

IP Restoration versus WDM Protection: Is There an Optimal Choice?

Andrea Fumagalli and Luca Valcarenghi *

Center for Advanced Telecommunications Systems and Services (CATSS)

Erik Jonsson School of Engineering and Computer Science

The University of Texas at Dallas

P.O. Box 830688

RICHARDSON, TX 75083-0688, USA

E-mail: {andrea, lucav}@utdallas.edu

October 10, 2000

Abstract

The exponentially growing number of Internet users armed with emerging multi-media Internet applications is continuously thirsty for more network capacity. Wavelength Division Multiplexing (WDM) networks that directly support the Internet Protocol (IP) — the so called IP over WDM architecture — have the appropriate characteristics to quench this bandwidth thirst. As every day life is increasingly reliant on telecommunication services, users are becoming more and more demanding, and connection reliability is currently as critical as high capacity. Both IP and WDM layers can fulfill this need by providing various resilient schemes to protect the user's traffic from disruptions due to network faults.

This paper first reviews the most common restoration and protection schemes available at the IP and WDM layers. These schemes may be concurrently present in the IP over WDM architecture, with the resilient mechanism of each connection being specifically chosen as a function of the overall cost, application requirements, and management complexity. The second part of the paper describes a versatile heuristic based on Simulated Annealing that may be adopted to optimize the concurrent use of IP restoration and WDM protection schemes in the same (mesh) network. The proposed heuristic allows to vary the percentage of traffic protected by the WDM layer and the percentage of traffic relying on IP restoration taking into account topology constraints and network cost minimization. An additional feature of the proposed heuristic is the potential to trade the solution optimality for computational time, thus yielding fast solutions in support of interactive design.

*This work was partially supported by Alcatel CRC of Richardson (TX) and the TxTEC Consortium.

1 Introduction

The skyrocketing growth of data-centric traffic is rapidly depleting today's Internet resources. Internet Service Providers anticipate that Internet traffic will grow between 50 and 300% per year. The aggregate bandwidth required in the backbone networks will shortly surpass hundreds of Terabits per second. In this scenario *optical networks* will play a key role in providing novel, high-capacity, and cost-effective transport networks that are compatible with existing transport and switching solutions, e.g., Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET), Asynchronous Transfer Mode (ATM), and Internet Protocol (IP).

In the Optical Layer (OL)¹, Wavelength Division Multiplexing (WDM) yields a cost-effective way to harness the fiber bandwidth by providing several parallel channels or *lightpaths*, each operating at a transmission rate compatible with current electronic rates². A lightpath is an end-to-end path of light that may be established between a node pair (e.g., IP routers) that may not be physically adjacent, i.e., not connected by a single fiber hop, thus increasing the logical network connectivity. To be of practical use, however, the advantages of high speed, high network connectivity, and optical transparency³ offered by a WDM network must be accompanied by adequate network survivability features.

In general, a network is referred to as *survivable* if it provides some ability to recover ongoing connections disrupted by the catastrophic failure of a network component, such as a line interruption or a node failure. The design of survivable networks is obtained by exploiting *restoration* and/or *protection* schemes. Upon occurrence of network failure, a restoration scheme dynamically looks for backup paths of spare capacity in the network. A protection scheme reserves, in advance, dedicated backup paths and wavelengths in the network. The former scheme is commonly available at higher layers, e.g., the IP layer. The latter scheme is commonly used in the transport layer, e.g., the WDM layer.

This paper addresses the issue of survivability in IP over WDM networks. The paper is organized in two parts.

The first part presents a survey of available restoration and protection schemes that may be used in networks with arbitrary (mesh) topology⁴. The advantages of the presented resilient schemes are discussed, leading to the conclusion that, very likely, IP over WDM networks will require multiple, co-existing resilient schemes in the same network.

The second part of the paper illustrates a heuristic approach that constitutes a framework for achieving a combined optimization of the IP restoration and the WDM protection schemes concurrently present in the same mesh networks. The heuristic is designed to optimally solve what we call the IP aware Wavelength minimum Mileage (IWM) problem. The IWM problem consists of minimizing the overall network cost, i.e., the wavelength mileage for both working and spare lightpaths in the OL plus the *resilience cost* of the IP

¹The Optical Layer is defined by International Telecommunication Union (ITU-T).

²Dense Wavelength Division Multiplexed (DWDM) systems with transmission capacity of 1.6 Tb/s (160 channels at 10Gb/s each) on a single fiber have been recently announced.

³Transparency is the capability of supporting multiple transmission rates and modulation formats.

⁴Arbitrary mesh topologies are expected to be the customary fabric of backbone and metro networks due to their high connectivity and design flexibility.

layer. The latter cost may be associated with either a performance related quantity — an equivalent cost representing the Quality of Service (QoS) degradation due to IP rerouting — or an abstract parameter representing the willingness of the designer to provide more or less reliability in either network layer. In the example discussed in the paper, the IWM problem is solved by assuming that the traffic routed on any line of the mesh can be made resilient to faults by either using an IP restoration scheme or a WDM protection scheme. For each line, the proposed heuristic chooses the resilient scheme that overall yields the minimum network cost. The heuristic is based on the combined use of i) a Simulated Annealing (SA) algorithm designed to select which lines of the mesh are protected at the optical layer (the others require IP restoration), and ii) a shortest path algorithm applied to route the lightpath demands on an auxiliary graph, that is derived from the mesh and takes into account the cost of both restoration and protection schemes.

Among other advantages, the SA algorithm allows us to exploit the trade-off between solution optimality and computational speed. The optimization framework is thus suitable for the interactive design of survivable IP over WDM mesh networks. In addition, due to SA versatility, the cost function under optimization can be easily modified by the designer to take into account various protection schemes. For the sake of demonstration, two protection schemes are considered in the paper, namely, the Dedicated-Path-switched WDM Self-Healing Ring (DP-WSHR) and the Shared-Line-switched WDM Self-Healing Ring (SL-WSHR), showing that in either case cost effective solutions are found with the proposed heuristic. By means of the auxiliary graph, it is possible to optimally deal with design constraints that may arise due to network layout, management complexity and/or technology limitations. Indeed, the percentage of traffic and network lines that are protected in either layer may be arbitrarily chosen by the designer, thus providing a flexible approach that can address a variety of distinct design scenarios.

2 Resilient Schemes at IP and WDM Layers

In the two-layer IP over WDM architecture, each layer can provide its own independent resilient scheme. Restoration/protection schemes may be implemented at the IP layer (possibly using the Multi-Protocol Label Switching (MPLS) sub-layer) and at the Optical (WDM) Layer (OL).

While the resilience concept is naturally embedded in the IP layer, in which the actual path used to route a packet from source to destination is dynamically found and maintained by the routers, protection techniques at the optical layer are just emerging, driven by the need for coarse and fast protection schemes. One can notice the increasing importance of WDM layer resilient schemes by the number of works recently published on this topic [1, 2, 3, 4, 5, 6, 7].

In this section we review the most common restoration and protection schemes, discussing their advantages and disadvantages.

2.1 IP Layer Restoration Schemes

In general, resilient schemes available at the network layer, such as IP (IP/MPLS), have the capability to recover multiple faults and operate at small traffic granularity⁵. However, these schemes are generally slow as they require on-line processing upon failure occurrence.

Dynamic routing and MPLS protection switching [8] are schemes currently considered to achieve network survivability at the IP (IP/MPLS) layer. These schemes are discussed in the next sections.

2.1.1 IP Dynamic Routing

With dynamic routing, reachable active routers are found dynamically, thus adapting the IP routing to possible network faults. This task is accomplished by exchanging, between adjacent routers, control messages that are used to update the routers' routing tables, thus enabling IP packets to be dynamically rerouted around link and node failures. This protocol guarantees network-wide survivability, independent of the underlying physical network.

The faults in the network can be detected by the routers either explicitly or implicitly [9]. Explicitly, faults are detected at the local level and signalled to the neighboring routers through regular exchange of routing protocol control messages, such as Internet Control Message Protocol (ICMP). Otherwise, the expiration of timers on background messaging, such as KEEPALIVE and HELLO messages, implicitly signals the presence of faults. Once a router detects a line fault, it recalculates the affected routes and updates its routing tables. Then it propagates the occurred changes to its neighboring routers using "UPDATE" messages such as Open Shortest Path First (OSPF) link state advertisement (LSA) or Border Gateway Protocol-4 (BGP-4). The dynamic routing protocol efficiently uses spare network resources and is flexible to topological changes. However, it is usually slow, from tens of seconds to minutes, and its behavior is unpredictable.

Some enhancements of the protocol have been proposed [10] to overcome the former drawbacks.

One approach is the so called Equal Cost Multipath Forwarding (ECMF) in which the router relies on more than one path for transmitting packets sharing a common destination. This solution is already implemented in some routing protocols, such as OSPF and Intermediate System-Intermediate System (IS-IS), by maintaining multiple next-hop entries for the same destination within each router's routing table. This way, in case of failure, a fraction of packets are guaranteed to flow to the destination until the router routing table is updated with the recalculated routes.

A second approach partitions the network into multiple areas, as defined in hierarchical link-state routing protocols such as OSPF and IS-IS. This way routing updates are confined to the affected area, minimizing the network reconfiguration convergence time.

Another proposed approach decreases the failure detection time by either reducing the HELLO time-out, so that HELLO messages are sent more frequently, or by rapid

⁵Granularity is determined by the protocol traffic unit at that particular layer.

rate pinging through ICMP ECHO requests [11]. In either case, this approach increases control traffic overhead.

2.1.2 MPLS Protection Switching

MPLS protection switching is an alternative approach to circumvent the latency drawback of dynamic routing. MPLS protection switching is enabled through a hierarchy of paths called Labeled Switched Paths (LSP's) that are obtained by prepending a stack of labels or tags to packet headers. The protection entities can be setup either dynamically or in a pre-negotiated way.

Protection entities, dynamically set up, restore traffic based upon failure information, bandwidth allocation and optimized reroute assignment. LSP's crossing a failed line or Label Switched Router (LSR) are disrupted at the point of failure and must be reestablished using reservation signaling.

Pre-negotiated protection consists of working LSP's that have pre-established protection paths. The pre-established protection path is node and link disjoint from the working path. The network resources of the protection path can be either reserved beforehand (unused unless failure occurs), or dynamically allocated to low priority traffic that is allowed to use them in absence of network failure. Preemption of low priority traffic may be necessary upon network failure.

Both MPLS protection switching techniques, dynamic and pre-negotiated, can be performed on a line basis (by rerouting portion of the LSP around the failed line, named *link rerouting*) or on a path basis (by rerouting the entire LSP, named *edge-to-edge rerouting*). In general, dynamic protection increases resource utilization but requires longer restoration times than pre-established protection. Link rerouting is faster than edge-to-edge rerouting because, in the latter case, the failure notification must reach the head-ends of all the LSP's affected by the failure. Link rerouting may be completed in about 50 ms but is not well suited for handling node failure.

2.2 WDM Layer Resilient Schemes

Both Optical Channel (OCh) Section and Optical Multiplex Section (OMS) — OL sub-layers — feature *dynamic restoration* and *pre-planned protection*. Like in the higher layers, restoration schemes are more efficient from a capacity viewpoint but relatively slow (common restoration completion time is on the order of seconds or minutes). Protection schemes guarantee service restoration completion times of hundreds, tens, and even fractions of milliseconds.

The main difference between OCh and OMS resilient schemes is represented by the granularity at which the layers operate. OCh resilient schemes protect individual lightpaths, thus allowing selective recovery of Optical Line Terminal (OLT) failures. OMS resilient schemes work at the aggregate signal level, thus recovering all lightpaths present on the failed line concurrently [12]. OCh resilient schemes require more spare devices, e.g., transponders, multiplexers, demultiplexers, than their OMS counterparts because

each working lightpath must be demultiplexed and multiplexed at every node in order to be individually switched [12].

In this section we provide a brief survey of the most common OL restoration and protection schemes summarized in Figure 1. For further details the interested reader is referred to [3, 12].

The following terminology is used in the paper. A *working lightpath* is the default path of light established between a source-destination pair absent a network failure. A *protection wavelength* is a spare channel that may be used in case of network failure. A concatenation of protection wavelengths along a path forms a *protection lightpath*.

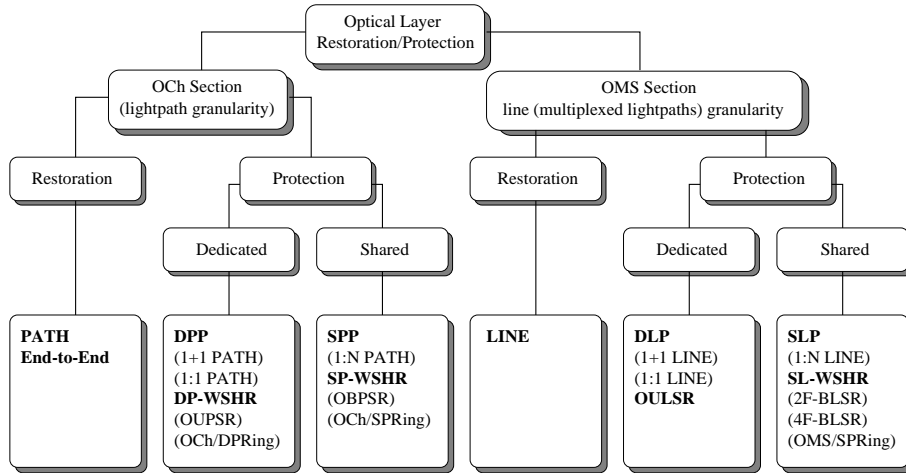


Figure 1: Classification of Optical Layer (WDM) resilience schemes. Acronyms in parenthesis are equivalent terms for a particular resilience scheme.

2.2.1 Optical Layer Restoration

The OCh path restoration scheme requires that, upon network failure, every affected working lightpath is replaced by a protection lightpath. The protection lightpath is computed using either a centralized [12] or a distributed [3, 13] approach. With the former approach a control node keeps record of the network status, computes the protection lightpaths, and passes the information onto the network nodes. With the latter approach, source and destination nodes dynamically search for the protection wavelengths required to re-establish the disrupted lightpaths.

The OMS line restoration scheme requires that an alternative route be found to locally divert all affected working lightpaths around the faulty line. This scheme is triggered by the failed line end-nodes that make use of a distributed algorithm to dynamically discover the alternative route.

2.2.2 Optical Layer Protection

OCh and OMS protection schemes are also called, respectively, *path protection* and *line protection*. In both schemes, protection (or spare) resources can be either *dedicated*, in which case the spare resource is dedicated to a single working lightpath, or *shared*, in which case the same spare resource may be used to provide protection to multiple working lightpaths. OCh and OMS protection schemes are available in *mesh* and *ring* network topologies.

Dedicated protection is commonly referred to as 1 + 1 and 1 : 1 protection. With the 1+1 protection the source node transmits on both working and protection lightpaths simultaneously. The destination keeps monitoring both lightpaths, dynamically choosing the signal with the best performance, e.g., signal to noise ratio. Therefore, if a degradation of the signal is detected on the working lightpath, the destination immediately switches over the protection lightpath. With the 1:1 protection, transmission occurs on the working lightpath only, while the protection lightpath may be used to transmit low priority traffic. Upon failure of the working lightpath, both source and destination switch over the protection lightpath, preempting the low priority traffic.

Shared protection, also referred to as 1 : N , allows spare wavelengths to be shared by a number of working lightpaths. In case of a fault, each disrupted transmission is switched over the protection wavelengths. This operation requires some signaling to notify the network nodes of the new transmission paths and to make sure that the protection wavelengths on the various fibers are correctly interconnected to form the required protection lightpaths. Once the spare resource is used to protect a working lightpath, it will not be available to protect the other working lightpaths until the original working lightpath is re-established.

Specific protection schemes based on these concepts are described below.

Dedicated-Path Protection (DPP), depicted in Figure 2(a), is typically applied to mesh networks. DPP can be fast (1+1 DPP just requires that the receiving node switches to the protection lightpath) and robust in the face of multiple faults (they must not occur contemporarily in lines belonging to the working and protection lightpath of the same connection). It requires a low degree of management complexity, but does not efficiently use protection resources.

Dedicated-Line Protection (DLP) reserves protection wavelengths between the end-nodes of each line utilized by working lightpaths. Similar to OCh DPP, DLP may require more spare capacity allocation than other schemes but can be even faster than DPP. Indeed, in the case of 1:1 protection, the restoration completion time is faster than 1:1 DPP because signalling is confined within the area around the faulty line.

Dedicated-Path-switched WSHR⁶ (DP-WSHR) (also called Optical Unidirectional Path Switched Ring (OUPSR) or OCh dedicated protection ring (OCh/DPRing)) is the DPP equivalent for ring networks (see Figure 3(a)). DP-WSHR restoration scheme is fast (on the order of ms or fraction of ms) but the total protection wavelength mileage is equal to or larger than the amount required in the other OCh and OMS ring protection

⁶WSHR stands for WDM Self-Healing Ring.

schemes.

Optical Unidirectional Line Switched Ring (OULSR) scheme is similar to DP-WSHR. It utilizes two counter-rotating fibers one for working lightpaths and the other for protection lightpaths. The difference is that, in the OULSR case, all the lightpaths passing through the failed line are jointly switched over the protection fiber. With respect to DP-WSHR, this scheme requires the same wavelength mileage but, due to its line switching, as opposed to DP-WSHR wavelength switching, it employs less expensive devices while achieving similar restoration completion times.

In **Shared-Path Protection (SPP)** (also termed 1:N Path Protection), protection wavelengths are shared by a number of line and node-disjoint working lightpaths, (see Figure 2(b)). Compared to DPP, SPP achieves more efficient utilization of spare resources at the price of a more complex control (signaling is required between source and destination nodes) and longer restoration completion time (order of 100 ms). In addition, if two or more faulty connections share the same protection wavelengths only one can be recovered.

Shared-Line Protection (SLP) (also termed 1:N Line Protection) applies the SPP technique, locally, to the faulty line. In this case, it is possible to make use of shared protection resources among different failure scenarios, thus yielding a better resource utilization than the one achieved in DLP. The restoration completion time is generally faster than the one of SPP because of locally limited signaling.

Shared-Path WSHR (SP-WSHR) (also termed Optical Bidirectional Path Switched Ring (OBPSR) or OCh shared protection ring (OCh/SPRing)) represents the SPP equivalent in ring networks. This scheme's peculiarity is the *non loop-back* switching, depicted in Figure 3(b). In SP-WSHR, in case of failure, each working lightpath is switched to the protection lightpaths at its source node. Therefore, the recovered traffic reaches the destination node only along the protection lightpath. The SP-WSHR is the most efficient among the WSHR protection techniques in terms of spare resource utilization but it requires complex control and signaling. Restoration time may also be affected for the same reason.

Bidirectional **Shared Line-switched WSHR (SL-WSHR)** are physically implemented with either 2 fibers (Optical 2-Fiber/BLSR (O-2F/BLSR)) or 4 fibers (Optical 4-Fibers/BLSR (O-4F/BLSR)). In either case, working lightpaths and protection wavelengths may be carried using both directions of propagation. Its peculiarity is the *loop-back* switching, depicted in Figure 3(c). Upon failure, the working lightpaths are switched, at one failure end, to the protection wavelengths of the counter rotating fiber. When they reach the other failure end they are looped-back along their original working wavelengths to reach their destination nodes. For each direction of propagation the number of protection wavelengths is determined by the largest number of working lightpaths in any line flowing with opposite direction (defined as the ring *load*). The SL-WSHR scheme is simple and fast (completion switching time in the order of tens of ms) because the switching mechanism is promptly activated upon fault detection without requiring any further signaling.

3 Coordination between IP and WDM Layers

Coordination between resilient schemes, possibly at distinct layers, is required to avoid multiple schemes concurrently activated upon a single network fault. This coordination is commonly achieved by resorting to *escalation strategies* that sequentially activate the different resilient schemes starting from either the lowest or the highest network layer. Escalation strategies are governed by either explicit messaging between the different layers or arbitrarily setting failure detection and restoration completion times.

Scheme	Detection time	Restoration completion time
IP Dynamic Routing	100 ms-180 s	1-100 s
MPLS fast (link) rerouting	0.1-100 ms	50 ms-100 ms
MPLS edge-to-edge rerouting	100 ms-180 s	1-100 s
OCh and OMS Restoration	> 100ms	\geq 50 ms
DP-WSHR, DL-WSHR, DPP	1-10 ms	10 μ s-10 ms
SP-WSHR, SL-WSHR, SPP	1-10 ms	1-30 ms

Table 1: Service restoration times of IP and WDM resilience techniques [11, 10, 3].

Table 1 summarizes some of the fault detection and restoration completion times at the IP/MPLS and WDM layers. It must be noted that MPLS resilient schemes are not yet mature and not supported by experimental data. Similarly, OCh/OMS restoration schemes are not yet standardized. On the contrary IP dynamic routing and OCh/OMS protection techniques are already either used in commercial networks or tested in field trials. Their characteristics are thus well known.

It is worth commenting on the emerging and promising MPLS schemes. Fault detection in MPLS can be achieved by exploiting different existing techniques, such as SONET/SDH-based framing alarms, OL fault detection techniques, and IP-based KEEPALIVE, HELLO, and ICMP messages, that guarantee detection times ranging from few tenths of milliseconds to hundred of seconds. MPLS may resort to control plane signaling, such as Constraint-based Routing Label Distribution Protocol (CR-LDP) or modified Resource Reservation Protocol (RSVP), to perform traffic restoration with time intervals ranging from few dozens of milliseconds to hundred of seconds.

In the rest of the paper we focus on well-established IP and WDM resilient schemes — IP dynamic routing and OCh/OMS WSHR protection — and we illustrate a framework for jointly designing the resilient schemes at both layers.

4 Survivable IP over WDM Mesh Networks Based on WSHR

Mesh topologies offer high connectivity that greatly improves network reliability and load balancing for congestion control in the Internet. The connectivity degree can be

further increased by means of lightpaths established at the optical layer. Although current IP/MPLS reliability schemes offer varying levels of restoration/protection granularity, they cannot provide all the necessary functionality needed by the next generation Internet, i.e., fast restoration. It is thus expected that both IP and WDM layers will each provide some degree of survivability against network faults.

An example of optical mesh is represented by the Pan-European backbone network, shown in Figure 4(a). Nodes are equipped with Optical Cross-Connects (OXC's) consisting of opto-mechanical switches and with wavelength conversion capabilities. OXC's provide the routing capabilities for establishing the lightpaths throughout the network while the opto-mechanical switches provide the survivability functions at the OMS sub-layer. Nodes are connected by bidirectional optical fiber lines, with the number of wavelengths in each direction determined by the traffic demands and the protection scheme being used.

For demonstration purposes, the optical protection schemes considered in the rest of the paper are WSHR based. A WSHR protection scheme can be adopted in a mesh network by overlaying a set of rings on the physical mesh topology. The set of rings, also called the ring cover, is then used to design multiple WSHR's that protect the traffic routed on the covered lines. We term this approach, illustrated in Figure 2(c), the Multi-WSHR scheme.

A complete covering of the mesh is possible when the topology is 2-connected⁷, as this property ensures that every node in the mesh can be connected to at least one ring. When using a Multi-WSHR scheme, the protection scheme of a single WSHR is applied to each individual ring that covers the mesh, with the following additional constraints:

- every working lightpath carried on a line covered (protected) by two or more rings must be protected by only one ring
- rings can share fibers but cannot share protection wavelengths.

An important feature of the Multi-WSHR scheme is the fact that each ring is managed independently from the others. Upon a fault, the required signaling and control is thus confined within the faulty ring. The Multi-WSHR scheme is resilient to multiple faults occurring on lines covered by distinct rings. Furthermore, as working lightpaths can span over multiple rings, only the nodes in which working lightpaths are switched from one protection ring to another require OXC capabilities. The remaining nodes need only optical add/drop multiplexing capabilities.

4.1 IP Aware Wavelength Minimum Mileage (IWM) Problem and Solution

The availability of two resilient schemes in the same network — IP dynamic routing and WSHR protection — poses the question of which scheme must be used to protect which traffic. The option of using both resilient schemes for all traffic may not be the most cost effective one. A more careful design may consist of a hybrid solution in which only part

⁷A graph is *2-connected* if it cannot be disconnected by removing less than 2 edges from the graph.

of the traffic is protected by the WSHR scheme, while the remaining part relies only on the IP restoration scheme.

An efficient heuristic is described to determine how both resilient schemes may be optimally combined to provide a cost effective survivable network. The problem solved by the heuristic is called IP aware Wavelength minimum Mileage (IWM) problem. In the IWM problem the total wavelength mileage in the WDM layer is minimized jointly with an arbitrarily defined IP layer cost. The cost of the IP layer may be defined to take into account various factors, including performance degradation determined by the IP restoration scheme, e.g., traffic disruption and congestion originating from the interaction of rerouted traffic with regular traffic.

More in detail, the WDM layer cost is defined as the total wavelength mileage, i.e., miles of working and protection wavelengths in the WSHR's, required in the network to support the given set of traffic demands. The IP layer cost is defined as the sum of the wavelength mileage of the traffic streams that are not protected by the WSHR scheme and a penalty factor, $K_{IP}^{s,d}(m,n)$. The penalty factor $K_{IP}^{s,d}(m,n)$ is normalized to the cost of one wavelength mile.

In its most general form, penalty $K_{IP}^{s,d}(m,n)$ is a function of the particular lightpath, identified by the source — s — and the destination — d — and of the network line, identified by the line end-node pair — (m,n) . High penalties may be assigned to special lightpaths (e.g., lightpaths with particular requirements such as maximum delay, minimum required bandwidth) or to particular network lines.

Alternatively, penalty $K_{IP}^{s,d}(m,n)$ may be used to enforce a specific type of resilient scheme on a selected set of network lines independent of the routed lightpaths, in which case it may be simplified as $K_{IP}(m,n)$.

Penalty $K_{IP}^{s,d}(m,n)$ may also be utilized to determine the fraction of traffic that must be protected by the WSHR scheme, independent of the lightpath and the network line under consideration. In this case the penalty is simply characterized by K_{IP} , which becomes a tuning factor that the designer may use to achieve the intended distribution of resilient schemes in the network. This application is further considered in the paper.

In solving the IWM problem, we assume that the designer defines a matrix of traffic demands in terms of lightpaths between node pairs. The traffic demands are based on the estimated network load. For the WDM layer, two WSHR protection schemes are considered: DP-WSHR and SL-WSHR. Practical design constraints, such as maximum ring size, maximum number of rings covering the same line and covering the same node, must also be taken into account in order to match available technology performance and desired network management complexity.

The IWM problem consists of three sub-problems:

- the RC sub-problem: select the (Multi-WSHR) ring cover that will provide the protection scheme in the optical layer;
- the WL sub-problem: select the working lightpath(s) for each traffic demand; and
- the SW sub-problem: select which ring protects which working lightpath and decide which part of the lightpath is protected by the optical and which part of the lightpath

is protected by the IP layer.

4.1.1 Applying Simulated Annealing (SA) to Solving the IWM Problem

The survivable mesh network under design is represented by a graph $G(V, E)$ in which V is the set of vertices or nodes of the network and E is the set of directed arcs representing the network lines connecting the nodes. The solution of the IWM problem consists of choosing, from a given set of candidate rings $C = \{c_1, \dots, c_i, \dots, c_R\}$ a subset $C' = \{c'_1, \dots, c'_i, \dots, c'_m\}$ that minimizes the cost function defined as

$$f_{tot}(d_{mn}, \lambda_{mn}^{sd}) \quad (1)$$

where λ_{mn}^{sd} indicates the number of working lightpaths from node s to node d routed on arc $(m, n) \in E$ and d_{mn} is the length of arc $(m, n) \in E$.

The equation representing the cost function f_{tot} may have different formulations, depending on the WSHR protection technique under consideration. Its general expression consists of one cost f_w that represents the total cost (working+protection) of optically protected lightpaths and another cost f_{IP} representing the cost of the lightpaths protected at the IP layer:

$$f_{tot} = f_w + f_{IP}. \quad (2)$$

Function f_w depends on the specific WSHR technique being utilized in the Multi-WSHR protection scheme and assumes the two formulations, respectively for DP-WSHR and SL-WSHR, computed (as f_1) in [5].

Function f_{IP} is calculated as follows:

$$f_{IP} = \sum_{(m,n) \text{ not OL protected}} \sum_{sd} (\lambda_{mn}^{sd} (d_{mn} + K_{IP} \cdot p)) \quad (3)$$

where p is a normalization factor that depends on the physical network characteristics (in our example $p = \sum_{m,n} d_{mn}$).

The algorithm designed to solve the IWM problem operates as shown in the flow chart of Figure 4(b). Input to the algorithm consists of the network topology $G(V, E)$, the set of candidate rings C , and the demand matrix $D(i, j)$ which denotes the number of lightpath demands required for each node pair. An initial solution consisting of a subset of rings C'_0 (subset of C) may be defined by the user. This initial solution is used by the algorithm to start the optimization process and performs incremental runs of the algorithm to improve previously found solutions. If not otherwise specified, C'_0 is empty.

The basic approach of the optimization algorithm consists of selecting a subset of rings from set C along which the working lightpaths are routed with the aim of minimizing cost function f_{tot} . The routing is performed utilizing an auxiliary graph called the Ring Interconnection Graph (RIG) [5] that indicates the various routing costs, i.e., the cost of the optical protection when a ring is available on the chosen line or the cost of the IP restoration, determined by K_{IP} , when a ring is not available on the chosen line. The cost of the chosen solution is computed and used to determine the suitability of the chosen

subset of rings. This operation is repeated until a stop condition is met, e.g., expiration of the allowed CPU time for the optimization process. The returned solution is the one with the lowest cost among the solutions explored by the algorithm.

More specifically, to select the rings of the cover a Simulated Annealing (SA) approach is used [5]. Other heuristic approaches, such as Genetic Algorithm or Tabu Search may be equally suitable to perform this task.

While selecting the ring cover, some practical (user defined) design constraints are also taken into account, namely

- N_r that is the maximum number of rings allowed to cover the same link and
- N_v that is the maximum number of rings allowed to connect a node.

Only subsets of rings that satisfy the specified constraints are considered by the SA algorithm.

4.2 Numerical Results

Some numerical results are discussed to illustrate the features of the proposed heuristic approach, i.e., the possibility 1) to trade the solution optimality for the solution time, 2) to optimize different WSHR protection techniques, and 3) to study the distribution of the optimal partition of the network lines between the WDM protection and the IP restoration schemes. The results are obtained after carefully tuning some of the SA parameters. A complete description of the tuning procedure can be found in [5].

ILP			SA			
# of paths	time	λ -miles	average time (s)	minimum λ -miles	average λ -miles	maximum λ -miles
1 (SP)	1 min	5711890	57	5155140	5280980	5403890
2	2 min	5037850	124	5042390	5172120	5282900
8	4 min	5030680	223	4959940	5100360	5225400
8	5 min	5018250	283	4949780	5082670	5161220
8	5 h	4515350	18331	4823110	4848464	4908660

Table 2: ILP results versus SA results for the Pan-European Network assuming non-uniform lightpath demands and SL-WSHR.

The advantage of using the SA heuristic when the solution time is limited is demonstrated by the results summarized in Table 2. These experiments consider the application of a Multi-WSHR scheme based on SL-WSHR's to the Pan-European backbone network depicted in Figure 4(a). The maximum number of nodes allowed in the rings is 6 which gives a set of 63 candidate rings. The lightpath demands are symmetric but non-uniform (see [5]), and the entire traffic is protected in the OL (i.e., K_{IP} is infinite) with $N_r = 2$ and $N_v = 4$. The computational time is limited from few minutes to 5 hours (on a Pentium 200 MHz based machine). Table 2 compares the results obtained by both an Integer

Linear Programming (ILP) formulation presented in [6] and the SA approach. The values in the leftmost column indicate the number of alternative paths between each node pair that the ILP solver may choose from to optimally route the working lightpaths ⁸. The SA heuristic outperforms the ILP solver best found result when computational time is limited to one minute or less ⁹.

WSHR protection	wavelength costs			fiber costs		
	min	ave	max	min	ave	max
DP-WSHR	5547690	5766082	5910070	711310	739911	759380
shared fiber SL-WSHR	4855710	4957815	5055350	620470	637270	650170
non-shared fiber SL-WSHR	4855710	4957815	5055350	639380	659206	675920

Table 3: Total cost for the Pan-European network with three types of WSHR protection schemes: DP-WSHR, shared fiber SL-WSHR (similar to the O-2F/BLSR), non-shared fiber SL-WSHR (similar to the O-4F/BLSR).

The versatility of the proposed heuristic approach is shown in Table 3. The setup for these experiments is the same as utilized previously. The last three columns report the total *fiber-mileage* required to guarantee optical protection of all traffic. The fiber mileage is simply obtained from the λ -mileage cost on a link-by-link basis and depends on the number of wavelengths per fiber (8 in the experiment) and on the particular WSHR scheme being utilized. Three different WSHR schemes have been considered: DP-WSHR, shared fiber SL-WSHR, and non-shared fiber SL-WSHR. The last two schemes are conceptually similar to the O-2F/BLSR and O-4F/BLSR, respectively, with the few significant differences that the number of fibers in the ring is not strictly limited to 2 or 4 and the fibers of a line may be shared by multiple rings. Results indicate that the Multi-WSHR based on DP-WSHR rings is approximately 15% more expensive than the SL-WSHR rings. The shared fiber SL-WSHR and the non-shared SL-WSHR solutions require the same λ -mileage but the former needs 3% less fiber-mileage.

Table 4 demonstrates that by varying the value of K_{IP} , it is possible to shift the percentage of working lightpaths and network lines protected, respectively, at the IP and WDM layers. These simulations are run on the network depicted in Figure 2(c) characterized by line lengths varying from few hundreds to thousands of miles. A symmetric and uniform traffic demand of 5 lightpaths between every node pair is considered. Physical constraints $N_r = 2$ and $N_v = 4$ are assumed. From the last column of Table 4 we see that, for decreasing values of K_{IP} , i.e., for decreasing cost of the IP restoration, the percentage of working λ -miles protected at the IP layer increases. This trend continues until all lightpaths are not protected at the optical layer and fully rely on the IP layer

⁸Value 1 means that there is only one path, which corresponds to solving the WL sub-problem first, then solving the RC and SW subproblems.

⁹The ILP solver solutions summarized in Table 2 are the best found solutions in the limited computational time and they may not correspond to the problem optimal solution.

K_{IP}	f_w	total λ -miles work.	total WDM λ -miles prot.	IP λ -miles work.	IP λ -miles work./ total λ -miles work.
0.20	975200	455800	519400	0	0.00
0.14	972200	453500	518700	8000	0.02
0.12	956700	452600	504100	13500	0.03
0.10	904700	459000	445700	43500	0.09
0.08	723000	445200	277800	196000	0.44
0.06	630400	440200	190200	269000	0.61
0.00	432500	432500	0	432500	1.00

Table 4: Variation of K_{IP} ($p = 23100$).

resilience capabilities. For $K_{IP} = 0$, the restoration at the IP layer is assumed to carry no additional cost beyond the working wavelength miles.

5 Conclusions

This paper reviewed the most common restoration and protection schemes available at either the IP and the WDM layer. It is envisioned that both layers will jointly cooperate to provide the necessary resilient schemes to protect the user’s traffic from disruptions due to network failures. A heuristic approach, based on Simulated Annealing (SA), was then presented to optimally choose the resilient scheme for each individual line of the IP over WDM mesh network. To illustrate the applicability of the proposed approach with a practical design case, the cost function under optimization was defined as the sum of the total provisioned WDM bandwidth and the cost of the IP restoration scheme characterized in the form of a penalty factor, K_{IP} . This penalty factor may be used to consider various design factors, e.g., blocking probability of the restoration scheme, restoration latency, IP router processing capability. The proposed heuristic proves to have the flexibility to deal with different Multi-Wavelength Self-Healing Ring protection schemes (WSHR), such as the DP-WSHR and the SL-WSHR, without requiring significant changes in the optimization technique. Only the cost function needs to be adjusted to the particular protection scheme under consideration.

More study is required in this relatively young field of survivable IP over WDM networks, and several additional critical factors must be considered in the design of such networks. These factors include the application’s requirements, e.g., not every application allows for the relatively slow IP restoration schemes; other protection schemes, e.g., end-to-end path protection; legacy constraints, e.g., nodes in the network may support only few resilient schemes.

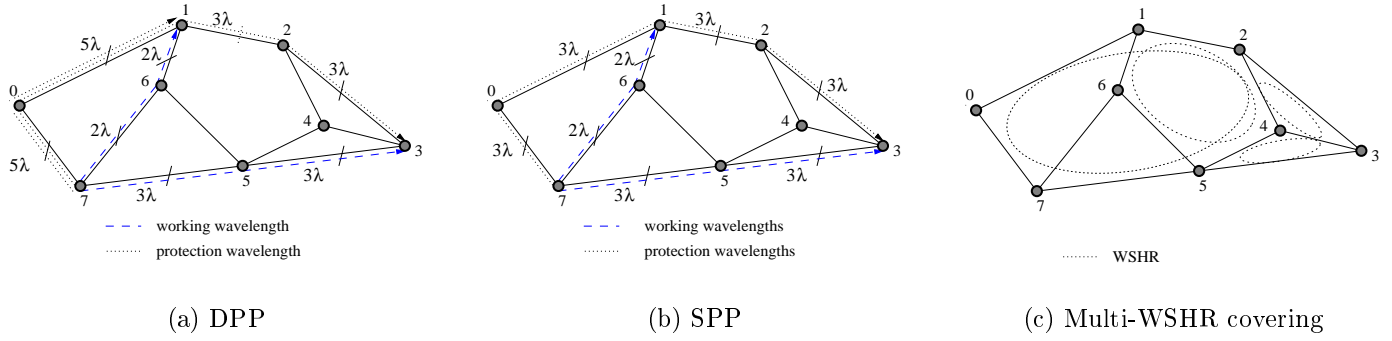


Figure 2: Protection wavelength allocation in WDM Mesh networks.

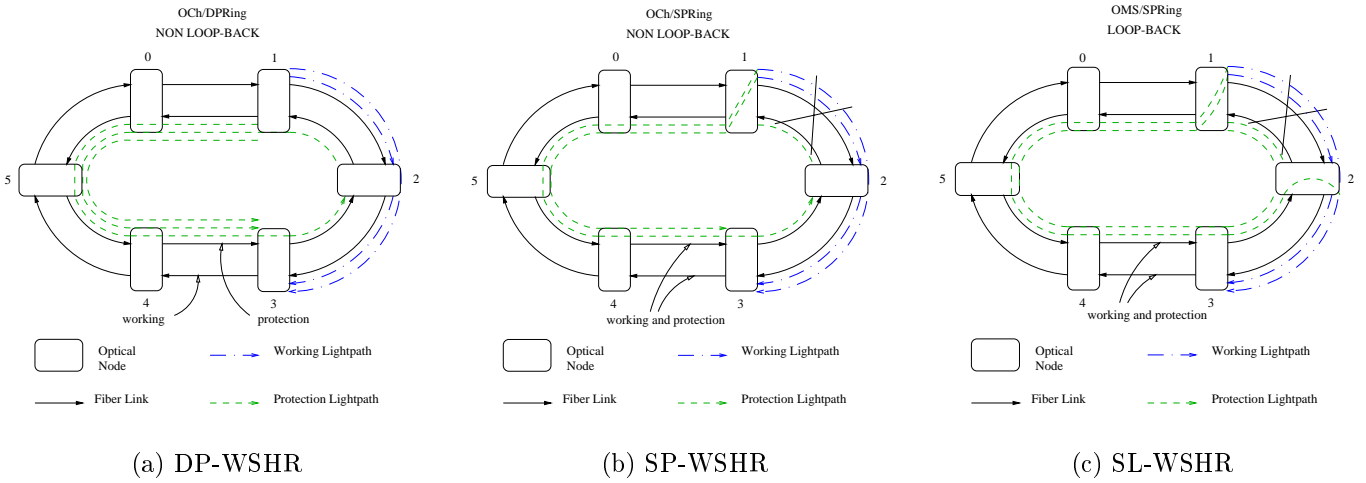
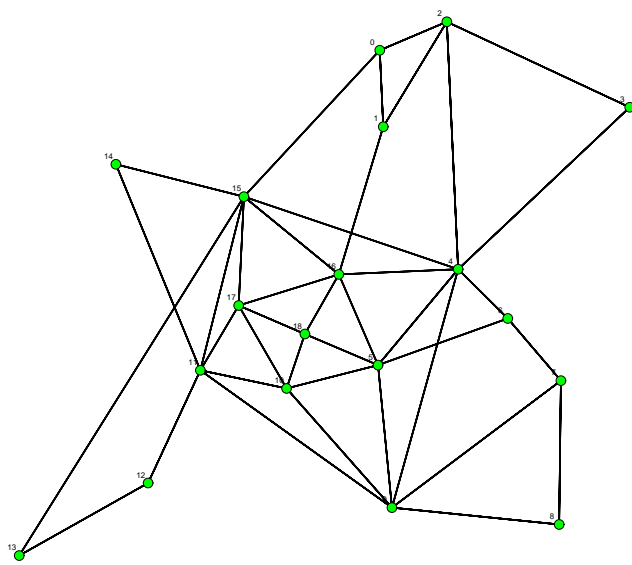
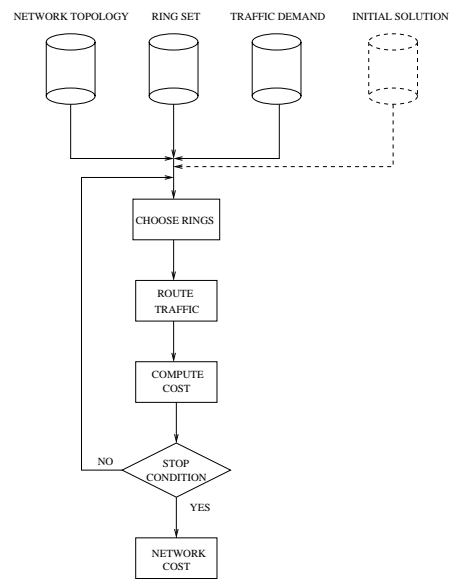


Figure 3: Protection wavelength allocation in WDM Self-Healing Rings.



(a)



(b)

Figure 4: Pan-European network and solution approach.

References

- [1] J. B. Slevinsky, W. D. Grover, and M. H. MacGregor, "An Algorithm for Survivable Network Design Employing Multiple Self-Healing Rings," in *Proceedings of IEEE GLOBECOM '93*, Nov.-Dec. 1993, vol. 3, pp. 1568–1573.
- [2] L. Crochat and J. Y. Le Boudec, "Design Protection for WDM Optical Networks," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, Sept. 1998.
- [3] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part II – Restoration," in *IEEE International Conference on Communications, 1999. ICC '99*, Vancouver, Canada, June, 6-10 1999, IEEE, vol. 3, pp. 2023 –2030.
- [4] B. V. Caenegem, W. V. Parys, F. De Turck, and P. M. Demeester, "Dimensioning of Survivable WDM Networks," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1146–1157, Sept. 1998.
- [5] A. Fumagalli and L. Valcarenghi, "Fast Optimization of Survivable WDM Mesh Networks Based on Multiple Self-Healing Rings," in *All-Optical Networking 1999: Architecture, Control, and Management Issues*, Boston, MA, 19-21 September 1999, vol. 3843, pp. 44–55.
- [6] A. Fumagalli, I. Cerutti, M. Tacca, F. Masetti, R. Jagannathan, and S. Alagar, "Survivable Networks Based on Optimal Routing and WDM self-Healing Rings," in *Proceeding of IEEE INFOCOM '99*, March 21-25 1999.
- [7] G. Mohan and K. Somani, A., "Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks," in *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2000*, Tel Aviv, Israel, March, 26-30 2000, vol. 3, pp. 1761–1770.
- [8] T. M. Chen and T. H. Oh, "Reliable Services in MPLS," *IEEE Communications Magazine*, vol. 37, no. 12, pp. 58–62, December 1999.
- [9] J. Anderson, S. Manchester, J., A. Rodriguez-Moral, and M. Veeraraghavan, "Protocols and Architectures for IP Optical Networking," *Bell Labs Technical Journal*, vol. 4, no. 1, pp. 105–124, January-March 1999.
- [10] C. Metz, "IP Protection and Restoration," *IEEE Internet Computing*, vol. 4, no. 2, pp. 97–102, March-April 2000.
- [11] G. Hjálmtýsson, P. Sebos, G. Smith, and J. Yates, "Simple IP Restoration for IP/GbE/10GbE Optical Networks," in *Optical Fiber Communication Conference, OFC 2000*, Baltimore, MD, March, 5-10 2000, PD36.
- [12] O. Gerstel and R. Ramaswami, "Optical Layer Survivability: a services perspective," *IEEE Communication Magazine*, vol. 38, no. 3, pp. 104 –113, March 2000.

- [13] S. Bandyopadhyay, Sengupta A., and A. Jaekel, “Fault-tolerant routing scheme for all-optical networks,” in *All-Optical Networking 1998: Architecture, Control, and Management Issues*, Boston, MA, November, 5-8 1998, vol. 3531, pp. 420–431, SPIE.