a sequence of physical links denoted as a set P_{ijk} and a sequence of wavelengths assigned at each physical link denoted as W_{ijk}.

The p-LSP request is defined by (s, d, r) where (s, d) is the source and destination node pair; and r, specifies the amount of bandwidth required for this request. For each setup request, a working p-LSP (WP) has to be set-up and

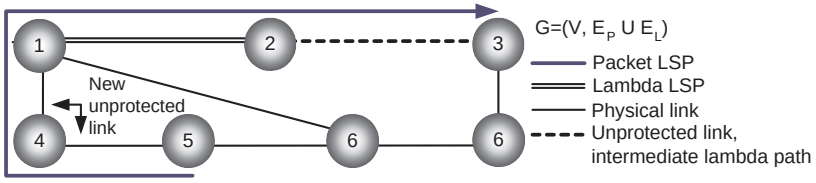

Fig. 2. Working p-LSP computation. Creation of a new λ-LSP using the physical links (5,4) and (4,1).

a backup p-LSP (BP) must be also setup, whenever the WP has, at least, one unprotected λ-LSP. If there are not enough resources in the network, for either the WP or the BP for the current request, the request is rejected.

3.2 Working Lambda and Packet LSP Computation

In our proposal, a new procedure to compute the working p-LSP (WP) is presented. In this procedure the following cost parameters are taken into account: 1) the residual bandwidth of the link candidates, B_{ijk}; 2) the maximum number of hops H; and 3) the free packet switching ports of each router, $PCSi$ and $PSCo$. Note that the residual bandwidth of the physical links with free wavelengths is the capacity of the wavelength. The proposed procedure called Dynamic Multi-Layer Working Path (DMWP) algorithm computes the min-hop working path based on a variation of the Dijkstra algorithm. In this case, the number of hops coincides with the number of λ-LSPs. Thus, the consecutive sequence of physical links, that constitutes a λ-LSP, are only considered as one hop. The DMWP procedure uses the network graph composed by the λ-LSPs and physical links, i.e., $G = (V, E_P \cup E_L)$. This procedure ends when it reaches the destination node or there is not any feasible path between source and destination nodes. If a feasible path exists then the procedure may return:

1. A sequence of existing λ-LSPs.
2. A sequence of physical links. In this case, a new λ-LSP is set up between source and destination node.
3. A sequence of lambda LSPs, physical links and intermediate lambda paths (unprotected λ-LSPs). In this case, new intermediate lambda paths are setup for each consecutive sequence of physical links as shown in Fig. 2. In the example, a new intermediate lambda path is set up with the physical links (5,4) and (4,1).

In the Dynamic Multi-Layer Working Path algorithm, $Cost(v)$ 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 $adjacency(u)$ represents the adjacency list of vertex u in graph G.

Dynamic Multi-Layer Working Path Algorithm
Input: (s, d, r): p-LSP request; $G = (V, E)$: current network graph;
H: maximum hop number.
Algorithm
For all $(v \in V)$ **do**
$Cost(v) = \infty$
$Pred(v) = null$
$WPlast(v) = 0$
$Cost(s) = 0$
$Q \leftarrow s$
while $(d \notin Q$ **and** $Q \neq \oslash)$ **do**
$u \leftarrow min\_cost(Q)$
for all $v \in adjacency(u, G)$ **do**
for all $(u, v, k) \in E$ **do**
if $(B_{ijk} \geq b)$ **and** $((k = WPlast(u) = 0)$ or $(Cost(u) + 1 < Cost(v) < H))$ **then**
if $(PSCi(v) > 0$ **and** $k = 0$ **and** $WPLast(u) > 0)$ **or**
$(PSCo(v) > 0$ **and** $k > 0$ **and** $WPlast(u) = 0)$ **or**
$(k = WPlast(u) = 0)$ **or** $(k > 0$ **and** $WPlast(u) > 0)$ **then**
$Pred(v) = u$
$WPlast(v) = k$
$Q \leftarrow v$
if not $(k = WPlast(u) = 0)$ **then**
$Cost(v) = Cost(u) + 1$

3.3 Backup Lambda and Packet LSP Computation

Once the WP is known, the backup p-LSP (BP) is computed. Three different procedures could be applied depending on the WP characteristics:

1. If the WP is a sequence of existing λ-LSPs, then each λ-LSP is already protected. In this case, the computation of the BP is not required.
2. If the WP is a new λ-LSP, and exists an available and shareable backup λ-LSP this is used to protect the WP. Otherwise, a new backup λ-LSP is set-up applying DMWP algorithm with $G = (V, E_P)$. A backup λ-LSP is shareable if the new λ-LSP does not belong to the same Shared Rink Link Group (SRLG) [7] of the both backup λ-LSP and the λ-LSPs protected by this backup λ-LSP.
3. If the WP is a combination of λ-LSPs and intermediate lambda paths, then a variation of the Partial Disjoint Path (PDP) presented in [8] 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 DMWP algorithm. The PDP may overlap with λ-LSPs of the WP, since they are already protected, and the nodes of the WP. Therefore, no extra resource is necessary in the IP/MPLS domain against failure of protected λ-LSPs in the optical layer. When the PDP overlaps the WP, more than one Segment Backup Paths

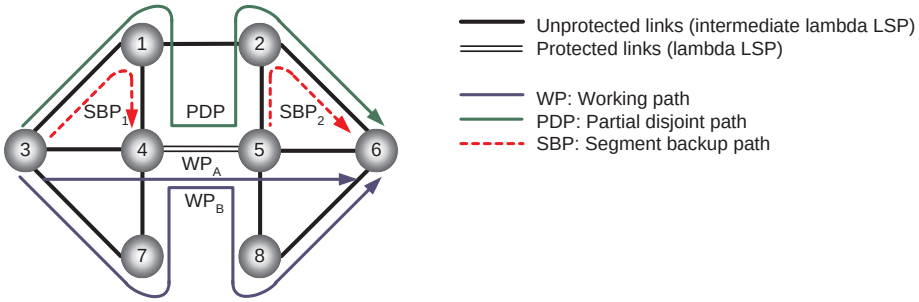

Fig. 3. Partial disjoint path computation and segment backup paths identification.

(SBP) are established. An example is shown in Fig. 3 where two WPs are sharing the protected λ-LSP 4-5. In this example, the same PDP is used to protect both the WPs. Two segment backup paths (SBP_1 and SBP_2) are established between the protected segment paths 3-4 and 5-6. Moreover, the SBP bandwidth is shared since the SBP defined at the IP/MPLS layer is not activated against the failure of the λ-LSP 4-5. For more details refer to [8]. The result of the PDP algorithm is a sequence of λ-LSPs, intermediate lambda paths and physical links. With the set of consecutive physical links new intermediate lambda paths are created. Note that in the logical topology λ-LSPs are protected at optical domain and intermediate lambda paths are protected at IP/MPLS domain.

3.4 Multi-Layer Routing with Protection against Single Fiber Failures

We propose the multi-layer routing scheme with protection against single fiber failures (PASFF). PASFF computes the WP using the DMWP algorithm and the BP according to the criteria described in Section 3.3.

In order to compare our proposal, the next two algorithms based on Oki policies [6] are implemented:

- Policy 1 with protection (P1P). The routing policy 1 first tries to allocate the p-LSPs to an existing λ-LSP. If the λ-LSP is not available then a sequence of existing λ-LSPs with two or more hops that connects the source and destination nodes are selected. In order to protect the λ-LSPs, backup λ-LSPs are set up to protect the new λ-LSPs.
- Policy 2 with protection (P2P). The routing policy 2 first tries to allocate the p-LSPs to an existing λ-LSP. If the λ-LSP is not available then a new one-hop λ-LSP is established and selected as the new p-LSP. The same procedure presented in P1P is used to compute the backup λ-LSPs. Note that protection is only applied at optical domain in both P1P and P2P.

4 Performance Evaluation

4.1 Network Topology and Traffic Request Parameters

For the simulations, the NSFNET network described in [6] was used. NSFNET network consists of 14 nodes and 21 physical links. Each physical link is bi-directional i.e., they acted like two unidirectional physical links of the same number of wavelengths. Each physical links has 8 wavelengths. The transmission speed of each wavelength was set to 10 Gbps. The number of PSC ports p was the same in each node. Requests arrived according to a Poisson distribution and exponentially distributed holding times. The required p-LSP bandwidth was set to 500Mbps. When an existing λ-LSP, intermediate lambda path or backup λ-LSP didn't accommodate any p-LSP, then it was disconnected. Ten independent trials were performed over a window of 10.000 requests. The maximum hop number H was set to 2.

4.2 Simulation Results

Figure 4a shows the performance of the proposed algorithm PASFF compared to P1P and P2P in terms of request rejection ratio. All the analyzed algorithms present a sharply decrease of the request rejection ratio as the p factor increases. However, PASFF shows around a 4% of rejected requests. PASFF performs 3 times better than P1P and 4 times than the P2P. This is because, as expected, PASFF is able to find a feasible working and backup p-LSP for most of the p-LSP requests, due to the application of protection at IP/MPLS. So, PASFF provides a better filling of the capacity. PASFF protects the intermediate lambda paths at IP/MPLS layer, whilst, the λ-LSPs are optically protected.

Next two simulated results show the percentage of the network protected at optical and IP/MPLS domain. This is evaluated using two parameters: 1) the rate of backup λ-LSPs respect to the number of logical links (lambda LSPs and lambda paths) shown in Fig. 4b and 2) the rate of spare capacity, i.e. the percentage of bandwidth used as a BP with respect to the bandwidth used as a WP shown at MPLSin Fig. 4c.

In Fig. 4b, P1P and P2P present similar behavior throughout the experiment. Note that protection is applied at optical domain for P1P and P2P algorithm. This means that mostly each λ-LSP has its own backup λ-LSP if not shareable. Therefore, the rate is close to 100% for these algorithms. On the other hand, for our proposed algorithm PASFF the number of backup λ-LSP is much more smaller as shown in Fig. 4b since some logical links are protected at IP/MPLS domain.

Finally Fig. 4c shows the percentage of BP bandwidth used at IP/MPLS domain respect to the bandwidth used as a WP. As the number of PSC, p, increases the amount of bandwidth used to recovery the traffic at IP/MPLS layer increases for PASFF. Moreover, this rate slightly decreases as well as the request rejection ratio, since more resources can be shared. On the other hand, this value is 0 for P1P and P2P since these algorithms only use protection at optical domain.

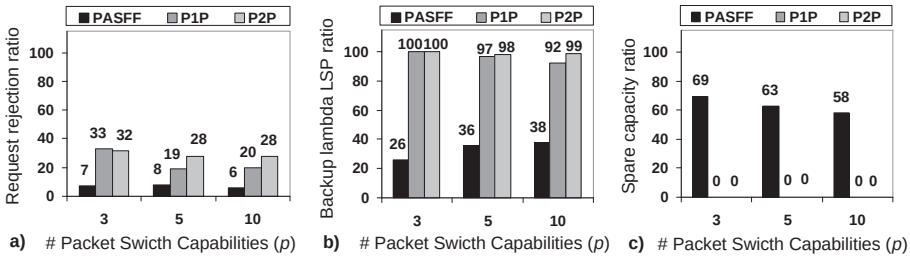

Fig. 4. a) Request rejection b) Backup lambda LSP and c) Spare capacity ratio.

5 Conclusions

In this paper a novel dynamic multi-layer routing scheme was introduced for optical IP/MPLS networks. The proposed scheme incorporated protection mechanisms in order to guarantee connectivity against any single fiber failure. As a novelty this scheme takes into account both wavelength and packet switching capabilities in order to provide protected packet LSPs cost effectively. Thus, optical protection and IP/MPLS protection mechanisms are combined. Two kinds of lambda paths were defined: the lambda LSPs that are protected at optical domain and the intermediate lambda paths that are protected at IP/MPLS domain. Shared resources and shared risk link group were also considered in the proposed scheme. Results showed the efficiency of the proposed scheme in terms of resources used to protect the network and the request rejection ratio in different multi-layer network scenarios.

References

1. J. Y. Wei: Advances in the management and control of optical Internet. Selected Areas in Communications, IEEE Journal, vol. 20, no. 4, pp. 768-785, May 2002.
2. E. Mannie: Generalized Multi-Protocol Label Switching (GMPLS) Architecture. RFC 3945, Oct. 2004.
3. W. D. Grover:Mesh-based survivable networks: Options and strategies for optical, MPLS, SONET, and ATM networking. Prentice Hall PTR, 2004.
4. K. Sato et al.: GMPLS-based photonic multi-layer router (Hichari router) architecture: An overview of traffic engineering and signling technology: IEEE Commun. Mag., vol. 40, no. 3, pp. 96-101, Mar. 2002.
5. K. Zhu, H. Zang and B. Mukherjee: A comprehensive study on next-generation optical grooming switches. Selected Areas in Communications, IEEE Journal, vol. 21, no. 7, pp. 1173-1186, Sept. 2003.
6. E. Oki et al.: Dynamic multilayer routing schemes in GMPLS-based IP+optical networks. IEEE Comm. Magazine, vol. 43, pp. 108-114, Jan. 2005.
7. P. Sebos, J. Yates, G. Hjalmtysson, A. Greenberg: Auto-discovery of Shared Risk Link Groups. In Proc. of the Optical Fiber Communication Conference and Exhibit (OFC), pp. WWD3-1-WWD3-3, March 2001.
8. A. Urra, E. Calle, J.L. Marzo: Enhanced multi-layer protection in multi-service GMPLS networks. In Proc. of IEEE Globecom, Dec. 2005.