Group Shared Protection (GSP): A Scalable Solution for Spare Capacity Reconfiguration in Mesh WDM Networks

Anwar Haque[1], Pin-Han Ho[1,2], Raouf Boutaba[1], and James Ho[2]

School of Computer Science, University of Waterloo, Ontario, N2L3G1, Canada[1]
Department of Electrical and Computer Engineering, University of Waterloo, Ontario, N2L3G1, Canada [2]

***Abstract*--This paper proposes a novel framework of shared protection, namely Group Shared Protection (GSP), in mesh Wavelength Division Multiplexing (WDM) networks with dynamically arrived connection requests. Based on the $(M:N)^n$ control architecture, GSP has n mutually independent protection groups, each of which containing N SRLG-disjoint working paths protected by M protection paths. Due to the SRLG-disjointedness of the working paths in each protection group, GSP not only allows the spare capacity to be totally sharable among the corresponding working paths, but also reduces the number of working paths affected due to a single link failure. Based on the framework, an Integer Linear Program (ILP) formulation that can optimally reconfigure the spare capacity for a specific protection group whenever a working-protection path-pair joins is proposed. Two heuristics namely link-shared (LSP) and ring-shared protection (RSP) are introduced for further compromising the performance and the computation complexity. The proposed schemes are compared with a reported one, namely Successive Survivable Routing (SSR). The experimental results show that LSP, RSP and SSR yield similar performance in terms of resource sharing, whereas ILP outperforms all of them by (6-16)%. Due to the limited number of working paths in each protection group, ILP can handle dynamically arrived connection request in a reasonable amount of time. Also, we find that the number of affected working paths in GSP is about half of that in SSR. We conclude that GSP provides a scalable and efficient solution for dynamic spare capacity reconfiguration following the $(M:N)^n$ control architecture.**

Keywords-Wavelength Division Multiplexing (WDM); $(M:N)^n$ control architecture; shared protection; spare capacity allocation

I. INTRODUCTION

The $(M:N)^n$ type protection has been recently defined in the Internet Draft [1] and will highly likely serve as a framework of spare capacity management in the Generalized Multi-Protocol Label Switching (GMPLS) standard control protocol for the next-generation backbone networks with Wavelength Division Multiplexing as the core technology. This paper introduces a novel approach, namely Group Shared Protection (GSP), for realizing the $(M:N)^n$ control architecture, which is aimed at providing a general approach for dynamic survivable routing in mesh WDM networks. With the $(M:N)^n$ type protection, n protection groups are defined in the networks, each of which supports N working paths protected by a pool of M protection paths. The design of GSP scheme is aimed at obtaining a higher degree of sharing and limiting the number of lightpaths subject to a single failure at a given instant of time. GSP is also expected to significantly reduce the control overhead in terms of spare capacity management by sub-grouping working lightpaths in the networks into multiple protection groups.

These unique features of the GSP scheme create the basis for providing an efficient solution to deal with single failure and can be easily extended to the multi-failure scenario. In addition to the great flexibility in the control aspect, GSP's advantages include: (a) spare capacity in a protection group can be totally sharable by corresponding working paths; (b) a significant amount of reduction in computation complexity can be seen since the spare capacity in a specific protection group is for protecting the working capacity in that protection group only; (c) the computation time for jointly allocating the current working-protection path-pair and reconfiguring the spare capacity in each protection group through ILP is well constrained and is reasonable for dynamic traffic scenario, and (d) it limits the number of working paths affected by a single failure.

To implement the GSP framework, three approaches are examined in this study. The first is an Integer Linear Program (ILP), which aims to reconfigure the spare capacity and to allocate the working and protection path-pair in a single step for the current demand. Due to the NP-completeness in solving an ILP [23] two heuristics are proposed, called *link-shared* (LSP) and *ring-shared* (RSP) protection. Simulation is conducted to verify the GSP schemes, in which a comparison is made with *Successive Survivable Routing* (SSR) [7] based on three metrics: (a) the total capacity in terms of wavelength channels; (b) the total number of working lightpaths affected due to a single failure, and (c) load distribution along each link in the network. We claim that GSP can well match with the $(M:N)^n$ framework, which results in a scalable control and management on the spare capacity in the networks.

The concept of Shared Risk Link Group (SRLG) serves as a key role in the development of our shared protection schemes. SRLG is defined as a group of network elements (i.e., links, nodes, physical devices, software/protocol identities, or a combination thereof) subject to the same risk of single failure. In practical cases, an SRLG may contain multiple seemingly

unrelated and arbitrarily selected links/nodes. The fact that two paths do not take any common SRLG is referred to as the *SRLG-disjointedness*, which is the major effort of achieving 100% restorability under a single failure scenario if one of the paths is taken as the working path and the other is taken as the protection path. A working path is considered involved in a SRLG only if it traverses through any network element that belongs to the SRLGs. A path may be involved in multiple SRLGs. This study focuses on the case that each arc in the network topology is an SRLG, where an arc is composed of two links in opposite directions terminated by two adjacent nodes in the network topology. Thus, a working path traversing through H hops will be involved in H different SRLGs. We work under the assumption that the probability of failure for each physical conduit is independent. In other words, to achieve 100% restorability, it is sufficient and necessary for every link traversed by the working path to be protected by at least one link-disjoint protection path. In the event where a failure interrupts a working path, the switching fabric in each node along the corresponding protection path is configured by prioritized signaling mechanisms; then traffic-switchover is performed to recover the original service supported by the working path. Therefore, the protection path of different working paths can share spare capacity if their working paths are not involved in any common SRLG. In other words, whether two protection paths can share spare capacity depends on the physical location of their working paths. The dependency is the reason for the existence of the SRLG constraint [1]. A simple example is shown in Fig. 1 where W_1 and P_1 form a working and protection path-pair. The backup path of W_2 (another working path) should exclude the possibility of using any of the spare capacity (or wavelength channels) taken by P_1 because W_2 traverses link A-B, which shares the same risk of a single failure with W_1.

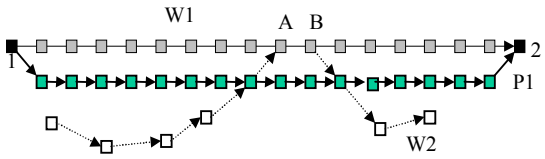

Figure 1. An example to illustrate the SRLG constraint

To develop an optimal or approximately optimal solution for dynamic reconfiguration of the spare capacity that can be both capacity and computation-efficient is still an open question. The most difficult problem is due to the scalability issue, where the reconfiguration process usually has to consider the global traffic distribution. In addition, the dependency between the working paths and the corresponding spare capacity further complicates the computation complexity. To serve large networks with frequently changing traffic, issues of survivability for the service continuity have become a great challenge to the design of survivable WDM optical networks [3].

Without considering grouping, the related study on path shared protection has been extensively reported in the past few years [6-21]. Most of these studies focus on the approach that the working path is first derived and then the corresponding protection path is solved on the residual network topology which is referred to as Two-Step-Approach [6], where working paths are routed with the maximum freedom. This idea is taken by the study in [7, 8], however, the study only focuses on the solution of the protection path without considering the working path. To explore a better solution in finding the least-cost working and shared protection path-pair, the study in [6,9,10] addresses the location of the working path by inspecting k-shortest paths between each S-D pair one after the other in an ascending order. All of the above schemes take the approach of exhaustively enumerating the k-shortest paths, which may wear out novelty and leaves room to improve. To speed up the routing process, an algorithm named Active-Path-First with Potential Backup Cost (APF-PBC) is proposed in [11], which aims to increase the chance of finding a cheaper protection path by elaborating the location of the working path. To improve the study in [11], [6] proposes an approach named Maximum Likelihood Relaxation (MLR), which finds the working path using a cost function which minimizes the reciprocal of the product between the total link cost and the number of the maximum number of links with sufficient sharable spare capacity in the network. These approaches adopt several simple schemes rather than exploit the functions of group protection and resource sharing which are integral to GMPLS. Many approaches still utilize NP-hard optimization processes based on static working traffic demands [15-18].

Comparing with the reported counterparts [1-5] where working lightpaths in the networks are sub-grouped, GSP has the working lightpaths in each protection group being SRLG-disjointedly routed. To the best of our knowledge, this is the first work that attempts to optimally reconfigure the spare capacity in each protection group (where working paths are routed link-disjointedly) using ILP in a dynamic traffic scenario.

The rest of the paper is organized as follows. Section II elaborates the proposed GSP framework and introduces proposed ILP and heuristics. Section III shows the experiment results. Section IV concludes the paper.

II. GROUP SHARED PROTECTION (GSP)

A. *Basis of GSP*

The common Control and Measurement Plane (CCAMP) working group has recently proposed a framework for an $(M:N)^n$ shared protection scheme [1]. With the $(M:N)^n$ protection architecture, each of the n $(M:N)$ protection groups in an $(M:N)$ recovery scheme has N working paths and a total of M protection paths. Some of the M protection paths in each $(M:N)$ group are shared with other protection groups while the rest are dedicated only to that particular group. Although the proposed GSP framework is based on this control architecture,

it possesses the following unique properties: (a) the number of working paths in each of the n protection groups is SRLG-disjointedly routed and thus well constrained; (b) it provides 100% intra-group sharing while not allowing inter-group sharing; (c) unlike $(M:N)^n$ architecture, a protection group in GSP can contain working paths between any source-destination pairs, while the $(M:N)^n$ framework only allows working paths to be set up between a particular source destination pair in a protection group.

The merits of using GSP are obvious. In addition to the scalability that can be gained due to the sub-grouping of the network traffic in the control plane, the restoration process can be more easily handled. In case of a link failure, all the working paths passing through the link subject to the failure get interrupted, leading to a high restoration cost since the restoration mechanism initiates the spare capacity for all the working paths passing through the link. This not only introduces the restoration cost at the optical layer, but also generating alarms to higher layers which is known as failure propagation. Since GSP requires the working paths to be link-disjointedly routed in a single protection group, thus the number of working paths along a link is upper-bounded by the number of protection groups in the network. Thus, the number of working paths affected by a single failure is also well bounded.

In the following two subsections, proposed ILP and heuristics are introduced for realizing the GSP scheme.

B. Integer Linear Program (ILP)

An ILP is proposed to optimally reconfigure the existing protection capacity in a protection group while setting up the working-protection path pair for the current request in a dynamic traffic scenario. It can be solved in a reasonable amount of time using the commercial optimizer CPLEX [22] because the number of working and protection path-pairs is limited by the network topology. Thus, we claim that the proposed ILP can be well suited to the dynamic traffic scenario. Basically, the ILP is solved based on the current link-state whenever there is an incoming connection request. Not only will the working and protection path-pair corresponding to the current call be settled, but also the spare capacity in the protection group will be reconfigured so that sharing of spare capacity is maximized. Following sections describes how our ILP is realized in GSP scheme for spare capacity reconfiguration:

Let k be the newly arrived connection request for which the working path w^k and protection path p^k need to be established in a protection group so that sharing of spare capacity is maximized in that protection group. Let W be the set of all existing working paths in a protection group and let N be the number of working paths in that group. Now $k = N+1$ for that protection group which means the k^{th} working-protection pair need to be setup in that protection group. Let $W = \{w^1, w^2, ..., w^{k-1}\}$ and $P = \{p^1, p^2, ..., p^{k-1}\}$ be the set of all existing working and protection paths respectively in that particular protection group. Note that, while setting up the working-protection pair for k^{th} connection request for a group, only P will be reconfigured.

Let $x^k_{i,j}$ be a binary variable that takes on a value of 1 if working path k goes through link (i,j) and 0 otherwise. A set of these values $(i.e., x^1_{i,j}, x^2_{i,j}, ..., x^{k-1}_{i,j})$ provides link-state information to the ILP for a current connection request k. These values are collected and supplied to the ILP. Let $y^k_{i,j}$ indicates whether a wavelength is used by protection path k on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}$ indicates whether a wavelength is used by any protection path on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise.

Given a network $G(V,E)$, a newly arrived connection request k, a link-state table L (that tells which link is being used by which working paths in a group); following ILP establishes working-protection path pair for a connection request k such that the total number of wavelengths used for working and protection paths are minimized by reconfiguring the existing protection wavelengths.

Minimize

$$\sum_{i,j}\sum_{k} x^k_{i,j} + \sum_{i,j} z_{i,j} \tag{1}$$

Subject to

$$\sum_j x^k_{i,j} - \sum_j x^k_{j,i} = \begin{cases} 1, & if \ \ i = src \\ -1, & if \ \ i = dst \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

$$\sum_j y^k_{i,j} - \sum_j y^k_{j,i} = \begin{cases} 1, & if \ \ i = src \\ -1, & if \ \ i = dst \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

$$\sum_k x^k_{i,j} + \sum_k x^k_{j,i} \le 1 \tag{4}$$

$$x^k_{i,j} + y^k_{i,j} + x^k_{j,i} + y^k_{j,i} \le 1 \tag{5}$$

$$y^k_{i,j} \le z_{i,j} \tag{6}$$

Eq. (1) is the target function aiming to establish working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource. Eq. (2) is flow conservation constraint for working paths that ensures the connectivity between respective source-destination pairs. Eq. (3) is flow conservation constraint for protection paths that ensure the connectivity between respective source- destination pairs. Eq. (4) is a link disjoint constraint which ensures that link (i,j) can only be used by a single working path in a group. Note that a set of $(x^1_{i,j}, x^2_{i,j}, ..., x^{k-1}_{i,j})$ variables represent the current link state information for a particular protection group for a current connection request k. These link state values $(i.e., x^1_{i,j}, x^2_{i,j}, ..., x^{k-1}_{i,j})$ are supplied to the ILP. Eq. (5) ensures that a working

path and its corresponding protection path are always link-disjoint. Eq. (6) ensures the maximum sharing of the wavelength among protection paths.

There could be two scenarios when ILP is applied to a protection group. Case 1: There is only one group in the network, ILP is applied to the only existing group and if the current connection *k* can not be satisfied, then a new group is created and ILP is applied to that new group to satisfy *k*. Case 2: There is more than one group in the network. ILP is only applied to the next group if a connection *k* can not be satisfied by the previous group. If a connection can not be established by any of the existing groups, then a new group is created to satisfy *k*.

Let us assume that there is currently *n* protection groups (PG) in the network and a new connection request *k* arrive that needs to be satisfied through ILP. The flowchart in Fig. 2 explains how ILP is used to manage the dynamic connection request for spare capacity reconfiguration:

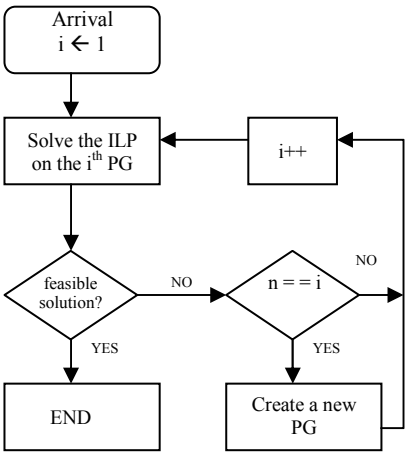

Figure 2. Managing connection requests using ILP

Note that all the existing protection capacity is totally re-configured using ILP every time a connection request arrives.

C. *Heuristic algorithms*

For further compromising the performance and the computation complexity of proposed ILP, two heuristics, namely link-shared protection (LSP) and ring-shared protection (RSP) are proposed. Dijkstra's shortest path algorithm (in terms of hop count) is adopted as routing scheme for determining working and protection paths. Following three rules are used while describing the heuristics:

Rule 1: All the working paths in a protection group *G* have to be mutually link-disjoint

Rule 2: Working path *W* and its corresponding protection path *P* are link disjointedly routed in a protection group *G*

Rule 3: A protection Ring *R* needs to cover all source-destination nodes of existing working paths in group *G*

Link-shared protection (LSP): In link-shared protection, any connection request is satisfied by setting up a working-protection path pair in a group based on the current link state information. This scheme follows a Two-Step approach [6] for setting up working path *W* and corresponding protection path *P* sequentially in a group. Once a protection path is chosen by this scheme, the link cost along that path becomes zero for any future protection path in that protection group. In other words, once a wavelength is used on a link in a group, that wavelength can be used by any other protection path with no cost in that particular protection group.

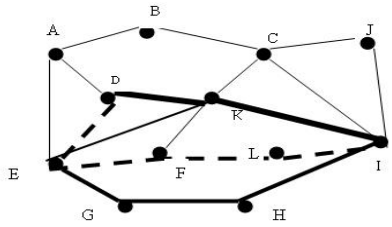

Figure 3. Link-shared protection (LSP)

Fig. 3 explains the link-shared protection. A working and protection path pair is established in this group through D-K-I and D-E-F-L-I respectively. According to the LSP, protection link cost database is updated by assigning a zero cost to link segments D-E-F-L-I and this updated link cost database will be applied to any future protection paths in this particular protection group. Now, to establish a protection path for working path E-G-H-I, path E-F-L-I will be chosen (with a cost of zero). LSP would follow Rule 1 and Rule 2. Note that in LSP, existing protection capacity in a protection group is never reconfigured. A dynamically arrived connection request is satisfied by checking Rule 1 and Rule 2 without reconfiguration of existing protection capacity. The flowchart in Fig. 4 explains how dynamic connection request is managed in LSP.

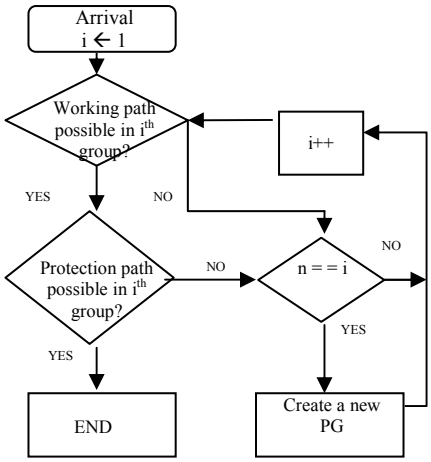

Figure 4. Managing connection arrival in LSP

In Fig. 4, there is *n* number of existing protection groups. Upon arrival of a new connection request, LSP starts checking sequentially the *n* protection groups whether a link-disjoint working path can be established for new connection request

along with the protection path. As soon as it finds a protection group that satisfies these requirements, it accommodates the new connection in that protection group. If there are no groups available where the new connection can be accommodated, it creates a new protection group and accommodates the request in $(n+1)^{th}$ group. The size of the protection group in LSP increases whenever it accommodates a new connection request.

Ring-shared protection (RSP): A ring based shared protection scheme is proposed that creates a protection ring which protects all link-disjointed routed working paths by covering all the source-destination node pairs of those working paths in a protection group.

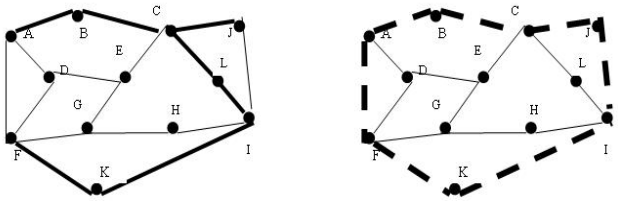

Figure 5. (a) Three link-disjoint working paths (A-B-C-J), (C-L-I) and (F-K-I) in a protection group. (b) Protection ring A-F-K-I-J-C-B-A provides protection for three working paths in (a)

Fig. 5(a) and 5(b) explain ring-shared protection. Working paths (A-B-C-J), (C-L-I) and (F-K-I) in a protection group are link-disjointedly routed (Rule 1). Now a protection ring needs to be established that will protect all these working paths. Rule 3 will be followed for this purpose. According to Rule 3, node A, J, C, I and F are required to be covered by the protection ring. Given a set of nodes in a network on which an optimal ring needs to be created is NP-hard [12]. For computational efficiency, following heuristic is proposed for creating such a ring.

Given a network *G(V,E) and* a set of nodes to be covered by the ring *R,* RSP works as follows to find ring *R* in a group:

Output: Protection Ring *R*
Initialize: *R* ← Null, *RingNodeSet* ← all src-dst pairs of working paths in a group, *RingEnd* ← any node randomly chosen from *RingNodeSet*, *Src*←*RingEnd*
Remove *Src* from *RingNodeSet*
For
ShortestPathSet ← all the shortest paths between *Src* to all nodes in *RingNodeSet*
LeastCostPath ← minimum cost path in *ShortestPathSet*
Dst ← destination node of *LeastCostPath*
R ← *R* ∪ *LeastCostPath*
update *G* by deleting all *(i,j), (i,j)*∈ *LeastCostPath*
Src ← *Dst*
remove *Dst* from *RingNodeSet*
If (number of nodes in *RingNodeSet* = = 1)
Then exit the loop
End For
LastRingHop ← *shortest path from Src to RingEnd*
R ← *R* ∪ *LastRingHop*

By applying the above algorithm, protection ring *A-B-C-J-I-K-F-A* (Fig. 5b) is constructed that protects all three working paths. Note that in RSP, only the protection resources (i.e., protection ring) are reconfigured every time a connection requests arrives in a protection group (PG). Dijkstra's shortest path algorithm (in terms of hop count) is adopted as routing scheme in RSP. A protection group starts with only one source-destination pair. The size of the protection group increases whenever it accommodates a new connection request. Fig. 6 explains how dynamic connection request is managed in RSP.

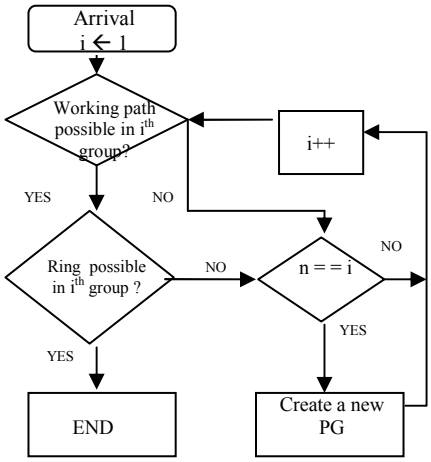

Figure 6. Managing connection arrival in RSP

In Fig. 6, there is *n* number of existing protection groups. Upon arrival of a new connection request, RSP starts checking sequentially the *n* protection groups whether a link-disjoint working path can be established for new connection request along with the protection ring. As soon as it finds a protection group that satisfies these requirements, it accommodates the new connection in that protection group. If there are no groups available where the new connection can be accommodated, it creates a new protection group and accommodates the request in $(n+1)^{th}$ group. It is important to note that RSP does not follow Rule 2 as protection is provided through a ring.

III. RESULTS AND DISCUSSIONS

The simulation is conducted on 8 different mesh networks [7,13], which are chosen as representatives of typical mesh topologies. The CPLEX linear optimizer is taken to solve the proposed ILP running on a SUN Ultra Enterprise server. The performance metrics taken in the study are (a) the total number of wavelengths taken by working and protection paths, (b) the number of affected working paths, and (c) the load distribution along each link in the network. The following assumptions are made. (a) Every connection request is a single lightpath that occupies a wavelength channel as traversing through the corresponding links. (b) The number of wavelengths along each link is infinite. (c) Each connection request arrives at the networks according to a Poisson process and departs after a period of time defined by an exponential

distribution function. For this simulation, average arrival rate and average lightpath holding time is 10 and 5 respectively. (d) Each node can serve as an ingress or egress node of the network with full wavelength conversion. (e) Dijkstra's shortest path algorithm (in terms of hop count) is adopted as routing scheme for determining working and protection paths. (f) After the network load reaches dynamic balance, the total number of wavelengths used, total number of affected working paths due to a single failure and load distribution along each link in the network are calculated.

Table I shows the simulation results for number of wavelengths required by standard dedicated protection (SDP), link-shared protection (LSP), ring-shared protection (RSP), ILP and SSR. Dijkstra's shortest path algorithm (in terms of hop count) is adopted in implementing SDP where working path is first established following a dedicated protection path link-disjointedly routed with the working path. In SDP, there is no sharing of protection wavelength channels among the protection paths.

TABLE I
TOTAL WAVELENGHTS USED BY PROTECTION SCHMES

V	SDP	LSP	RSP	ILP	SSR
10	370	298	284	250	300
12	418	356	336	306	349
13	486	423	397	353	423
15	645	573	594	504	586
17	569	504	498	422	480
18	662	589	563	525	587
23	835	738	759	680	750
50	1114	1008	1061	884	1026

The computation time for allocating a connection with ILP ranges from a few seconds to a few minutes, depending on the size and degree of the networks. Heuristics take much less time compared to reconfigurable ILP.

From Table I, it is clear that (a) LSP, RSP and SSR show similar performance; (b) ILP outperforms LSP, RSP and SSR schemes by (7-14)%, (6-16)% and (9-14)%, respectively.

The objective of measuring the number of working paths affected due to any single failure is to see how much less working paths are affected using group based approach with a scenario where no grouping is considered. For this experiment, SSR is applied in the network where grouping is not considered and LSP is applied considering grouping in the network. Table II shows the average number of affected working paths due to a single failure in GSP and SSR. Experimental results show that (31 – 55)% less working paths are affected by a single failure in GSP than SSR in each network topology. This fact leads into a huge reduction in restoration overhead in the network control and management

TABLE II
THE NUMBER OF AFFECTED WORKING PATHS DUE TO A SINGLE FAILURE

V	GSP	SSR
10	13	24
12	13	27
13	12	22
15	11	17
17	11	18
18	10	22
23	9	19
50	9	13

We also observe the traffic distribution by using different schemes. To investigate the effect of grouping, LSP and SSR [7] are implemented and compared for the cases of grouping and non-grouping, respectively. Due to the disjointedness of working paths in each group, GSP yields the network traffic much more evenly distributed along each link compared with that by SSR, leading to a better total throughput. Fig. 7 shows the load distribution in the 23-node network, where we assume that the number of wavelengths along each link is infinite.

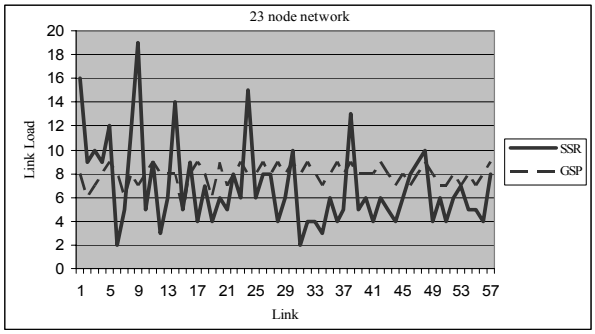

Figure 7. Load distribution in GSP and SSR – comparison between the cases of grouping and non-grouping

IV. CONCLUSIONS

In this paper, we demonstrated a novel framework called Group Shared Protection (GSP). Based on $(M:N)^n$ protection defined in the Generalized Multi-Protocol Label Switching (GMPLS), GSP is characterized by grouping the working and protection paths in the networks such that the spare capacity reconfiguration can be performed in a scalable way. For this purpose, an ILP-based approach was proposed for dividing the working traffic, allocating the current connection request, and reconfiguring the spare capacity in each protection group. In addition, two heuristics were introduced, namely Link-Shared Protection (LSP) and Ring-Shared Protection (RSP). We verified and compared the proposed schemes with a reported one - Successful Survivable Routing (SSR), by conducting simulation on 8 different network topologies. The simulation yields similar results in terms of resource sharing (i.e., number of wavelengths used) for LSP, RSP and SSR, while the ILP-based scheme outperforms all the others by (6-16)%. It is also observed that with GSP, the number of affected working paths

in case of a single link failure is around half of that with SSR. This would lead to a huge saving in restoration overhead in the network control and management. We conclude that GSP can serve for the future optical Internet that addresses a high requirement on scalability and survivability.

REFERENCES

[1] D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G. Li, B. Rajagopalan, and Y. Rekhter, "Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)", *Internet Draft*, <*draft-papadimitriou-ccamp-gmpls-recovery-analysis-03.txt*>, *working in progress*, May 2003.

[2] K. Sriram, D. Griffith, S. Lee, and N. Golmie, "Backup Resource Pooling in (M:N)^n Fault Recovery Schemes in GMPLS Optical Networks", Opticomm 2003.

[3] P. –H. Ho and H. T. Mouftah, "Reconfiguration of Spare Capacity for MPLS-based Recovery in the Internet Backbone Networks", *IEEE/ACM Transaction on Networking* Vol. 12, No. 1, Feb. 2004

[4] P. –H. Ho and H. T. Mouftah, "A Framework of a Survivable Optical Internet using Short Leap Shared Protection (SLSP)", *IEEE Workshop on High Performance Switching and Routing (HPSR 2001), Dallas,* May 2001.

[5] B. Ramamurthy and A. Ramakrishnan, "Design of Virtual Private Networks (VPNs) over Optical Wavelength Division Multiplexed (WDM) Networks", SPIE Optical Networks Magazine, Vol. 3, Issue 1, Jan./Feb. 2002.

[6] P. –H. Ho and H. T. Mouftah, "On Optimal Diverse Routing for Shared Protection in Mesh WDM Networks", *IEEE Transactions on Reliability,* Vol. 53, No. 6, pp. 216 - 225, June 2004

[7] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing", *Proceedings IEEE Infocom'01*, vol. 2, pp. 699-708, April.

[8] S. Datta, S. Sengupta, and S. Biswa, "Efficient Channel Reservation for Backup Paths in Optical Mesh Networks," *Proceedings IEEE Globecom'01*, San Antonio, Texas, Nov. 2001, OPC01-7.

[9] C. Xin, Y. Ye, S. Dixit, and C. Qiao, "A Joint Lightpath Routing Approach in Survivable Optical Networks," *Optical Network Magazines,* May/June, 2002, pp. 23-32.

[10] E. Bouillet, J. –F. Labourdette, G. Ellina, R. Ramamurthy, and S. Chaudhuri, "Stochastic Approaches to Compute Shared Mesh Restored Lightpaths in Optical Network Architectures", *Proceedings IEEE Infocom* 2002.

[11] D. Xu, C. Qiao, and Y Xiong, "An Ultra-fast Shared Path Protection Scheme -- Distributed Partial Information Management, Part II", *Proceedings IEEE International Conference on Network Protocols (ICNP 2002),* Paris, France, Nov. 2002.

[12] A. Fink, G. Schneidereit and S. Vo, "Ring network design for metropolitan area networks", *TU Braunschweig*, March 17, 1998

[13] S. Ramamuthy and B. Mukherjee, "Survivable WDM mesh networks: Part I--Protection," presented at the Infocom'99, New York, Mar. 1999.

[14] O. J. Wasem, "Optimal Topologies for Survivable Fiber Optic Networks Using SONET Self-healing Ring", *Proceedings IEEE GLOBECOM'91*, Nov. 1991, pp. 2032-2038.

[15] O. J. Wasem, "An Algorithm for Designing Rings for Survivable Fiber Networks", *IEEE Transactions on Reliability*, vol. 40, pp. 428-32, 1991.

[16] C. Thomassen, "On the Complexity of Finding a Minimum Cycle Cover of a Graph", *SIAM Journal of Computation*, vol. 26, no. 3, pp. 675-677, 1997.

[17] G. Ellinas and T. E. Stern, "Automatic Protection Switching for Link Failures in Optical Networks with Bi-directional Links", *Proceedings IEEE GLOBECOM'96*, November 1996, vol. 1, pp. 152-156.

[18] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 10, Oct. 2000.

[19] D. Stamatelakis and W. D. Grover, "Network Restorability Design Using Pre-configured Trees, Cycles, and Mixtures of Pattern Types", *TRLabs Technical Report TR-1999-05*, Issue 1.0, Oct. 2000.

[20] W. D. Grover and D. Stamatelakis, "Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration", *Proceedings IEEE International*

[21] W. D. Grover, J.B. Slevinsky, M.H. MacGregor, "Optimized Design of Ring-Based Survivable Networks", *Canadian Journal of Electrical and Computer Engineering*, vol. 20, no.3, August 1995, pp. 138-149.

[22] CPLEX: An optimizer by ILOG Inc, url : www.ilog.com

[23] M. Garey and D. Johnson, "*Computers and Intractability: A Guide to the Theory of NP-Completeness*", W. H. Freeman, 1979.