Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Networks 50 (2006) 168–180
Computer Networks
www.elsevier.com/locate/comnet

Group shared protection for spare capacity reconfiguration in optical networks

Anwar Haque [a,1], Pin-Han Ho [a,b,2], Raouf Boutaba [a,*]

[a] School of Computer Science, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1
[b] Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1

Available online 17 June 2005

Abstract

This paper introduces GSP, a group shared protection scheme, for wavelength division multiplexing (WDM) mesh networks with dynamically arrived connection requests. Based on the $(M{:}N)^n$ control architecture, GSP has n mutually independent protection groups (PGs), each of which containing N shared risk link groups (SRLG) disjoint working paths protected by M protection paths. Due to the SRLG-disjointedness of the working paths in each PG, 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 PG whenever a working–protection path-pair joins is proposed. This approach is appropriate for a dynamic traffic scenario where inter-arrival time is large and where arriving request can tolerate some delay, but may not be suitable where traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link-shared protection (LSP) are proposed. The proposed schemes are compared with an exiting one, namely the successive survivable routing (SSR). The simulation 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 PG, ILP can handle dynamically arrived connection requests 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.

* Corresponding author. Tel.: +1 519 888 4820.
E-mail addresses: ahaque@bbcr.uwaterloo.ca (A. Haque), pinhan@bbcr.uwaterloo.ca (P.-H. Ho), rboutaba@bbcr.uwaterloo.ca (R. Boutaba).
[1] Tel.: +1 519 888 4567x2529.
[2] Tel.: +1 519 888 4567x2452.

1389-1286/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2005.05.022

Keywords: Optical networks; Shared path protection; Shared risk link group; Spare capacity reconfiguration; $(M{:}N)^n$ protection architecture; Integer linear programming (ILP)

1. Introduction

The design of survivable wavelength division multiplexing (WDM) based optical networks is crucial. In this perspective, several path protection and restoration techniques have been proposed in the recent years. The $(M{:}N)^n$ protection architecture [1] is likely to serve as a basis for spare capacity management in the generalized multi-protocol label switching (GMPLS) standard control protocol for next-generation WDM backbone networks. In the $(M{:}N)^n$ protection architecture, n protection groups (PGs) are defined in the network, each of which supports N working paths protected by a pool of M protection paths. This paper introduces GSP, a group shared protection scheme, based on the $(M{:}N)^n$ control architecture, and aimed at providing a general approach for dynamic survivable routing in optical mesh networks. The design objectives for GSP are to obtain a high degree of sharing and to limit the number of lightpaths subject to a single failure at a given time. GSP is also expected to significantly reduce the control overhead in terms of spare capacity management by sub-grouping working lightpaths into multiple PGs. The envisioned features of the GSP scheme will create the basis for providing an efficient solution to deal with single failure and its extension to the multiple failures scenario.

The concept of shared risk link group (SRLG) is central to the development of our GSP scheme. SRLG is defined as a group of network elements (i.e., links, nodes, physical devices, software/protocol entities, or a combination thereof) subject to the same risk of single failure. In practice, 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 required for 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 any network element that belongs to the SRLGs. A path may be involved in multiple SRLGs. This paper focuses on the case where each arc in the network topology is an SRLG, and 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.

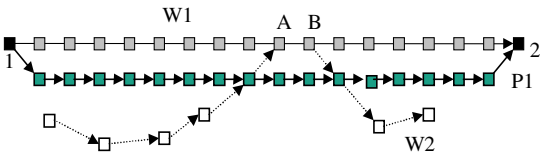


Fig. 1. An example to illustrate the SRLG constraint.

The development of optimal or near optimal solutions for dynamic reconfiguration of the spare capacity that can be both capacity- and computation-efficient is a difficult problem. This is particularly the case in large-scale networks where the reconfiguration process has to consider the global traffic distribution. In addition, the dependency between the working paths and the corresponding spare capacity further increases the computation complexity.

To implement our proposed GSP scheme, an integer linear programming (ILP) approach is used to reconfigure the spare capacity and to allocate the working and protection path pair in a single step for the current connection demand. Because of the computational complexity involved in the ILP approach, it is appropriate for a dynamic traffic scenario where inter-arrival time is large and arriving requests can tolerate some delays, but may not be an acceptable solution when traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link-shared protection (LSP), are proposed. RSP extends the *p*-cycle based path protection technique [25] for creating a protection ring which protects all link-disjointed routed working paths in a PG. LSP follows a two-step approach [5] for setting up the working path and the corresponding protection path sequentially in a PG. Simulations are conducted to verify the GSP scheme, and a comparison is made with the *successive survivable routing* (SSR) [6] 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 find that GSP is very suitable approach for realizing the $(M{:}N)^n$ architecture, and results in a scalable control and management on the spare network capacity.

The remaining of the paper is organized as follows. Section 2 discusses related works. Section 3 describes the proposed GSP scheme, its ILP formulation and the proposed heuristics. Section 4 shows the simulation results. Section 5 concludes the paper.

2. Related work

A number of recent works focused on shared path protection [5–20,22–26]. Most of these works derive the working path first and then determine the corresponding protection path from the residual network topology. This approach is referred to as the two-step-approach [5], where working paths are routed with the maximum freedom. In [6,7], solutions for deriving the protection path are presented without considering the working path. In order to find the least-cost working and shared protection path pair [5,8,9], consider the location of the working path by inspecting *k*-shortest paths between each source–destination pair one after the other in an ascending order. The approach adopted in the above schemes consists in exhaustively enumerating the *k*-shortest paths. To speed up the routing process, an algorithm named active-path-first with potential backup cost (APF-PBC) is proposed in [10]. This algorithm aims at increasing the chances of finding a cheaper protection path by considering the location of the working path. To improve on [10], Ho and Mouftah [5] proposes an approach named maximum likelihood relaxation (MLR), which finds the working path using a cost function that minimizes the reciprocal of the product between the total link cost and the maximum number of links with sufficient sharable spare capacity in the network. In [26], the authors proposed two schemes namely shared-path partial path protection (SP-PPP), and greedy-partial path protection (greedy-PPP) with a dynamic traffic scenario. The greedy-PPP and SP-PPP select a specific protection path for each link along a primary path where wavelengths can be shared among protection paths. Greedy-PPP is formulated as an ILP, which is a discrete optimization problem. Due to the significant computation complexity involved in this scheme, SP-PPP was proposed. Both schemes are then compared against the shared path-protection scheme [26], which is also a discrete optimization problem formulated as an ILP. None of the above approaches exploit the functions of group protection and resource sharing among the protection groups, which is integral to GMPLS. In [25], the authors extend the conventional "span-protecting" *p*-cycles [19] to a "path-

protecting'' p-cycle scheme where static working traffic demands are considered. This is typical in many existing works [14–17] where NP-hard optimization processes based on static working traffic demands are used.

Comparing with related works [1–4] where working lightpaths in the network are sub-grouped, our GSP scheme considers working lightpaths in each PG as SRLG-disjointedly routed. To the best of our knowledge, this is the first work that attempts to optimally reconfigure the spare capacity in each PG (where working paths are routed link-disjointedly) using ILP in a dynamic traffic scenario.

3. Group shared protection (GSP)

3.1. GSP foundation

The common Control and Measurement Plane (CCAMP) working group has recently proposed an architecture for an $(M{:}N)^n$ shared protection [1]. With $(M{:}N)^n$, each of the n PGs 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 PGs 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 PGs 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 PG 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 PG.

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 with GSP. Indeed, 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. This not only introduces the restoration overhead at the optical layer, but also generates alarms to higher layers known as *failure propagation*. Since GSP requires the working paths to be link-disjointedly routed in a single PG, the number of working paths along a link is upper-bounded by the number of PGs in the network. Thus, the number of working paths affected by a single failure is also well bounded. Fig. 2 explains how an incoming connection request can be placed into an appropriate PG.

Fig. 3 gives an example on the $(M{:}N)^n$ protection architecture considered in our study. In this example, let six lightpaths be required to be established, and the link-disjointedness of working paths be taken as the grouping policy. In *PG 1* (Fig. 3a), three working paths are protected by two protection paths, where the two working paths between nodes 1 and 6 completely share their spare resources. In *PG 2* (Fig. 3b), three link-disjoint working paths are protected by three protection paths, where *path 2* shares spare resources partially with *path 1*. In the terminology of GMPLS, *PG 1* and *PG 2* are represented as $(2{:}3)^1$ and $(3{:}3)^2$, respectively.

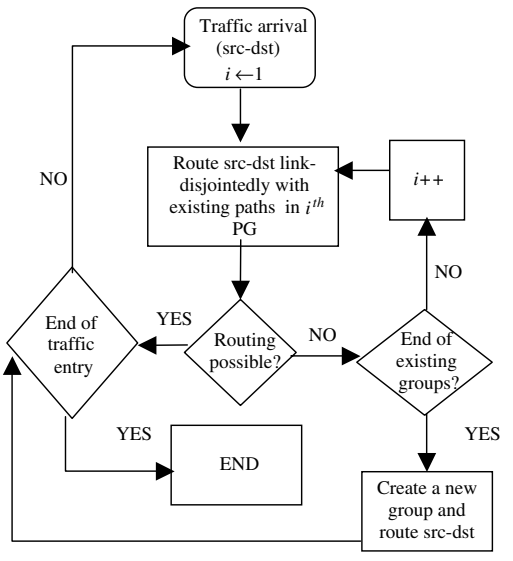
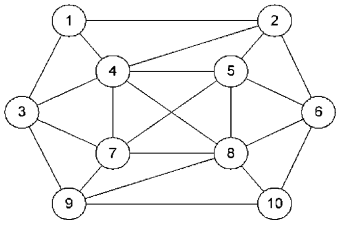


Fig. 2. Establishing a newly arrived connection request into a PG.



a

S	D	Working Path	Protection Path
1	6	1-2-6	1-4-5-6
1	6	1-3-7-8-6	1-4-5-6
7	8	7-9-10-8	7-5-8

b

S	D	Working Path	Protection Path
3	10	3-9-10	3-7-8-10
1	2	1-2	1-3-7-8-10-2
4	6	4-5-6	7-5-8

c

Fig. 3. (a) Ten node topology, (b) *PG 1*, and (c) *PG 2*.

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

3.2. ILP formulation

An ILP approach is proposed to optimally reconfigure the existing protection capacity in a PG 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 [21] because the number of working and protection path-pairs is limited by the network topology. Thus, the proposed ILP can be well suited to the dynamic traffic scenario. 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 PG will be reconfigured so that sharing of spare capacity is maximized. The following 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 PG so that sharing of spare capacity is maximized in that PG. Let W be the set of all existing working paths in a PG and let N be the number of working paths in that group. Now $k = N + 1$ for that PG which means the kth working–protection pair need to be setup in that PG. Let $W = \{w^1, w^2, \ldots, w^{k-1}\}$ and $P = \{p^1, p^2, \ldots, p^{k-1}\}$ be the set of all existing working and protection paths respectively in that particular PG. Note that, while setting up the working–protection pair for kth connection request for a group, only P will be reconfigured.

Let $x_{i,j}^k$ 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., $x_{i,j}^1, x_{i,j}^2, \ldots, x_{i,j}^{k-1}$) provides link-state information to the ILP for a current connection request k. These values are collected and supplied to the ILP. Let $y_{i,j}^k$ 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:

$$\text{Minimize} \quad \sum_{i,j}\sum_{k} x_{i,j}^{k} + \sum_{i,j} z_{i,j}, \tag{1}$$

Subject to

$$\sum_{j} x_{i,j}^{k} - \sum_{j} x_{j,i}^{k} = \begin{cases} 1 & \text{if } i = \text{src}, \\ -1 & \text{if } i = \text{dst}, \\ 0 & \text{otherwise}, \end{cases} \tag{2}$$

$$\sum_{j} y_{i,j}^{k} - \sum_{j} y_{j,i}^{k} = \begin{cases} 1 & \text{if } i = \text{src}, \\ -1 & \text{if } i = \text{dst}, \\ 0 & \text{otherwise}, \end{cases} \tag{3}$$

$$\sum_{k} x_{i,j}^{k} + \sum_{k} x_{j,i}^{k} \leqslant 1, \tag{4}$$

$$x_{i,j}^{k} + y_{i,j}^{k} + x_{j,i}^{k} + y_{j,i}^{k} \leqslant 1, \tag{5}$$

$$y_{i,j}^{k} \leqslant z_{i,j}. \tag{6}$$

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 $(x_{i,j}^{1}, x_{i,j}^{2}, \ldots, x_{i,j}^{k-1})$ variables represent the current link state information for a particular PG for a current connection request k. These link state values (i.e., $x_{i,j}^{1}, x_{i,j}^{2}, \ldots, x_{i,j}^{k-1}$) 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 PG. Case 1: There is only one group in the network, ILP is applied to the only existing group and if the current connection k cannot 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 cannot be satisfied by the previous group. If a connection cannot be established by any of the existing groups, then a new group is created to satisfy k.

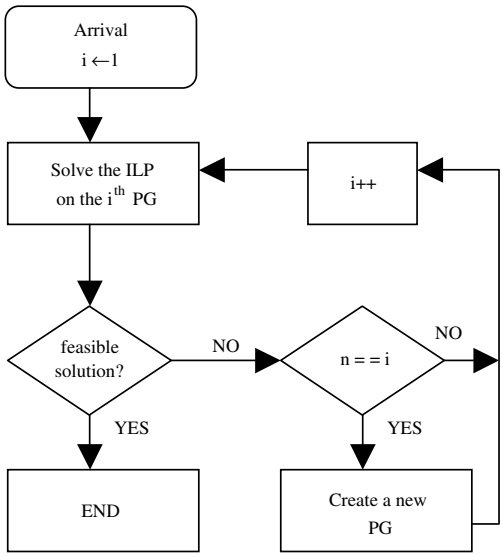


Fig. 4. Managing connection requests using ILP.

Let us assume that there is currently n PG in the network and a new connection request k arrives that needs to be satisfied through ILP. The flowchart in Fig. 4 explains how ILP is used to manage the dynamic connection request for spare capacity reconfiguration.

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

3.3. Heuristics

The above ILP scheme is appropriate for a dynamic traffic scenario where inter-arrival time is large and where arriving request can tolerate some delay, but may not be suitable where traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link-shared protection (LSP) are proposed. Dijkstra's shortest path algorithm (in terms of hop count) is adopted as routing scheme for determining working and protection paths. The following three rules are used while describing the heuristics:

Rule 1: All the working paths in a PG G have to be mutually link-disjoint.
Rule 2: Working path W and its corresponding protection path P are link disjointedly routed in a PG.
Rule 3: A protection ring R needs to cover all source–destination nodes of existing working paths in a PG.

3.3.1. Ring shared protection (RSP)

RSP 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 PG.

Fig. 5a and b explain ring-shared protection. Working paths (A–B–C–J), (C–L–I) and (F–K–I) in a PG 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 [11]. For computational efficiency, the 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 PG. Dijkstra's shortest path algorithm (in terms of hop count) is adopted as routing scheme in RSP. A PG starts with only one source–destination pair. The size of a PG increases whenever it accommodates a new connection request. Fig. 6 explains how dynamic connection request is managed in RSP.

In Fig. 6, there is n number of existing PGs. Upon arrival of a new connection request, RSP starts checking sequentially the n PGs whether a link-disjoint working path can be established for new connection request along with the protection ring. As soon as it finds a PG that satisfies these

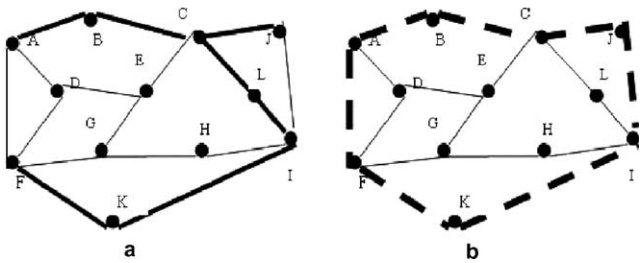


Fig. 5. (a) Three link-disjoint working paths (A–B–C–J), (C–L–I) and (F–K–I) in a PG. (b) Protection ring A–F–K–I–J–C–B–A provides protection for three working paths in (a).

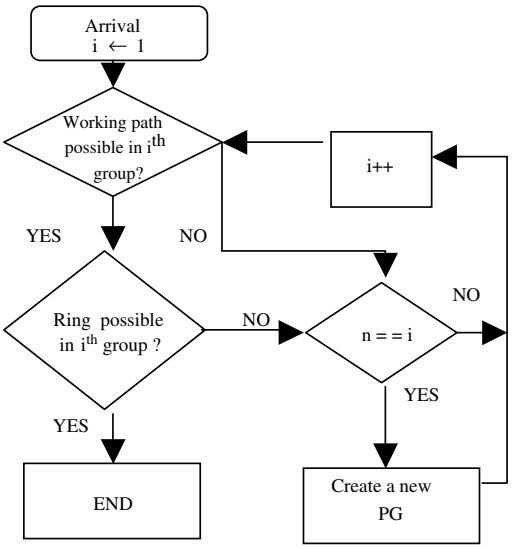


Fig. 6. Managing connection arrival in RSP.

requirements, it accommodates the new connection in that PG. If there are no groups available where the new connection can be accommodated, it creates a new PG 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.

3.3.2. Link shared protection

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 [5] 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 PG. 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 PG.

Fig. 7 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

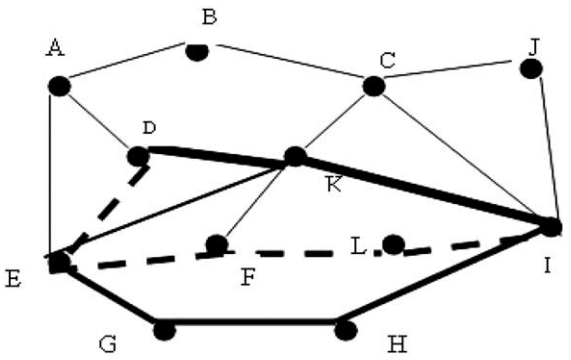


Fig. 7. Link-shared protection (LSP).

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 PG. 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 follows Rules 1 and 2. Note that in LSP, existing protection capacity in a PG is never reconfigured. A dynamically arrived connection request is satisfied by checking Rules 1 and 2 without reconfiguration of existing protection capacity.

In Fig. 8, there is n number of existing PGs. Upon arrival of a new connection request, LSP

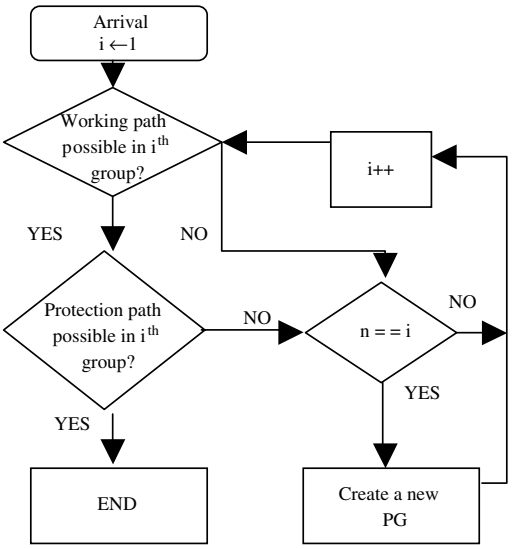


Fig. 8. Managing connection arrival in LSP.

starts checking sequentially the n PGs whether a link-disjoint working path can be established for new connection request along with the protection path. As soon as it finds a PG that satisfies these requirements, it accommodates the new connection in that PG. If there are no groups available where the new connection can be accommodated, it creates a new PG and accommodates the request in $(n+1)$th group. Similar to RSP, size of the PG in LSP increases whenever it accommodates a new connection request.

4. Results and discussion

The simulation is conducted on eight different mesh networks [6,12] shown in Fig. 9, which are chosen as representatives of typical mesh

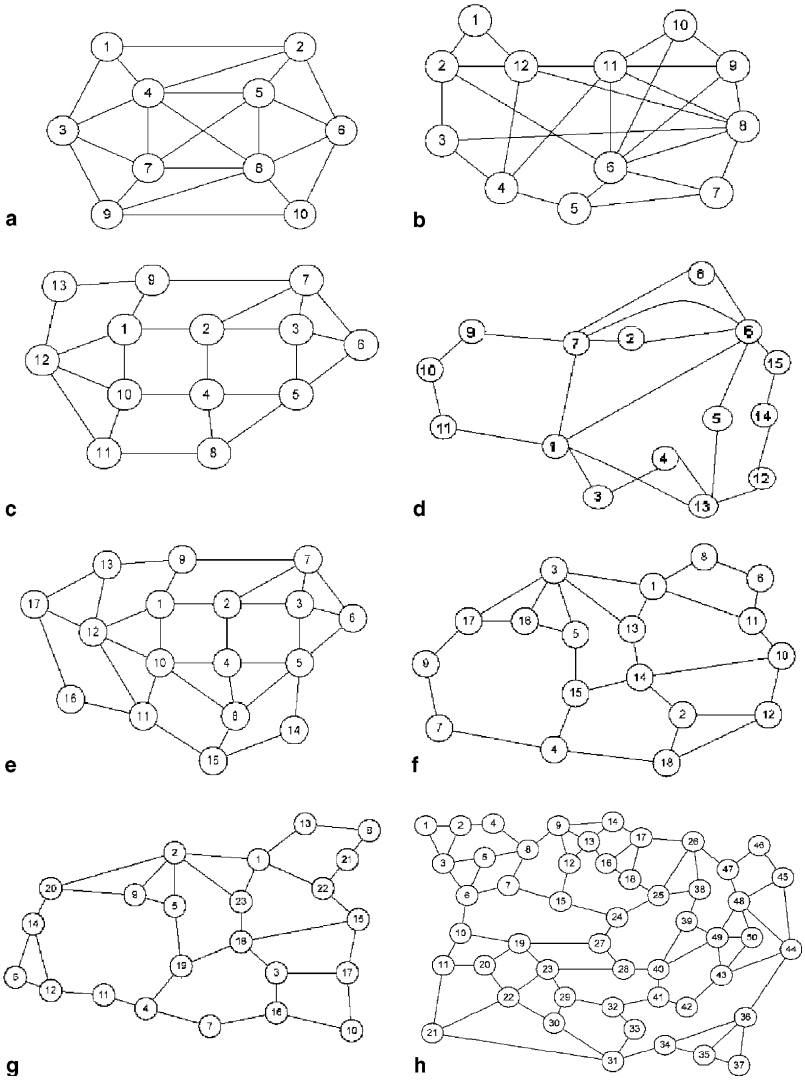


Fig. 9. (a) 10 node topology, $l = 22$, $d = 4.4$; (b) 12 node topology, $l = 25$, $d = 4.17$; (c) 13 node topology, $l = 23$, $d = 3.54$; (d) 15 node topology, $l = 23$, $d = 3.07$; (e) 17 node topology, $l = 31$, $d = 3.65$; (f) 18 node topology, $l = 27$, $d = 3.00$; (g) 23 node topology, $l = 27$, $d = 3.00$ (h) 50 node topology, $l = 82$, $d = 3.28$.

topologies. The CPLEX linear optimizer is used to solve the proposed ILP. The performance metrics used in the simulation 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 while 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. (d) Each node can serve as an ingress or egress node in the network with full wavelength conversion. (e) Dijkstra's shortest path algorithm (in terms of hop count) is adopted as the routing scheme for determining working and protection paths.

Since the objective of this study is to compare the performance of ILP and the heuristics in terms of capacity utilization, some constraints are relaxed to avoid connection blocking. This relaxation includes keeping the number of wavelength channels along each link very high and assuming that each link has a full wavelength conversion capacity.

Table 1 shows the simulation results for the number of wavelengths required by the standard dedicated protection (SDP), ring-shared protection (RSP), link-shared protection (LSP), 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.

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

Table 1
Total wavelengths used by protection schemes

$\|V\|$	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 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 2 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 significant reduction in restoration overhead.

We also observe the traffic distribution while using different schemes. To investigate the effect of grouping, LSP and SSR [6] 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. 10 shows the load distribution in the 23-node network, where

Table 2
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

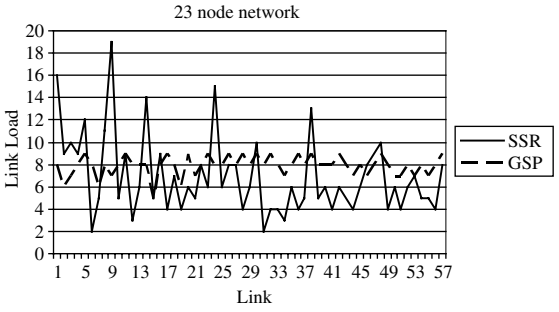


Fig. 10. Load distribution in GSP and SSR—comparison between the cases of grouping and non-grouping.

we assume that the number of wavelengths along each link is infinite.

5. Conclusions

In this paper, we presented our proposed group shared protection (GSP) for spare capacity reconfiguration. Based on the $(M{:}N)^n$ protection architecture defined for the generalized multi-protocol label switching (GMPLS), GSP is characterized by grouping the working and protection paths in the network such that the spare capacity reconfiguration can be performed in a scalable way. For this purpose, an ILP-based approach was used for dividing the working traffic, allocating the current connection requests, and reconfiguring the spare capacity in each protection group (PG). Furthermore, two heuristics were introduced, namely ring-shared protection (RSP) and link-shared protection (LSP).

The advantages of GSP include: (a) control flexibility; (b) spare capacity in a PG totally sharable among corresponding working paths; (c) significant reduction in computation complexity since the spare capacity in a specific PG is used for protecting the working capacity in that PG only; (d) computation time for jointly allocating the current working–protection paths pair and reconfiguring the spare capacity in each PG through ILP is well constrained and is reasonable for dynamic traffic scenario, and (e) limits the number of working paths affected by a single failure.

Through simulations, we evaluated our proposal and compared it with an existing one, namely the successful survivable routing (SSR). The simulation results showed similar performance 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%. Also, with GSP, the number of affected working paths in case of a single link failure is around half of that with SSR. This yields a significant saving in restoration overhead. In light of the obtained results, we believe that GSP is a suitable scheme for highly scalable and survivable networks such as the future optical Internet.

References

[1] D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G. Li, B. Rajagopalan, 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, N. Golmie, Backup resource pooling in $(M{:}N)^n$ fault recovery schemes in GMPLS optical networks, in: Opticomm 2003.

[3] P.-H. Ho, H.T. Mouftah, A framework of a survivable optical internet using short leap shared protection (SLSP), in: IEEE Workshop on High Performance Switching and Routing (HPSR 2001), Dallas, May 2001.

[4] B. Ramamurthy, A. Ramakrishnan, Design of virtual private networks (VPNs) over optical wavelength division multiplexed (WDM) networks, SPIE Optical Networks Magazine 3 (1) (2002).

[5] P.-H. Ho, H.T. Mouftah, On optimal diverse routing for shared protection in mesh WDM networks, IEEE Transactions on Reliability 53 (6) (2004) 216–225.

[6] Y. Liu, D. Tipper, P. Siripongwutikorn, Approximating optimal spare capacity allocation by successive survivable routing, in: Proceedings IEEE Infocom'01, vol. 2, April 2001, pp. 699–708.

[7] S. Datta, S. Sengupta, S. Biswa, Efficient channel reservation for backup paths in optical mesh networks, in: Proceedings IEEE Globecom'01, San Antonio, TX, November 2001.

[8] C. Xin, Y. Ye, S. Dixit, C. Qiao, A joint lightpath routing approach in survivable optical networks, Optical Network Magazines (May/June) (2002) 23–32.

[9] E. Bouillet, J.-F. Labourdette, G. Ellina, R. Ramamurthy, S. Chaudhuri, Stochastic approaches to compute shared mesh restored lightpaths in optical network architectures, in: Proceedings IEEE Infocom, 2002.

[10] D. Xu, C. Qiao, Y. Xiong, An ultra-fast shared path protection scheme—distributed partial information management, Part II, in: Proceedings IEEE International Conference on Network Protocols (ICNP 2002), Paris, France, November 2002.
[11] A. Fink, G. Schneidereit, S. Vo, Ring network design for metropolitan area networks, TU Braunschweig (March 17) (1998).
[12] S. Ramamuthy, B. Mukherjee, Survivable WDM mesh networks: Part I–Protection, in: Infocom'99, New York, March 1999.
[13] O.J. Wasem, Optimal topologies for survivable fiber optic networks using SONET self-healing ring, in: Proceedings IEEE GLOBECOM'91, November 1991, pp. 2032–2038.
[14] O.J. Wasem, An algorithm for designing rings for survivable fiber networks, IEEE Transactions on Reliability 40 (1991) 428–432.
[15] C. Thomassen, On the complexity of finding a minimum cycle cover of a graph, SIAM Journal of Computation 26 (3) (1997) 675–677.
[16] G. Ellinas, T.E. Stern, Automatic protection switching for link failures in optical networks with bi-directional links, in: Proceedings IEEE GLOBECOM'96, vol. 1, November 1996, pp. 152–156.
[17] G. Ellinas, A.G. Hailemariam, T.E. Stern, Protection cycles in mesh WDM networks, IEEE Journal on Selected Areas in Communications 18 (10) (2000).
[18] D. Stamatelakis, 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, October 2000.
[19] W.D. Grover, D. Stamatelakis, Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration, in: Proceedings IEEE International Conference on Communications, vol. 1, June 1998, pp. 537–543.
[20] W.D. Grover, J.B. Slevinsky, M.H. MacGregor, Optimized design of ring-based survivable networks, Canadian Journal of Electrical and Computer Engineering 20 (3) (1995) 138–149.
[21] CPLEX: An optimizer by ILOG Inc, www.ilog.com.
[22] J.Q. Hu, Diverse routing in mesh optical networks, IEEE Transactions on Communications 51 (3) (2003) 489–494.
[23] G. Li, B. Doverspike, C. Kalmanek, Fiber span failure protection in mesh optical networks, in: Opticomm, August 2001.
[24] E. Modiano, A. Narula-Tam, Survivable lightpath routing: a new approach to the design of WDM-based networks, IEEE Journal of Selected Areas of Communications 20 (4) (2002) 800–809.
[25] G. Shen, W.D. Grover, Extending the *p*-cycle concept to path segment protection for span and node failure recovery, IEEE Journal on Selected Areas in Communications 21 (8) (2003) 1306–1319.
[26] H. Wang, E. Modiano, M. Medard, Partial path protection for WDM networks: end-to-end recovery using local failure information, in: IEEE ISCC, July 2002.

Anwar Haque received the B.S. and M.Sc. degrees in Computer Science from the North South University, Bangladesh, and from the University of Windsor, ON, Canada, in 1997 and 2001, respectively. He is working towards the Ph.D. degree in Computer Science at the University of Waterloo, ON, Canada. He has published more than 15 referred technical papers. He has served as a reviewer for many international journals and conferences. His research interests include WDM optical networks with focus on survivability, Quality of Service (QoS), and network security. He is the recipient of the University of Waterloo Graduate Scholarship, Natural Sciences and Engineering Research Council of Canada Industrial Postgraduate Scholarship (NSERC-IPS), Ontario Graduate Scholarship (OGS), and David R. Cheriton Graduate Scholarship.

Pin-Han Ho received his B.Sc. and M.Sc. Degree from the Electrical and Computer Engineering department in the National Taiwan University in 1993 and 1995. He started his Ph.D. study in the year 2000 at Queen's University, Kingston, Canada, focusing on optical communications systems, survivable networking, and QoS routing problems. He finished his Ph.D. in 2002, and joined the Electrical and Computer Engineering department in the University of Waterloo, Waterloo, Canada, as an assistant professor at the same year. He is the first author of more than 70 referred technical papers and book chapters, and the co-author of a book on optical networking and survivability. He is the recipient of the Best Paper Award in SPECTS'02 and ICC'05 Optical Networking Symposium, and the Outstanding Paper Award in HPSR'02.

Raouf Boutaba is an Associate Professor in the School of Computer Science of the University of Waterloo. Before that he was with the Department of Electrical and Computer Engineering of the University of Toronto. Before joining academia, he founded and was the director of the telecommunications and distributed systems division of the Computer Science Research Institute of Montreal (CRIM). He conducts research in the areas of network and distributed systems management and resource management in multimedia wired and wireless networks. He has published more than 150 papers in referred journals and conference proceedings. He is the recipient

of the Premier's Research Excellence Award, the NORTEL Networks research excellence Award and several Best Paper awards. He is a fellow of the faculty of mathematics of the University of Waterloo and a distinguished lecturer of the IEEE Computer Society. He is the Chairman of the Working Group on Networks and Distributed Systems of the International Federation for Information Processing (IFIP), the Vice Chair of the IEEE Communications Society Technical Committee on Information Infrastructure, and the Director of standards board of the IEEE Communications Society. He is the founder and acting editor in Chief of the IEEE eTransactions on Network and Service Management, on the advisory editorial board of the Journal of Network and Systems Management, on the editorial board of the KIKS/IEEE Journal of Communications and Networks, the editorial board of the Journal of Computer Networks and the Journal of Computer Communications. He has also served as a guest editor of several special issue of IEEE Journal of Selected Areas in Communications (JSAC), the Journal of Computer Networks, the Journal of Computer Communications and the Journal of Network and System Management. He acted as the program chair for the IFIP Networking conference and the IEEE Consumer Communications and Networking Conference (CCNC), and a program co-chair for the IEEE/IFIP Network Operation and Management Symposium (NOMS), the IFIP/IEEE Conference on Management of Multimedia Networks and Services (MMNS), the IEEE Feature Interaction Workshop, the IEEE Autonomic Computing and Communications (ACC) and two IEEE International Conference on Communications (ICC) symposia.