Protection in IP-over-WDM Networks using GMPLS

N.S.C.Correia and M.C.R.Medeiros

Universidade do Algarve, Portugal

Abstract: A new protection strategy for IP-over-WDM networks is proposed. This new protection strategy maximizes the amount of protected traffic while providing fast recovery times. It assumes coordination between the IP and the WDM layer provided by the *generalized multi-protocol label switching* (GMPLS) in a peer model. The IP LSPs that are aggregated into a lightpath (high capacity LSP) are protected together, as a unity, using spare capacity of edge-disjoint lightpaths whenever necessary.

1 Introduction

The optical layer of *wavelength division multiplexing* (WDM) networks is now able to implement some network functionalities. This leads to an evolution from point-to-point WDM transmission systems towards *wavelength routed networks* (WRN). Wavelength routing techniques enable the routing of high-capacity optical signals according to their wavelengths without opto-electronic conversion or processing allowing the establishment of lightpaths between network node pairs that are geographically far apart.

In WRNs routing is done at the lightpath level. Although presenting several advantages, this strategy becomes inappropriate if traffic requests consist of subrate data streams (e.g. OC-3, OC-12, OC-48, OC-192, 100/1000 Ethernet, 1.0 Gb/s fiber channel, etc). Under this scenario, to render the network efficient and profitable, it is necessary to groom the low rate data streams onto high capacity lightpaths [1]. Traffic grooming reduces the number of wavelengths required in the network and avoids the waste of bandwidth in lightpaths that rises from the mismatch between the traffic demand and the lightpath capacity. Groomed networks have, however, some potential problems. The most serious is the network survivability. Fiber cuts or *optical cross-connects* (OXCs) failures can be catastrophic unless rapid restoration of service is an integral part of the network design and operation strategy.

Since networks are becoming more IP data centric, and it is widely accepted that transporting IP traffic directly over WDM will lead to more cost efficient networks, how to provide survivability to these networks becomes a fundamental issue. The *generalized multi-protocol label switching* (GMPLS) is the proposed signaling and control plane for IP-over-WDM networks. The WDM core network consists of GMPLS capable OXCs interconnected by optical links. On top of the WDM core network the IP network has a collection of *label switching routers* (LSRs) that can use GMPLS to set up an optical connection, called *label-switched path* (LSP), from itself to another LSR. The LSRs can perform the aggregation of lower rate LSPs [2]. Here we propose a protection scheme that assumes coordination between the IP and the WDM layer provided by GMPLS. This scheme presents fast recovery times while using resources efficiently.

2 GMPLS Network Architecture

The GMPLS architecture extended MPLS to include LSRs whose forwarding plane is not capable of processing individual IP packets. Such LSRs include devices where the forwarding decision is based on time slots, wavelengths or physical ports. In the context of WDM optical networks we consider *lambda switch capable* (LSC) interfaces, that forward data based on the wavelength on which the data is received, where an LSP is also called lightpath [2]. A lightpath from an ingress port in an OXC to an egress port in a remote OXC is established by setting up suitable cross-connects in the ingress, the egress and a set of intermediate OXCs such that a continuous physical path exists from the ingress to the egress port. IP/MPLS routers that have direct physical connectivity with the optical network are referred to as *edge routers*. Edge routers have *packet switch capable* (PSC) devices and communicate through lightpaths [3].

2.1 Interoperability Models

Two models emerged for interoperability between the IP and the optical layer: the *overlay model* and the *peer model*. In the peer model the IP and optical networks are treated together as a single integrated

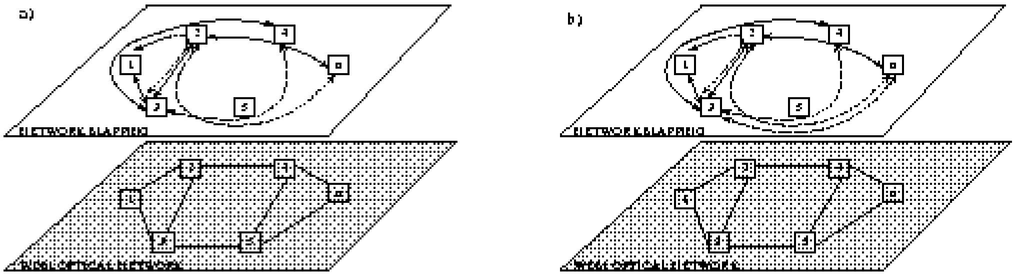

Figure 1: Network example using: a) WDM protection; b) Our protection.

network from a control plane point of view. The optical layer control information can be transferred to the IP layer, that is, an edge router can create, delete or modify lightpaths as it creates LSPs. The overlay model is architecturally more direct and simplified while the peer model needs additional communication between the IP and optical layer, although allowing better resource utilization. In the proposed protection scheme a peer model is assumed since topology information from both layers is required [4].

2.2 Forwarding Adjacency

An LSR uses GMPLS *traffic engineering* (TE) procedures to create and maintain an LSP. The LSR may then announce this LSP as a TE link into the same instance of the GMPLS control plane as the one that was used to create the LSP. In a peer model this is used to realize LSP hierarchy. Such link is called a *forwarding adjacency* (FA). We refer to this LSP as *forwarding adjacency LSP* (FA-LSP). An FA is therefore a TE link between two GMPLS nodes whose path crosses zero or more GMPLS nodes in the same instance of the GMPLS control plane [5]. For details on FAs see [5].

Using this mechanism, a lightpath between two edge-routers can be advertised as a forwarding adjacency (a virtual link) in a link state protocol. A node, when performing route computation, is then able to use conventional and virtual links since they appear in the IS-IS/OSPF routing database [3]. This enables our protection scheme to use the bandwidth available on working lightpaths for backup purposes.

3 Suggested Protection for IP-over-WDM Networks

WDM protection and IP restoration are two fault management schemes that have been discussed for IP-over-WDM network. In the first, protection is performed at the physical level, where lightpaths are re-mapped to new physical links after a failure making it invisible to upper layers. The second involves rerouting of disrupted traffic around failure. In these schemes the two layers are not aware of each other.

With GMPLS, network state information from both layers can be integrated. In this context, the *integrated protection* scheme has been discussed in [6]. In this scheme, for each IP LSP request, bandwidth is both reserved in a primary (working) and in a backup path (these are placed on lightpaths in a way that they use disjoint sets of links). In [6] results show that this scheme can accommodate more requests than WDM protection. The advantage of WDM protection is that it provides aggregate protection to all IP LSPs in a lightpath, having fast recovery times, while integrated protection protects individual IP LSP. Both WDM and integrated protection can use dedicated and shared resources. In GMPLS the SRLGs are used for resource sharing between backup paths that have link-disjoint working lightpaths [3, 2].

The scheme we suggest uses, if necessary, spare bandwidth of working lightpaths to provide end-to-end-protection to other lightpaths. This is illustrate in figure 1 where working lightpaths are represented by solid lines and backup lightpaths by dashed lines. Considering that just two wavelengths are available at each link, only the lightpaths between the node pairs (3,4), (2,6) and (1,3) were protected using WDM shared protection. The lightpath (2,3) could not be protected. The protection lightpaths of working lightpaths (1,3) and (2,6) can share the physical link (2,3) because they are link-disjoint. For the same scenario, using our scheme, the traffic of lightpath (2,3) was protected using lightpath (2,6) since there is enough spare bandwidth available. For that to be possible the backup lightpath (6,3) must be activated when lightpath (2,3) fails. Wavelength sharing can be used by backup lightpaths in physical link (3,5) since the corresponding working lightpaths are link-disjoint. This scheme is feasible because we assume the use of GMPLS and, as explained earlier, working lightpaths can be announced as virtual links to the network. Lightpath (2,6) can be used to protect lightpath (2,3) because they are link-disjoint.

4 Maximum Throughput Problem Formulation

The network consists of physical edges connecting nodes with *wavelength division multiplexers* (WDMs) and *wavelength cross connects* (WXCs) with conversion functionality. A physical edge includes two links (optical fibers) for transmission in both directions and an edge failure affects both links in it. Thus, working and backup routes must be edge-disjoint. The edge IP routers must establish IP LSP connection requests, each with a bandwidth requirement (OC-3,OC-12,OC-48 or OC-192, where OC-$n \approx n * 51.84$ Mb/s [1]) and end-to-end protection. The notation for connection requests follows [1]. The inputs are:

$\mathcal{G}(\mathcal{N},\mathcal{L})$	all-optical WDM physical network, where $\mathcal{N}$ is the set of nodes and $\mathcal{L}$ is the set of links.
$\mathcal{Z}$	set of lightpaths, already mapped, that can become part of the virtual topology. The source and destination nodes of a lightpath $z \in \mathcal{Z}$ is given by $s(z)$ and $d(z)$ respectively.
δ^z_{ij}	one if the lightpath $z \in \mathcal{Z}$ uses the link $ij \in \mathcal{L}$; zero otherwise.
$\mathcal{F}$	set of physical edges, possible faults, where the physical edge $f \in \mathcal{F}$ connecting nodes i and j includes both links ij and $ji \in \mathcal{L}$.
$\mathcal{P}_f$	set of primary lightpaths in $\mathcal{Z}$ affected by fault $f \in \mathcal{F}$.
$\mathcal{Y}$	set of granularities of connection requests: $\mathcal{Y} = \{3, 12, 48, 192\}$.
Λ	traffic matrix set: $\Lambda = \{\lambda_y\}$ where $y \in \mathcal{Y}$. The number of OC-y connection requests (LSPs) from the source node s to the destination node d is given by $\Lambda^{s,d}_y$.
W	number of wavelength channels available on each link.
C	bandwidth of a lightpath; assumed to be equal to OC-192.

Variables:

σ^z	one if lightpath $z \in \mathcal{Z}$ belongs to the virtual topology; zero otherwise.
$\phi^{s,d}_{y,t}$	one if the t^{th} OC-y LSP request from s to d has been established; zero otherwise.
$\beta^{s,d,t}_{z,y}$	one if the t^{th} OC-y LSP request from s to d uses $z \in \mathcal{Z}$ in its primary route; zero otherwise.
$\alpha^{s,d,t}_{z,f,y}$	one if the t^{th} OC-y LSP request from s to d will have bandwidth reserved for backup in lightpath $z \in \mathcal{Z}$ when fault $f \in \mathcal{F}$ occurs; zero otherwise.
$\nu^z_{z'}$	one if the backup route of lightpath $z \in \mathcal{Z}$ uses lightpath $z' \in \mathcal{Z}$; zero otherwise.
θ^z_{ij}	one if the backup route of lightpath $z \in \mathcal{Z}$ includes physical link $ij \in \mathcal{L}$; zero otherwise.

The maximization of total network throughput is achieved by the following objective function:

$$Maximize \sum_{s,d \in \mathcal{N}} \sum_{y \in \mathcal{Y}, t \in [1, \Lambda^{s,d}_y]} y * \phi^{s,d}_{y,t} \tag{1}$$

The constraints are:

- Routing of IP LSPs primary routes:

$$\sum_{z \in \mathcal{Z} : s(z)=i} \beta^{s,d,t}_{z,y} - \sum_{z \in \mathcal{Z} : d(z)=i} \beta^{s,d,t}_{z,y} = \left\{ \begin{array}{rl} \phi^{s,d}_{y,t}, & if\ s = i \\ -\phi^{s,d}_{y,t}, & if\ d = i \\ 0, & otherwise \end{array} \right. , \forall s, d, i \in \mathcal{N}, \forall y \in \mathcal{Y}, \forall t \in [1, \Lambda^{s,d}_y] \tag{2}$$

- Backup routes of virtual topology lightpaths:

$$\sum_{j : ij \in \mathcal{L}} \theta^z_{ij} + \sum_{z' \in \mathcal{Z} : s(z')=i} \nu^z_{z'} - \sum_{j : ji \in \mathcal{L}} \theta^z_{ji} - \sum_{z' \in \mathcal{Z} : d(z')=i} \nu^z_{z'} = \left\{ \begin{array}{rl} \sigma^z, & if\ s(z) = i \\ -\sigma^z, & if\ d(z) = i \\ 0, & otherwise \end{array} \right. , \forall z \in \mathcal{Z}, \forall i \in \mathcal{N} \tag{3}$$

$$\sigma^z * \delta^z_{ij} + \theta^z_{ij} + \theta^z_{ji} \leq \sigma^z, \forall z \in \mathcal{Z}, \forall ij, ji \in \mathcal{L} \tag{4}$$

$$\sigma^z * \delta^z_{ij} + \nu^z_{z'} (\delta^{z'}_{ij} + \delta^{z'}_{ji}) \leq \sigma^z, \forall z, z' \in \mathcal{Z}, \forall ij, ji \in \mathcal{L} \tag{5}$$

- Limitation of wavelengths used and bandwidth available on lightpaths:

$$\sum_{s,d \in \mathcal{N}} \sum_{y \in \mathcal{Y}, t \in [1, \Lambda^{s,d}_y]} (y * \beta^{s,d,t}_{z,y} + y * \alpha^{s,d,t}_{z,f,y}) \leq C * \sigma^z, \forall z \in \mathcal{Z}, \forall f \in \mathcal{F} \tag{6}$$

$$\alpha^{s,d,t}_{z,f,y} \geq \beta^{s,d,t}_{z',y} + \nu^{z'}_z - 1 \quad , \quad \forall z \in \mathcal{Z}, \forall f \in \mathcal{F}, \forall z' \in \mathcal{P}_f, \forall s, d \in \mathcal{N}, \forall y \in \mathcal{Y}, \forall t \in [1, \Lambda^{s,d}_y] \tag{7}$$

$$\sum_{z \in \mathcal{Z}} \sigma^z * \delta^z_{ij} + \sum_{z \in \mathcal{P}_f} \theta^z_{ij} \leq W \quad , \quad \forall ij \in \mathcal{L}, \forall f \in \mathcal{F} \tag{8}$$

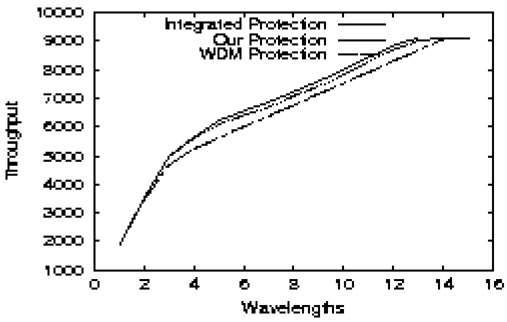

Figure 2: Throughput vs wavelengths.

Constraint 2 guarantees flow conservation of IP LSPs primary routes. Constraint 3 guarantees flow conservation of backup lightpaths (both basic TE links and FAs can be used). Constraint 4 ensures that the edges used by the backup are different from the ones used by the lightpath being protected and constraint 5 ensures that the edges used by FAs are different from the ones used by the lightpath being protected. Constraint 6 limits the bandwidth of lightpaths. Constraint 7 forces bandwidth reservation for backup in lightpath $z \in \mathcal{Z}$, due to fault $f \in \mathcal{F}$, if the primary route of the IP LSP has been affected by fault $f \in \mathcal{F}$ and the backup route of the lightpath used by the primary route of the IP LSP uses lightpath $z \in \mathcal{Z}$. Constraint 8 limits the number of wavelengths used in each physical link considering sharing the wavelengths between lightpaths with edge-disjoint primary routes. This problem is NP-complete.

5 Results

The following results were obtained, using CPLEX 8.0, for the network in figure 1. The traffic matrices used for OC-3, OC-12, OC-48 and OC-192 connection requests were randomly generated using different uniform distributions as in [1]. Uniformly distributed random numbers between 0 and 16 were generated for OC-3, between 0 and 8 for OC-12, between 0 and 4 for OC-48, and between 0 and 2 for OC-192. The set of lightpaths $\mathcal{Z}$ include one lightpath for each node pair using the shortest path.

Figure 2 shows the throughput of the protection schemes. The integrated protection presents the best throughput and accommodates all IP LSPs using 13 wavelengths. Our protection scheme has a throughput close to the integrated and accommodates all IP LSP with 14 wavelengths. The WDM protection requires 15 wavelengths to accomodate all IP LSPs. Thus, our scheme uses capacity in a more efficient way than WDM protection while presenting fast recovery times, as WDM protection, since it protects IP LSPs in an aggregated way.

6 Summary

We present a protection scheme for IP-over-WDM networks using GMPLS. The performance of this scheme was analyzed and results show that while using resources efficiently, since spare bandwidth on working lightpaths can be used, it provides fast recovery times because aggregated protection is provided.

Acknowledgment: This work was supported by FCT from Portugal (DOPNET-POSI/CPS/42073).

References

[1] Keyao Zhu and Biswanath Mukherjee: Traffic Grooming in an Optical WDM Mesh Network. IEEE JSAC, Vol. 20, No. 1 (Jan 2002).

[2] Eric Mannie et al.: Generalized Multi-Protocol Label Switching (GMPLS) Architecture. Internet Draft, draft-ietf-ccamp-gmpls-architecture-02.txt (2002).

[3] Bala Rajagopalan, James Luciani and Daniel Awduche: IP over Optical Networks: A Framework. Internet Draft, draft-ietf-ipo-framework-03.txt (2003).

[4] Krishna Bala: Internetworking between the IP and the Optical Layer. Opt. Net. Mag. (May 2001).

[5] Kireeti Kompella and Yakov Rekhter: LSP Hierarchy with Generalized MPLS TE. Internet Draft, draft-ietf-mpls-lsp-hierarchy-08.txt (2002).

[6] Yinghua Ye, Chadi Assi, Sudhir Dixit and Mohamed A. Ali: A Simple Dynamic Integrated Provisioning/Protection Scheme in IP over WDM Networks. IEEE Com. Magazine (Nov 2001).